TARTU ÜLIKOOL
ÕIGUSTEADUSKOND
Avaliku õiguse instituut

Merike Küngas

TRADITSIOONILISTE ÕIGUSKAITSEVAHENDITE RAKENDATAVUS ISIKUANDMETE KAITSE ÕIGUSE TAGAMISEL INFOÜHISKONNAS JA NENDE VÕIMALIKEST ARENGUTEST

Magistritöö

Juhendaja
Prof. Raul Narits

Tallinn
2015

Sisukord

Sissejuhatus

Franklin Roosevelt'i teadusminister Vannevar Bush kirjutas oma essees „*As We May Think*" järgmist: „Teises maailmasõjas lõi teadus suurima hävitustehnoloogia, mida eales on nähtud. Uuel ajastul aitab teadus aga kaasa suurimale teadmistetehnoloogia sünnile, mida inimkond kunagi on tunnistanud".[1] Teadmistetehnoloogia, millest V. Bush kirjutas, oli visioon saabuvast infoühiskonnast.

Magistritöö autori hinnangul oli teadusministril õigus, sest maailm on läbi teinud revolutsioonilise info- ja kommunikatsioonitehnoloogia (IKT) arengu, mille tulemusena elatakse 2015. aastal ühiskonnas, kus inimeste elusid juhib internet ja informatsioon. Informatsiooni ei ole olnud kunagi rohkem, kui praegu, sest ühiskonna „nälg" info järele on suurem kui eales varem. Nõudluse suurenedes kasvab ka pakkumine, mistõttu eksisteerivad infohulgad on muutunud mõõtmatuks tänu innovaatilistele IKT lahendustele.

Innovaatilised tehnoloogilised lahendused esitavad väljakutse nii riigile tervikuna kui ka igale indiviidile eraldi, sest infoühiskonnas mängib pearolli inimene ja temaga seonduvad andmed. IKT võimaldab aga ulatuslikke andmekaitseõiguse rikkumisi, mistõttu on infoühiskonnas oluline kaitsta isikute privaatsusõigust. 2013. aasta jaanuaris privaatsuse ja andmekaitse teemalisel konverentsil väitis konverentsi patroon Eesti Vabariigi president Toomas Hendrik Ilves, et Eesti on oma ühiskonna põhiprotsesside digitaliseerimises läinud kaugemale kui ükski teine riik maailmas ja see kõik käib turvaliselt. Oluline on aga selles turvalises süsteemis muuta mõtteviisi privaatsusest mõiste privaatsuse tähenduse muutumise tõttu, mis on tingitud tehnoloogia arengust. T. H. Ilves kasutas privaatsuse uue tähenduse iseloomustamiseks John Perry Barlow[2] sõnu öeldes, et õiguslikud kontseptsioonid, mis on liberaalse demokraatia aluseks, tõesti ei pruugi enam meie kohta kehtida, keda iganes "meie" all ka mõelda.[3]

IKT ja üleilmastumise kiire areng on teinud võimalikuks automatiseeritult koguda, kasutada ja edastada suurtes kogustes isikustatud andmeid. Euroopas on umbes 250 miljonit internetikasutajat, kelle elusid mõjutavad uued teabevahetuskanalid ja suurte andmehulkade

[1] G. D. Garson. Public Information Technology and E-Governance: Managing the Virtual State. London: Jones and Barlett Publishers International 2006, lk 3.
[2] J. P. Barlow on USA luuletaja ja esseist ning Harvardi ülikooli teadur.
[3] T. H. Ilves. Kõne demokraatiaorganisatsiooni NDI 30. aastapäeva auhinnadineel Washingtonis 10. detsembril 2013. Arvutivõrgus: http://president.ee/et/ametitegevus/koned/9712-2013-12-17-13-28-46/index.html, 26.01.2014.

kaugsäilitamine. Kui varem oli isikute kohta andmete kogumine valitsuste privileeg, siis tänapäeval omab palju infot isikute kohta ka erasektor. Isikuandmed on trumbiks paljude ettevõtjate jaoks. Potentsiaalsete klientide andmete kogumine, koondamine ja analüüsimine moodustab sageli olulise osa nende majandustegevusest.[4] Tänapäeva majanduse kontekstis peame rääkima digitaalmajandusest, mille edukuses IKT etendab väga tähtsat rolli. Kuigi IKT ajaloolist mõju, selle lühiduse tõttu, on võib-olla veel liiga vara hinnata, siis IKT seos majanduskasvuga paistab väga selgelt silma uute töökohtade loomisega, majandusliku kasu toomisega ja üldise heaolu soodustamisega. Lisaks majanduslikule mõjule on IKT-l ka oluline roll innovatsiooni ja loomingulisuse arendamisel.[5]

Eesti eduka IKT arengu tulemuseks on e-riik. Eesti e-riigi areng sai alguse, kui 1998. aastal võeti vastu Eesti esimene infopoliitiline dokument[6], milles sedastati, et infoühiskond on kogu sotsiaalne reaalsus, milles elatakse ja informatsioonitehnoloogia revolutsioon on muutnud ja muudab tänast maailma, kuigi kõiki eesolevaid muutusi ei hoomata. Eesti e-riigina on kogunud ülemaailmselt palju tunnustust oma innovaatiliste lahendustega, mis on sündinud avaliku sektori ja erasektori koostöös. Eesti tunnussõnadeks on digitaalallkiri, eID, mobiil-ID, e-valimised ja andmevahetuskiht X-tee. Viimase e-saavutusena on Eesti rahvusvahelist tuntust omandanud e-residendi programmiga. IKT arendamine riiklikul tasandil on endiselt üks Eesti prioriteete, mille üheks näitajaks on seegi, et ministeeriumid loovad valitsemisalaüleseid infotehnoloogiaasutusi e-teenuste arendamiseks ja haldamiseks. Tunnustus Eestile kui e-riigile oli ka Euroopa Liidu siseministrite otsus rajada Tallinnasse Euroopa Liidu IT-agentuuri peakorter. Suures plaanis võib tõdeda, et Eesti on juba muutunud või kohe muutumas üheks IKT kompetentsikeskuseks Euroopas, kui mitte maailmas. E-Eesti edulugu ei ole tõenäoliselt veel lõppenud.

Informatsioon demokraatiat edasi viiva jõuna on oluline osa heast riigivalitsemisest. Halb valitsus vajab ellujäämiseks saladusi. Kui rahvas ei tea, mis ühiskonnas toimub ja valitsuse tegevus ei ole läbipaistev, siis rahvas ei saa omada tähenduslikku rolli oma ühiskonna tegevustes.[7] Saksamaa konstitutsioonikohus rõhutas, et automatiseeritud andmetöötluse

[4] Euroopa Komisjoni 25.01.2012 teatis „Eraelu puutumatuse kaitsmine ühendatud maailmas. Euroopa isikuandmete kaitse raamistik 21. sajandil“. KOM (2012) 9 (lõplik), lk 2. Arvutivõrgus: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0009:FIN:ET:HTML, 09.03.2014.
[5] Euroopa andmekaitseinspektori arvamus, mis käsitleb usalduse suurendamist infoühiskonnas andmekaitse ja eraelu puutumatuse tugevdamise kaudu. – ELT C 280/01, 16.10.2010, lk 2.
[6] Eesti Infopoliitika põhialused. – RT I 1998, 47, 700.
[7] Mendel, T. The Public's Right to Know. Principles on Freedom of Information Legislation. – London: Article 19, 1999, lk 1. Arvutivõrgus: http://www.article19.org/data/files/pdfs/standards/righttoknow.pdf, 05.02.2014.

ajastu, kus paar hiireklikki loob inimesest tervikpildi, ei viita mitte üksnes ühe indiviidi piiratud eneseteostusele, vaid tähendab ka ohtu demokraatlikule ühiskonnakorraldusele.[8]

Infoühiskonna arenedes sünnib aina uusi e-teenuseid, mis toovad kaasa erinevaid isikuandmeid sisaldavate andmekogude moodustamise. Andmekogud peavad olema turvalised, et tagada isikuandmete kaitse. Isik peab teadma, kes tema kohta andmeid kogub, milliseid andmeid tema kohta kogutakse ja millisel eesmärgil neid andmeid kasutatakse. Tänapäeva tehnoloogiliste võimaluste juures inimesed sageli ei teagi, kes ja kus tema andmeid töötleb, mistõttu puudub isikul kontroll oma isikuandmete üle. Andmete vahetamine infosüsteemide vahel nii riigisiseselt kui ka piiriüleselt on lubatud, kui on tagatud isikute privaatsusõigus, mis infoajastul seisneb eelkõige õiguses isikuandmete kaitsele. Informatsioon annab selle valdajale võimu ja seetõttu on oluline kaitsta üksikisiku õigusi andmete töötlemisel tekkida võivate võimalike andmete kuritarvitamiste eest. Kaasaegsel automatiseeritud andmetöötluse ajastul peab riik olema võimeline tagama üksikisikule põhiõigusena isikuandmete kaitse õiguse, mis on osa demokraatlikust riigikorraldusest.

Magistritöö autori hinnangul on oluline, et õigus ja IKT areneksid paralleelselt ajas ja ruumis. Infoühiskonnas, kus kõigi tähelepanu on suunatud tehnoloogiale, valitseb oht, et õigus võib jääda teisejärguliseks. Eelnimetatu vältimiseks, üksikisikute õiguste tõhusamaks tagamiseks ning andmekaitseõiguse harmoniseerimiseks Euroopa Liidu liikmesriikides algatas Euroopa andmekaitse reformi, mille tulemusena kehtestatakse Euroopa Liidu liikmesriikidele otsekohalduv isikuandmete kaitse üldmäärus. Andmekaitsereform on kogunud aktuaalsust kogu Euroopas, sest tegemist on konkreetsete privaatsusreeglite kehtestamisega võrguühiskonnas, millega omavad puutumust üldjuhul kõik inimesed. Lisaks rõhutavad magistritöö teema päevakajalisust ka 2014. aasta Euroopa Kohtu otsused, mida võib nimetada teedrajavateks lahenditeks ning millest esimene[9] puudutab üldkasutatavate elektrooniliste sideteenuste või üldkasutatavate sidevõrkude pakkujate tegevusega kaasnevate või nende töödeldud andmete säilitamist käsitlevat direktiivi 2006/24/EÜ[10] ja millega muudetakse

[8] Teder, I. Kas soovime suletud ühiskonda? Postimees 7.06.2012. Arvutivõrgus: http://arvamus.postimees.ee/868200/indrek-teder-kas-soovime-suletud-uhiskonda, 05.02.2014.

[9] EKo 08.04.2014, C-293/12 ja C-594/12, Digital Rights Ireland Ltd. v Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Ireland.

[10] Euroopa Parlamendi ja nõukogu 15.03.2006. a direktiiv 2006/24/EÜ, üldkasutatavate elektrooniliste sideteenuste või üldkasutatavate sidevõrkude pakkujate tegevusega kaasnevate või nende töödeldud andmete säilitamist ja millega muudetakse direktiivi 2002/58/EÜ, EÜT L 105/54, 13.04.2006.

direktiivi 2002/58/EÜ[11] ning teine[12] interneti otsingumootori andmete kõrvaldamise kohustust interneti otsingumootorilt ning „õigust olla unustatud“ internetikeskkonnas.

Magistritöö autori arvates pälvivad uudsed tehnoloogiad alati palju rohkem tähelepanu, kui miski muu. Kui tänasel päeval on tegemist pilvtehnoloogiate aina hoogustuva levikuga, asjade interneti ja suurandmete pealetungiga, siis homme on tehnoloogia juba pilvest kaugemale arenenud ning ülehomset arengut ei oska veel ette nähagi. Ajaga muutub IKT aina võimsamaks ja keerulisemaks, võimaldades töödelda tohutus koguses informatsiooni sh ka isikustatud andmeid, mistõttu ei tohi selles tehnoloogia maailmas unustada isikut ja tema õiguseid. Samamoodi ei tohi ka inimene ise unustada, millist ohtu tema ja teiste kaasisikute privaatsusele võivad endas kujutada kaasaskantavad ja isikustatud informatsiooni sisaldavad nutiseadmed, mida on võimalik igal ajahetkel internetti ühendada ja nii oma andmeid erinevate meediate ja keskkondade vahel jagada. Ajaga aina arenev IKT esitab väljakutse nii tehnoloogia tootjale, seadusandjale kui ka üksikisikule endale. IKT, mis on oluline osa igapäevaelust, on loonud olukorra, kus isikutel on kadunud kontroll selle üle, kes ja miks nende kohta andmeid kogub ning kus ja millistel tingimustel neid andmeid hoitakse. Selleks, et oma õiguseid kaitsta peab isik teadma oma õiguseid, peab teada saama oma õiguste rikkumisest ning tundma õiguskaitsevahendeid, mida rikkumiste korral rakendada. Kui arvestada infotehnoloogilistele keskkondadele iseloomulikku keerukust, siis isik ei pruugigi teada saada oma andmekaitseõiguse rikkumisest. Juhul, kui isik saab teada oma õiguste rikkumisest, siis kehtivad õiguskaitsevahendid peavad olema ka sisuliselt rakendatavad isiku õiguste kaitseks tänapäeva IKT tingimustes.

Kui IKT on oma arengus jõudnud muuhulgas erinevate innovaatiliste privaatsustehnoloogiate tasemele ja internetitegevus on andmekaitses suure riskiga valdkond, siis Euroopas kehtiv andmekaitsedirektiiv[13] on endiselt pärit aastast 1995. Võrreldes IKT arenemiskiirust õiguse, mitte ainult andmekaitseõiguse, arenemise kiirusega, siis on igati õigustatud küsimus – kas tänasel hetkel digitaliseeritud ühiskonnas kehtivatest õiguskaitsevahenditest piisab kaitsmaks isikute õigust oma isikuandmete kaitsele? Kas seadusandja suutis ligi 20 aastat tagasi ette näha tänapäevaseid tehnoloogilisi arenguid ja kehtestas õigusakti, mis õigustab ennast ka tänapäeval? Eeltoodust tulenevalt püstitab magistritöö autor hüpoteesi, et hetkel kehtivad

[11] Euroopa Parlamendi ja nõukogu 12.07.2002. a direktiiv 2002/58/EÜ, milles käsitletakse isikuandmete töötlemist ja eraelu puutumatuse kaitset elektroonilise side sektoris (eraelu puutumatust ja elektroonilist sidet käsitlev direktiiv), EÜT L 201, 31.07.2002.
[12] EKo 13.05.2014, C-131/12, *Google Spain v Agencia de Protectíon de Datos, Mario Coseja Gonzáles*.
[13] Euroopa Parlamendi ja nõukogu 24.10.1995. a direktiiv 95/46/EÜ üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta, EÜT L 281, 23.11.1995.

õiguskaitsevahendid isikuandmete kaitse õiguse kui privaatsusõiguse tagamiseks ei ole tänases progresseeruvas infoühiskonnas enam sisuliselt rakendatavad.

Magistritöö eesmärgiks on hinnata kehtivate õiguskaitsevahendite rakendatavust ja infoühiskonnast tulenevat võimalikku vajadust uute õiguskaitsevahendite järele, et digitaliseeritud maailmas kaitsta põhiõigushüvena isiku õigust oma isikuandmete kaitsele. Magistritöös selgub, kas eksisteerib vajadus "uue õiguse" järele. Magistritöö eesmärgiks ei ole hinnata, kas käimasolev Euroopa andmekaitsereform täidab oma eesmärgid, kui kehtestatakse isikuandmete kaitse üldmäärus, vaid kas eelnimetatud üldmääruses sisalduvad õiguskaitsevahendid isikuandmete kaitse õiguse tagamiseks õigustavad ennast võrguühiskonnas või mitte.

Magistritöös püstitatud hüpoteesi tõestamiseks püstitab autor järgmised uurimisküsimused:

1) Millised isikuandmete kaitsega seonduvad õiguslikud probleemid on seotud digiühiskonnas toimuva IKT arenguga?
2) Kas objektiivsest õigusest tulenevad õiguskaitsevahendid andmekaitseõiguse tagamiseks peegeldavad adekvaatselt IKT arenguid?
3) Kas kvalitatiivsed muudatused isikuandmete kaitse tagamiseks kehtestatud õiguskaitsevahendites on vajalikud?
4) Milline peaks olema isikuandmete kaitse õiguslik regulatsioon kaasaegses infoühiskonnas?

Magistritöö koosneb kolmest peatükist, mis jagunevad alapeatükkideks vastavalt teemakäsitlustele.

Esimeses peatükis käsitleb magistritöö autor, millist mõju on IKT areng avaldanud isikute andmekaitseõigusele. Magistritöö autor heidab samuti pilgu andmekaitseõiguse ajalukku ning vaatleb, kuidas on tänasesse tegelikkusesse jõutud ja käsitleb eraelu puutumatuse ja isikuandmete kaitse kontseptsioonide omavahelisi seoseid. Magistritöö autor toob välja nii siseriiklikust, Euroopa Liidu kui ka rahvusvahelisest õigusest tulenevad tagatised isikuandmete kaitse tagamiseks. Kõne alla tuleb ka hetkel tähelepanu keskmes olev Euroopa andmekaitsereform ning reformiga kaasnevate uute õigusmeetmete roll üksikisiku põhiõiguste tagamisel. Kõneallolevas peatükis selgub, kas kehtivatest õiguskaitsevahenditest piisab üksikisiku isikuandmete kaitsmiseks infoühiskonnas.

Teises peatükis keskendub magistritöö autor tänasele tegelikkusele tehnoloogiamaailmas ja analüüsib, kas tänane reaalsus vastab ka homsetele vajadustele, tuues välja probleemid seoses isikuandmete kaitsega, mis on tõusetunud seoses uue IKT seadmete kasutusele võtmisega. Magistritöö autor pühendub sisuliselt ka neljale tehnoloogilisele trendile andmetöötluses, milleks on pilvetehnoloogiad, suurandmed ja profileerimine ning asjade internet. Eelnimetatud trendide puhul toob magistritöö autor välja, mismoodi on need tehnoloogiad seotud isikuandmetega ja milliseid ohte kätkevad need uued andmetöötlustehnoloogiad isikuandmete kaitse õigusele kui põhiõigusele. Magistritöö autor pöörab tähelepanu õigust kujundavatele strateegiatele ja poliitikatele ning alternatiivsetele võimalustele andmekaitseõiguse tagamisel.

Kolmanda peatüki pühendab magistritöö autor uue isikuandmete kaitse regulatsiooni vajaduse analüüsile tulenevalt magistritöö kahes esimeses peatükis tehtud järeldustest. Samuti hindab magistritöö autor isikuandmete kaitse perspektiive ning autor toob välja oma järeldused ja ettepanekud.

Magistritöö autor kasutab magistritöös püstitatud küsimuste uurimiseks peamiselt analüütilisi ja süsteemseid meetodeid, analüüsides probleemide algpõhjuseid ja tagajärgi, mille tulemusena esitab võimalikke lahendusettepanekuid. Magistritöö autor pöörab tähelepanu ka ajaloole, mis aitab avada uuritavate probleemide tausta.

Magistritöö autori hinnangul on Eestis magistritöö ainelist õiguskirjandust vähe. Magistritöö autorile teadaolevalt on infoühiskonna ja andmekaitse teemadel magistritöid Tartu Ülikoolis kaitsnud Sandra Sillaots[14], Reet Oorn[15] ja Eneken Tikk[16]. Magistritöös kasutatud allikad on valdavalt võõrkeelsed. Magistritöö autor tugineb oma magistritöös tunnustatud õigusteadlaste töödele ning suuresti Euroopa Liidu institutsioonide (Euroopa Komisjon, artikli 29 alusel asutatud andmekaitse töörühm jmt) poolt välja antud materjalidele.

[14] S. Sillaots. Isikuandmete kaitse regulatsiooni ühtlustamine isikuandmete kaitse üldmääruse eelnõus ja selle mõju Eestile. Magistritöö. Tartu: Tartu Ülikool 2014.
[15] R. Oorn. Infoühiskond ja selle erinevad aspektid riigihalduses ja andmekaitses. Magistritöö. Tartu: Tartu Ülikool 2007.
[16] E. Tikk. Informatsioonilise enesemääratlemise rahvusvahelis-õiguslik raamistik, sisustamine Eesti õiguses ja selle praktilisest kohaldamisest veebikeskkonnas. Magistritöö. Tartu: Tartu Ülikool 2004.

Magistritöö autoril on olnud võimalus vahetada mõtteid andmetöötlejatega ning igapäevaselt osaleda andmetöötleja, kes tagab andmete töötlemiseks vajaliku riist- ja tarkvara tõrgeteta toimimise, praktilises tegevuses ja teha magistritöö raames järeldusi. Magistritöös esitatud lahendusettepanekuid saab vajadusel kasutada nii õigusloomes kui ka praktiliste probleemide lahendamisel. Magistritöö autor soovib E-Eestis panustada isikuandmete kaitsesse põhiõiguste tagamise kontekstis, arvestades andmekaitseõiguse piiride ebaselgust reaalsuses.

1. Isikuandmete kaitse õiguslik raamistik

1.1. Info- ja kommunikatsioonitehnoloogia arengu mõju isikuandmete kaitse õigusele

Kui eelmine generatsioon nägi tehnoloogilisi muutusi tööstusliku revolutsiooni näol, siis tänapäeval on tegemist digitaalse revolutsiooniga. Tänase maailma digitaalne areng ei ole mööda läinud isikute privaatsust mõjutamata. Peamiste tehnoloogiliste arengutena, mis on isikute privaatsust sügavalt mõjutanud, võib nimetada suurenenud andmete, sh isikuandmete kogumist, põhjustatuna moodsast salvestustehnikast, andmeturu globaliseerumist ja igaühe võimalust andmeid töödelda ning kontrollimehhanismide puudumist digitaalsete andmete kaitseks. Kõik eelnimetatud digitaalse tehnoloogia arengud on suurendanud informatsiooniga manipuleerimise võimalusi. Digitaalseid andmeid on palju, sest iga liigutus võrguühiskonnas salvestatakse. Kogutud andmeid võib koheselt ja odavalt jagada terve maailmaga. Isikutel on vähe võimalusi kontrollida oma andmete kogumist ja andmetega manipuleerimist, sest enamus isikuid ei ole teadlikudki, kas ja millist informatsiooni kogutakse ja kuidas seda kasutatakse.[17]

Tänapäeva infoühiskonnas tekitavad isikuandmete kaitse valdkonnaga seotud teemad vastandlikke lähenemisi. Ühiskonnas on suurenenud teadmine isikuandmete kaitse tähtsusest ja seda mitte ainult üksikisikute eraelu puutumatusega seoses, vaid ka seoses isikliku vabadusega. Mitmetest rahvuslikest ja rahvusvahelistest dokumentidest tulenevalt tunnustatakse andmekaitset isiku autonoomse õigusena, põhiõigusena, mis ei ole enam hõlmatud eraelu puutumatusega, vaid on eraldiseisev privaatsusõigusest.[18]

Privaatsuse kontseptsioon hõlmab erinevaid dimensioone, kus muude enesemääramise õiguste hulgas eristub isiku õigus informatsioonilisele enesemääramisele. Informatsiooniline enesemääramise õigus seisneb isiku õiguses oma andmete kaitsele. Isikuandmete kaitse üheks peamiseks iseloomustavaks tunnuseks, mis üksiti on ka privaatsusõiguse tuumaks, on olla vaba teiste isikute tähelepanust ja mitte olla teiste poolt jälgitud. Teise iseloomustava tunnusjoonena võib nimetada isikuandmete kaitse elementi, mis muutub oluliseks olukorras, kus keegi kolmas isik omab isikulist informatsiooni ja andmesubjekt tahab kontrollida tema kohta kogutud andmete kasutust sh avalikustamist. Õigus isikuandmete kaitsele on kergesti

[17] W. T. DeVries. Protecting Privacy in the Digital Age. – Berkeley Technology Law Journal 2014, nr 18 (1), lk 291-292.

[18] S. Rodota. Case studies on data protection. Arvutivõrgus: http://www.ictparliament.org/sites/default/files/1pf_odotaCaseStudies.pdf, 07.03.2015, lk 1.

riivatav. Isiku eraelu puudutavad aspektid on tuletatavad ka andmetest, mis seostuvad isiku teiste eluvaldkondadega. Eelnimetatu toob kaasa selle, et isiku teistest eluvaldkondadest pärinevatest andmetest saab osa inimese isikustatud andmetest. Andmetest inimese koduse keskkonna, sotsiaalsuhtlusvõrgustike ja tervise kohta on saanud osa, mida hõlmab informatsiooniline dimensioon. Isikuandmete kaitse omab väärtust, mis aitab kaasa privaatsuse eesmärkide saavutamisel.[19] Privaatsusõiguse ja isikuandmete kaitse õiguse kontseptsioonid on koos IKT arenguga ajas ja ruumis muutunud.

Privaatsuse kontseptsiooni kui eraldiseisvat õiguslikku väärtust tunnustati esmakordselt ning hakati arendama Ameerika Ühendriikides palju varem kui Euroopas. 1890. aastal S. Brandeis ja L. Warren sisustasid privaatsuse mõistet kui „õigust olla üksi jäetud". See õigus pärineb Ameerika Ühendriikide põhiseadusest tulenevatest piirangutest avaliku võimu jõule sekkuda kodanike eraellu ja põhines seega ajalooliselt sügavalt juurdunud usaldamatusel riigivõimu vastu. Ameerikast levis privaatsusõiguse kontseptsioon üle Atlandi ookeani Euroopasse.[20]

Privaatsusõigust inimõigusena võib pidada selle hilise ilmumise tõttu suhteliselt uueks tulijaks.[21] 1.detsembril 2009. aastal jõustus Lissaboni leping, millega andmekaitseõigus sai Euroopa Liidus põhiõiguseks privaatsusõiguse kõrval. Euroopa konstitutsionaalses kontekstis tähendab see vähemalt, et andmekaitselt oodatakse omapoolse väärtuse lisamist privaatsusesse.[22] Oluline on meeles pidada, et privaatsusõigus on seotud, mitte ei ole identne, andmekaitseõigusega. Privaatsusõigus hõlmab isikute õigust olla üksi, õigust olla vaba riigivõimu sekkumisest eraellu ja õigust mitte olla pealtkuulatud, pealtvaadatud või mingil muul moel jälgitud või jälitatud. Andmekaitseõigus tähendab aga, nagu ka eelpool juba sai mainitud, isiku informatsioonilise enesemääramise õigust. Vastupidiselt privaatsuse mõistele on andmekaitse kontseptsioon Euroopa innovatsioon ja leiutis.[23]

Omavahel väga tihedalt seotud õigus privaatsusele ja õigus andmete kaitsele ei ole sünonüümid, kuigi neid selleks väga tihti peetakse. Andmekaitseõiguse kohaselt peavad inimesed omama kontrolli oma isikuandmetega toimuva üle. Eelnimetatu viitab esiteks

[19] A. Roosendaal. We Are All Connected to Facebook … by Facebook! – European Data Protection: In Good Health?. Dordrecht: Springer 2012, lk 14.
[20] C. Kuner. Privacy, Security and Transparency: Challenges for Data Protection Law in a New Europe. Hague: Kluwer Law International 2005, lk 45.
[21] B. R. Ruiz. Privacy in Telecommunications. A European and an American Approach. Hague: Kluwer Law International 2005, lk 45.
[22] M. Tzanou. Data Protection as a fundamental right next to privacy? 'Reconstructing' a not so new right. – International Data Privacy Law 2013, nr 3 (2), lk 88.
[23] C.Kuner (viide 20), lk 3.

sellele, et inimesed on vabad ja nende poolt teadlikult antud nõusolek on alus seaduslikule andmete töötlemisele. Teiseks on isikutel erinevaid õiguseid oma isikuandmete töötlemisel nagu näiteks muuhulgas õigus andmete parandamisele ja kustutamisele.[24] Probleem infoajastul seisneb aga selles, et isiku enesemääramise õigust kujundavad andmete töötlemise toimingud. See, mismoodi isikustatud andmeid töödeldakse, määrab tingimused, millele vastavalt isik osaleb sotsiaalses ja poliitilises elus. Siinjuures võib tuua järgmise näite: veebilehel hiireklikiga nõusoleku andmine oma teatud andmete töötlemiseks on mõnede vaatlejate arvates valik, mis sõltub isikust endast. Kuid siiski, teavitus ekraanil võib sisaldada standardsõnastust, mis lubab andmete edasist töötlemist ja edastamist. Eeltoodust tulenevalt võib tunduda, et isik omab kontrolli oma andmete avaldamise ja edastamise üle lihtsalt seetõttu, et ta ise on teostanud selleks kindla tegevuse hiirekliki näol. Kas isik aga tegelikult teab, kus ja kellele tema andmed avaldatakse või edastatakse? Reaalselt omab kontrolli aga see pool, kes nõudis hiirekliki tegemist ning kes soovitud sündmuse saabumiseks otsustas, millised tingimused täidetakse, kui hiirenupuga klikk teostatakse. Andmete avaldamise vabadus on seotud isiku autonoomiaga ja on privaatsuse aktiivseks elemendiks. See rõhutab andmete avaldamist, kui toimingut, mis sõltub isikust endast. Privaatsuse passiivne komponent seisneb õiguses olla üksi jäetud ja mitte olla jälgitud. Lisaks aktiivsetele ja passiivsetele elementidele eksisteerivad ka kontrollimehhanismid, milleks on *ex post* isiku õigus teada, muuta ja kustutada ning *ex ante* isiku teadlik nõusolek andmete töötlemiseks.[25] Õigust privaatsusele ja õigust oma andmete kaitsele kirjeldatakse kui mitteidentseid kaksikuid. Kuigi andmekaitse on privaatsusesse sügavalt sisse imbunud, siis ei pruugi andmekaitsest tõstatuda privaatsusküsimusi. Vastupidiselt privaatsuse reeglitele ei ole andmekaitse reeglid keelavad, vaid need reeglid korraldavad ja kontrollivad, mil viisil isikuandmeid töödeldakse.[26] Andmekaitse ulatus on palju kitsam kui privaatsusel, vaatamata sellele, et mõlema kontseptsiooni eesmärk on kaitsta osaliselt isikute teisi õiguseid ja väärtusi.[27] Andmekaitse langeb privaatsuse selle aspekti alla, mida tuntakse õigusena kontrollida oma andmeid. See, mida privaatsus kaitseb, on aga taandumatu isikuandmete kaitsele, sest privaatsuse kontseptsioon hõlmab rohkem õiguseid ja väärtuseid.[28] Eelnimetatu tähendab seda, et isiku õigus privaatsusele ei hõlma mitte kõiki andmeid, mis tuvastavad

[24] B.-J. Koops. The trouble with European data protection law. – International Data Privacy Law 2014, nr 4 (4), lk 251.
[25] A. Roosendaal (viide 19), lk 15.
[26] Euroopa Komisjon. EU study on the Legal analysis of a Single Market for the Informatsion Society. Privacy. The future of online privacy and data protection. Arvutivõrgus: http://ec.europa.eu/information_society/newsroom/cf/newsletter-item-detail.cfm?item_id=7022, 07.03.2015, lk 4.
[27] *Op.Cit.,* lk 4-5.
[28] M. Tzanou (viide 22), lk 90.

isikut või võimaldavad tuvastada identifitseeritavat isikut vastupidiselt andmekaitse hõlmatavale ulatusele.[29]

Saksamaa Konstitutsioonikohtu arvamuse kohaselt õigus informatsioonilisele enesemääramisele on üks demokraatia eksisteerimise tingimusi. Selleks, et isik saaks autonoomset elu elada peab ta olema teadlik, millist informatsiooni riik tema kohta omab ja kuidas seda infot kasutatakse. Vastasel juhul peab isik alati kartma tehes oma kohustuslikke tegevusi, et need pälvivad riigi tähelepanu ja riik kasutab oma teadmisi isiku kahjuks. Selleks, et indiviidid saaksid vabalt ühiskonnas osaleda või kasutada oma põhiõiguseid, peavad nad omama autonoomia positsiooni, mis tähendab, et kui riik ei ole täiesti ignorantne selle suhtes, mida isikud ei taha, et riik teaks, siis peaksid vähemalt need teadmised olema piiratud. Selline autonoomsus ei ole tähtis ainult üksikisikule, vaid see puudutab ühiskonda tervikuna ja kogu demokraatlikku riigikorraldust, sest autonoomsus on ühiskondlikus elus osalemise ja põhiõiguste lihtsa kasutamise tingimuseks. Poliitilisest aspektist vaadatuna peab demokraatlik riigikorraldus tagama võimaluse üksikisikule osaleda poliitiliste otsustuste tegemise protsessis. Vaba avalik diskussioon ja demokraatlik riik on teineteisest vastastikuses sõltuvuses: demokraatia tagab avaliku diskussiooni samal ajal, kui demokraatia on õigustatud ainult senikaua kuni ta loob tingimused vabaks avalikuks diskussiooniks. See tähendab, et demokraatlik riik peab tagama vaba osalemise avalikus debatis ja põhiõiguste vaba kasutamise riigi enda eksisteerimise eesmärgil. Selle vaatenurga järgi ei ole õigus eraelu kaitsele puhtalt enam üksikisiku huvi, vaid väga olulise tähtsusega poliitiline huvi.[30]

Isiku eraelu puutumatus on küll peamine väärtus, mida andmekaitsereeglid tagama peavad, kuid andmekaitse seadused arenevad eesmärgiga, et tagada ka muid privaatsusega seotud huvisid nagu infosüsteemide turvalisus ja nendes sisalduvate andmete kvaliteet, mis tänapäeva tehnoloogia maailmas omavad olulist tähtsust isiku andmete kaitsmisel. Isikuandmete töötlemisel eksisteerivad andmete turvalisuse ja andmete kvaliteedi põhimõtete kõrval veel printsiibid, mis hõlmavad väärtusi läbipaistvusest, ettenähtavusest ja individuaalsest osalemisest isikuandmete töötlemisel. Kõigi eelnimetatud väärtuste kaitseks jääb alati õigus pöörduda oma õiguste kaitseks järelevalveasutuse poole.[31]

[29] J. Kokott, C. Sobotta. The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR. – International Data Privacy Law 2013, nr 3 (4), lk 225.
[30] B. R. Ruiz (viide 2121), lk 52-53.
[31] M. Tzanou (viide 22), lk 91.

Magistritöö autori hinnangul on privaatsus ja informatsiooniline enesemääramine traditsioonilised väärtused, mida isikuandmete kaitset tagavad seadused reguleerivad. Viimasel ajal on aga rohkem hakatud andmekaitse kontekstis tähelepanu pöörama ka mittediskrimineerimise põhimõttele, mis on omaette väärtuseks ja jääb muude hüvede kõrval andmekaitseseaduste kaitsealasse. Mittediskrimineerimine seostub delikaatsete isikuandmetega ja on keelatud Euroopa andmekaitseõiguse kontekstis, sest delikaatsete andmete töötlemine võib viia inimeste diskrimineerimiseni.[32]

Privaatsuse ja andmekaitse kontseptsioonide ühiseid ja erinevaid tunnusjooni analüüsides seisneb andmekaitse esmane tähtsus magistritöö autori hinnangul üksikisiku kaitsmises ehk tema informatsioonilise enesemääramise õiguse tagamises, sest tänapäeva infoühiskonnas on IKT areng teinud suures osas võimatuks kontrollida, kes ja mida tema isikuandmetega teeb. Kuna isikuandmete töötlemisega sekkutakse isiku eraellu, mis võib riivata isiku põhiõigust, siis seepärast tuleks andmetöötlust piirata ning ära määratleda andmetöötlusesse mittesekkumise ja sekkumise piiramise vajaduse põhimõtted.[33] Magistritöö autori hinnangul seisneb andmekaitse teisene, kuid mitte vähetähtsam esimesest, tähtsus üksikisiku autonoomia tagamises riigi poolt, mis on osa demokraatlikust riigikorraldusest, võimaldades üksikisikul osaleda avalikus diskussioonis ja osaleda poliitiliste otsustuste protsessides, panustades selliselt kogu ühiskonna heaolusse ja arengusse. Andmekaitseõigus on kui uus „vana“ õigus, mis on tinginud teistsuguse, ebatraditsioonilisema lähenemisviisi eraelu puutumatusele kui see siiani on olnud.[34]

Andmekaitseõiguse normatiivne areng on Euroopas otseselt seotud info- ja kommunikatsioonitehnoloogilise arenguga,[35] mis sai alguse 1970. aastal, kui Hesseni liidumaal Saksamaal võeti vastu maailma esimene siseriiklik andmekaitsealane õigusakt. Rootsi võttis vastu oma esimese andmekaitse seaduse 1973. aastal. See, et andmekaitseõiguse areng sai alguse just Saksamaalt ja Rootsist, ei pruugi olla üldse kokkusattumus, vaid illustreerib hoopis süsteemi positiivset ja negatiivset aspekti. Saksamaa puhul oli tegemist andmete väärkasutamisega, lääne pool totalitaarse valitsuse ja ida pool kommunistliku režiimi poolt. Seadusel nähti peamiselt kaitsvat rolli, kui määrati piire avaliku ja erasektori võimekusele isiklikke andmeid töödelda. Olukord Rootsis oli hoopis teistsugune, sest seal

[32] *Op.Cit.,* lk 91-92.
[33] E. Tikk, A. Nõmper. Informatsioon ja õigus. Tallinn: Juura 2007, lk 36-38.
[34] M. Tzanou (viide 22), 91.
[35] A. Kiss, G. L. Szoke. Evolution or Revolution? Steps Forward to a New Generation of Data Protection Regulation. – Reforming European Data Protection Law. Dordrecht: Springer 2015, lk 311.

puudus totalitaarne taust, vaid eksisteeris kahe sajandi tagune informatsioonivabaduse traditsioon, mille järgi iga infokild, mis oli avaliku sektori valduses, loeti avalikkuse omandiks ning oli kättesaadav igaühele. Kuna isikutel oli vaba juurdepääs informatsioonile, mis oli talletatud ükskõik millises arvutis, siis andmekaitses nähti infovabaduse kontseptsiooni, mis ulatus ka juba erasektorisse. Suurbritannia ajaloos ei ole ei türannia ega ka sellist infovabaduse kogemust tugevalt esile tõstetud ja tõenäoliselt ei ole ka üllatus, et andmekaitse võib vahetevahel näida perifeerne, juurteta õigusharu.[36]

Kuigi esimesed andmekaitse seadused kehtestati rahvuslikul tasandil, siis juba eelnevalt oli tekkinud tungiv vajadus tegutseda ka rahvusvahelisel tasandil, mis oli tingitud informatsiooni elektroonilisest edastamisest telegraafi kaudu. Valitsused olid rahvusvaheliste sidevõrkudega ühinemise vastu eelkõige seetõttu, et kardeti informatsiooni mittekättesaamist. Telegraafi kaudu jõuab info teise pooleni hetkeliselt ja eksisteerib võimalus, et info ei jõua adressaadini, mis oli välistatud sõnumite saatmisel vanemate postisüsteemidega. Andmekaitse kontekstis nõudsid rahvusvahelist tegutsemist kaks, võib-olla üksteisele vasturääkivat, teemat. Esiteks kardeti, et rahvuslikud seadused, mis sätestasid tugeva kontrolli andmete ekspordi üle, omavad kaitseefekti. Teiseks tundsid aga andmekaitsealased regulatsioonid kehtestanud riigid hirmu, et organisatsioonid, kes edastavad andmeid töötlemiseks sihtkohtadesse, kus on kehtestatud vähene kontroll andmete töötlemisele, vaatavad seadustest mööda. 1960ndate lõpust alates on rahvusvahelised organisatsioonid aktiivselt tegelenud andmekaitse valdkonna arendamisega.[37]

1.2. Traditsiooniline õigusraamistik

Euroopa Liidu Põhiõiguste Ameti arvates vajavad kodanikud tõhusat ja kättesaadavat kaitset andmekaitse seaduste rikkumiste eest, sest kõikjal Euroopa Liidus on inimestest saanud andmekaitse rikkumiste ohvrid. Andmekaitse rikkumised Euroopa Liidus on aga tingitud IKT laialdasest kasutamisest nii riigiasutustes kui ka eraettevõtetes. Euroopa Komisjoni asepresidendi Viviane Reding'i sõnul tuleb tagada andmekaitse kui põhiõiguse kaitse ja selle õiguse kättesaadavus inimestele. Kui tõhusaks osutub aga õigusnormide ja õiguste

[36] I. J. Lloyd. Information Technology Law. 6th edition. New York: Oxford University Press: 2011, lk 22.
[37] *Op.cit*., lk 23.

rakendamine, siis see sõltub sellest, kas normide ja õiguste jõustamiseks on olemas asjakohased mehhanismid.[38]

Alljärgnevalt magistritöö autor analüüsib isikuandmete kaitset reguleerivaid instrumente info- ja kommunikatsioonitehnoloogilisest aspektist lähtuvalt, millest tulenevalt magistritöö autor otsib vastust eelkõige küsimusele, kas kehtivad õigusaktid kaitsevad piisavalt ja tõhusalt isiku õigust oma andmete kaitsele tänapäeva infoühiskonnast tulenevate õigusrikkumiste eest.

1.2.1. Rahvusvaheline õigus

Rohkem kui 60 aastat tagasi algas maailma taastumine traumast, mille põhjustajaks oli teine maailmasõda. Teise maailmasõja metsikus pani eurooplasi nägema eraelu kaitse väärtust ja sellest globaalsest konfliktist väljatulemiseks sätestati õigus eraelu puutumatusele 1948. aastal ÜRO inimõiguste ülddeklaratsioonis[39] ja 1950. aastal Euroopa inimõiguste ja põhivabaduste kaitse konventsioonis (EIÕK)[40]. Eelnimetatud instrumentidest koos said suunanäitajad sel tervenemise teel, sest üksikisikute õiguste tugevdamises nähti parimat ravimit sellele globaalsest terrorist põhjustatud traumale.[41] Lisaks eelnimetatud instrumentidele andis Majanduskoostöö ja Arengu Organisatsioon (OECD) 23. septembril 1980. aastal välja juhendi eraelu kaitsest ja piiriülesest isikuandmete kaitsest (OECD juhend), mida täiendati 2013. aastal.[42] Euroopa Nõukogust ja OECD-st said esinumbrid andmekaitse valdkonna edasiarendamisel rahvusvahelisel tasandil.[43]

Magistritöö autor keskendub alljärgnevalt arvestatavamat õigusjõudu omavatele rahvusvahelistele instrumentidele, mis on jõustatud Euroopa Nõukogu poolt ja on liikmesriikidele õiguslikult siduvad võrreldes OECD ja ÜRO isikuandmete kaitset

[38] Euroopa Liidu Põhiõiguste Amet. Kodanikud vajavad tõhusat ja kättesaadavat kaitset andmekaitse seaduste rikkumise eest. Arvutivõrgus : http://fra.europa.eu/sites/default/files/fra_press_release_data_protection_remedies_report_et.pdf, 14.03.2015.
[39] Ühinenud Rahvaste Organisatsioon. Inimõiguste ülddeklaratsioon. Arvutivõrgus: http://www.un.org/en/documents/udhr/, 14.03.2015.
[40] Inimõiguste ja põhivabaduste kaitse konventsioon. - RT II 2010, 14, 54.
[41] I. J. Lloyd (viide 36), lk 19.
[42] OECD. The OECD privacy framework. Arvutivõrgus: http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf, 14.03.2015.
[43] I. J. Lloyd (viide 36), lk 19.

reguleerivate instrumentidega, sh 18. detsembri 2013. aasta veebiprivaatsuse resolutsioon[44], millel on pigem deklaratiivne ja soovituslik iseloom.[45]

1.2.1.1. Euroopa inimõiguste ja põhivabaduste kaitse konventsioon

1950. aastal võttis Euroopa Nõukogu vastu Euroopa inimõiguste ja põhiõiguste konventsiooni, mis jõustus 1953. aastal. EIÕK-i eesmärgiks on edendada Euroopa riikides ühiseid ja demokraatlikke printsiipe ning sätestada üldised reeglid põhiõiguste ja –vabaduste tagamiseks. Tänaseks hetkeks on kõik Euroopa Nõukogu liikmesriigid EIÕK-i ratifitseerinud ning seega võtnud endale kohustuse konventsiooni järgida. Konventsioonist tulenevate õiguste tagamiseks asutati 1959. aastal Strasbourgis Euroopa Inimõiguste Kohus (edaspidi EIK), kus käsitletakse üksikisikute, üksikisiku rühmade, vabaühenduste või juriidiliste isikute avaldusi konventsiooni väidetavate rikkumiste kohta.[46] Isikuandmete rikkumise kaitseks on isikule tagatud õiguskaitse kättesaadavus eraldiseisva õigusena artiklis 6 sätestatud õiglase kohtumenetluse õiguse raames[47] ning EIÕK-i artikkel 13 sätestab õiguse tõhusale õiguskaitsevahendile[48].

EIÕK on tehnoloogianeutraalne, mis magistritöö autori hinnangul tähendab, et EIÕK ei erista, kas isikute õiguste rikkumisel kasutatakse tehnoloogilisi lahendusi või muid võimalusi, vaid räägib põhiõiguste kaitsest abstraktselt. Isikuandmete kaitse õiguse tagamisel rakendatakse EIÕK-i artiklit 8, mis küll ei sätesta *expressis verbis* õigust isikuandmete kaitsele, vaid on tuletatav igaühe õigusest nõuda, et tema era- ja perekonnaelu, kodu puutumatust ja kirjavahetuse saladust austataks ning võimud võivad sekkuda selle õiguse kasutamisse ainult kooskõlas seadusega ja kui see on demokraatlikus ühiskonnas vajalik riigi julgeoleku, ühiskondliku turvalisuse või riigi majandusliku heaolu huvides, korratuse või kuriteo ärahoidmiseks, tervise või kõlbluse või kaasinimeste õiguste ja vabaduste kaitseks.[49] Euroopa Inimõiguste Kohus on asunud korduvalt seisukohale, et eraelu mõistet ammendavalt sisustada

[44] ÜRO peaassamblee inimõiguste komitee poolt heaks kiidetud Saksamaa ja Brasiilia algatatud veebiprivaatsuse resolutsioon, mille eesmärk on kaitsta isikuandmeid internetis. Resolutsiooni kohaselt võib valitsuste ja ettevõtete jälgimistegevus ning inimeste isikuandmete kogumine rikkuda inimõigusi.
[45] C. Kuner. The European Union and the Search for an International Data Protection Framework. – Groningen Journal of International Law 2014, nr 2 (1), lk 58.
[46] Euroopa Liidu Põhiõiguste Amet ja Euroopa Nõukogu. Euroopa andmekaitseõiguse käsiraamat. Luxembourg: Euroopa Liidu Väljaannete Talitus 2015, lk 14-15.
[47] EIÕK art 6.
[48] EIÕK art 13.
[49] L. A. Bygrave. Data Protection Pursuant to the Right to Privacy in Human Right Treaties.- International Journal of Law and Information Technology 1998, nr 6 (3), lk 255-259.

ei ole võimalik ega ka vajalik.[50] Euroopa Nõukogu Parlamentaarse Assamblee resolutsioonis nr 428 (1970) määratletakse eraelu kui õigust elada omaenda elu minimaalse sekkumisega. Eelnimetatule lisati veel resolutsiooniga nr 1165 (1998) õigus kontrollida enda kohta käivat informatsiooni.[51] Euroopa Inimõiguste Kohtu praktika järgi hõlmab eraelu lisaks isiku sisemisele sfäärile ka isiku õigust luua ja arendada suhteid teiste inimeste ja välismaailmaga[52] kui ka võimude poolt isiku kohta käiva informatsiooni kogumist ja talletamist.[53] Eraelu puutumatust ohustavad järelikult ka isikuandmete kogumine, säilitamine ja juurdepääsu võimaldamine kolmandatele isikutele.[54] Seega hõlmab eraelu puutumatus ka õigust isikuandmete kaitsele.

EIÕK-i artikkel 8 mitte ainult ei kohusta liikmesriiki hoiduma isikute eraellu sekkumast, vaid loob täiendava positiivse kohustuse liikmesriigile võtta tarvitusele meetmed, mis tõhusalt kaitseksid isikute eraelu, ka isikute omavahelistes suhetes.[55] Millised need meetmed olema peavad, ei ole täpsustatud. Seega tähtsust ei oma, millist laadi meetmetega tegemist on, peaasi et need oleksid tõhusad. Seega võib magistritöö autori arvates rakendada isikuandmete kaitseks ka info- ja kommunikatsioonitehnoloogilisi meetmeid.

Isikuandmete kaitsest EIÕK-i artikli 8 kaitsealas hakati rääkima 1984. aastal, kui kohtunik Pettiti jäi eriarvamusele otsuses *Malone v The United Kingdom*. Eriarvamuse kohaselt rikub avalik võim isiku õigust informatsioonilisele enesemääramisele, kui õigusliku aluseta teostatakse telekommunikatsioonivahendite mõõtmist.[56] EIÕK-i artikli 8 kaitsealasse jääb ka informatsiooni kogumine ja avaldamine isiku võimaluseta ebaõiget informatsiooni ümber lükata[57] ning isiku õigus nõuda juurdepääsu enda kohta kogutud andmetele.[58] Lisaks juhtis kohtunik Pettiti tähelepanu asjaolule, et IKT võimaldab koostada isikute profiile ja seda juba 1984. aastal.[59] Magistritöö autori arvates, vaatamata sellele, et EIÕK-i artikkel 8 ei sisalda

[50] EIKo 16.12.1992, 13710/88, *Niemietz v Saksamaa*, p 29 ; EIKo 06.05.2001, 44599/98, *Bensaid v* Ühendatud Kuningriigid, p 47.
[51] Euroopa Nõukogu Parlamentaarse Assamblee resolutsioon nr 1165 (1998) Right to privacy. - In view of the new communication technologies which make it possible to store and use personal data, the right to control one's own data should be added to this definition. Arvutivõrgus kättesaadav: http://assembly.coe.int/main.asp?Link=/documents/adoptedtext/ta98/eres1165.htm, 09.03.2015, p 5.
[52] EIKo 06.09.1978, 5029/71, *Klass jt v Saksamaa*, p 33-34; EIKo 25.09.2001, 44787/98, *P.G. and J.H. v* Ühendatud Kuningriigid, p 56.
[53] EIKo 04.05.2000, 28341/95, *Rotaru v* Rumeenia, p 43 .
[54] U.Lõhmus. PõhiS § 26/9.4. – E. J Truuväli jt (toim) Eesti Vabariigi põhiseadus. Komm vlj. 2. vlj. Tallinn: Juura 2012.
[55] B. Bygrave (viide 49), lk 258.
[56] EIKo 02.08.1984, 8691/79, *Malone v The United Kingdom,kohtunik Pettiti eriarvamus.*
[57] EIKo 26.03.1987, 9248/81, *Leander v Sweden,* § 59.
[58] EIKo 07.07.1989, 10454/83, *Gaskin v The United Kingdom,* § 41, §49.
[59] EIKo 02.08.1984, 8691/79, *Malone v The United Kingdom,kohtunik Pettiti eriarvamus.*

sõnaselgelt isikuandmete kaitse õigust, oli võimalik isikute õiguseid andmekaitse reeglite rikkumise korral kaitsta koheselt, kui selleks ühiskonnas vajadus tekkis.

Artiklit 8 sisustav kohtupraktika isikuandmete kaitse teemadel on äärmiselt lai. Euroopa Nõukogu ja Euroopa Inimõiguste Kohtu kavatsus on hoida EIÕK-i nn „elava instrumendina", mida tuleb kohaldada „tänase päeva" tingimustes. EIÕK-i sätete tõlgendamisel pöörab EIK arvestatavamat tähelepanu EIÕK-i eesmärgile, milleks on kaitsta inimõiguseid ja edendada demokraatliku ühiskonna ideaale ja väärtuseid. Arvestades ühiskonnas toimuvaid arenguid, tuleb EIK-il olla valmis EIÕK-ist välja lugema ka täiendavaid reegleid, tagamaks isikuandmete paremat kaitset seoses probleemidega, mis ei ole spetsiaalselt ära nimetatud või mille sätestamist ei ole võimalikuks peetud. Eelnimetatut tehakse ainult kooskõlas EIÕK-i eesmärkidega. Arvestades asjaolu, et paljude Euroopa Nõukogu liikmesriikide andmekaitseseadused põhinevad rahvusvaheliselt tunnustatud printsiipidel, mis peamiselt tulenevad konventsioonist nr 108, siis oodatakse EIK-ilt valmidust, et EIÕK-ist, eriti artiklist 8, loetakse välja nõue, mille kohaselt liikmesriigid austaksid elementaarseid andmekaitse garantiisid. Kuid EIK ja Euroopa Komisjon nõuavad, et EIÕK-i sätted oleksid autonoomse tähendusega teiste õigusinstrumentide sätetest. EIK on seisukohal, et konventsioonist nr 108 tulenevad andmekaitse põhigarantiid on EIÕK-i artikli 8 valdkondlik instrument automaatse andmetöötluse kontekstis, mida võib kasutada artikli 8 tõlgendamisel.[60] Seega on magistritöö autori hinnangul EIÕK kohaldatav ka tänapäeva ühiskonnas, kus kõik protsessid on digitaliseeritud.

Olgugi, et EIÕK on kõige olulisem instrument isikute põhiõiguste tagamisel rahvusvahelisel tasandil, ei saa magistritöö autor siiski jätta nimetamata rahvusvahelisi instrumente, mis omavad tähendusliku osa isikuandmete kaitse õiguse kujunemisel. Nimelt, EIÕK-ist on küll välja kasvanud arvestatav kohtupraktika andmekaitseõiguse valdkonnas, kuid kohtupraktikat on aidanud kujundada ka ÜRO kodaniku- ja poliitiliste õiguste rahvusvaheline pakt[61]. Eelnimetatud pakti artikkel 17 ei sõnasta õigust isikuandmete kaitsele sõnaselgelt, nii nagu ka EIÕK-i artikkel 8, siis pakti artikli 17 ümber arenema hakanud pretsedendiõigus andis selgelt mõista, et andmekaitse põhiprintsiibid on hõlmatud privaatsusõigusega rahvusvahelises õiguses. Artikliga 17 seonduv ÜRO inimõiguste komitee üldine kommentaar 16, mis puudutab andmekaitse oluliste printsiipide nagu näiteks muuhulgas andmete kogumise

[60] *Op.Cit.*, lk 256.
[61] Kodaniku- ja poliitiliste õiguste rahvusvaheline pakt. – RT II 1994, 10, 11.

minimaalsus ja andmete turvalisus seaduslikku jõustamist nii avalikus kui ka erasektoris, on selgelt inspireerinud tänaseid seadusandjaid nii rahvuslikul kui ka rahvusvahelisel tasandil.[62]

Eeltoodust tulenevalt on magistritöö autor arvamusel, et Euroopa Nõukogul ja EIK-il on õnnestunud oma kavatsus ellu viia ja hoida EIÕK-i instrumendina, mida on võimalik kohaldada igal ajal ja igasugustes tingimustes, sh ka tänapäeva infoühiskonnas. Magistritöö autori hinnangul on selle teinud võimalikuks EIÕK-i väga abstraktne sõnastus, mida on võimalik tõlgendada vastavalt asjaoludele ning samal ajal ka EIÕK-i eesmärke arvestades.

1.2.1.2. Euroopa Nõukogu 1981. aasta isikuandmete automatiseeritud töötlemisel isiku kaitse konventsioon

Euroopa Nõukogu 1981. aasta isikuandmete automatiseeritud töötlemisel isiku kaitse konventsiooni, mida tavapäraselt nimetatakse ka lihtsalt konventsioon nr 108 ja mille lõplik versioon avaldati 1980. aastal, avati allkirjastamiseks 1981. aastal. 28. jaanuariks 1982 olid konventsiooni nr 108 allkirjastanud seitse riiki.[63] Konventsiooni nr 108 allkirjastamisele eelnesid mitmed Euroopa Nõukogu ministrite soovitused,[64] millele omakorda eelnes veel Euroopa Nõukogu Parlamentaarse Assamblee soovitus nr 890 (1980), isikuandmete kaitse kohta, mille kohaselt paluti Euroopa Nõukogu Ministrite Komiteel täiendada EIÕK-i isikuandmete kaitse õiguse sätetega, sest osa riike oli juba selleks ajaks juba tunnustanud ning osadel oli plaanis tunnustada isikuandmete kaitse õigust privaatsusõigusest eraldiseisva põhiõigusena.[65]

Konventsiooni nr 108 eesmärgina on sätestatud tagada osalisriigi territooriumil igale isikule, olenemata tema kodakondsusest või alalisest elukohast, tema põhiõiguste ja -vabaduste austamine. Eriti oluline on isikuandmete automatiseeritud töötlemisel tagada isiku õigus säilitada privaatsus andmekaitse kontekstis.[66] Konventsioon nr 108 on õiguslik instrument, mis sisaldab isikuandmete töötlemise nn võtmenorme, mille põhjustena võib välja tuua

[62] L. A. Bygrave (viide 49), lk 252-253.
[63] Austria, Taani, Prantsusmaa, Saksamaa, Luxembourg, Šveits ja Türgi.
[64] Euroopa Nõukogu ministri soovitus 73 (22). Arvutivõrgus: https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=589402&SecMode=1&DocId=646994&Usage=2, 18.03.2015. Euroopa Nõukogu ministri soovitus 74 (29). Arvutivõrgus: https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=590512&SecMode=1&DocId=649498&Usage=2, 18.03.2015.
[65] G. G. Fuster. The Emergence of Personal data Protection as a Fundamental Right of the EU. Switzerland: Springer International Publishing 2014, lk 81-88.
[66] Konventsioon nr 108 art 1.

järgmised asjaolud: esiteks konventsioon nr 108 oli ja on veel praegugi andmekaitse valdkonnas ainus rahvusvaheline õiguslikult siduv dokument, teiseks paigutub andmekaitse üldisesse põhiõiguste ja –vabaduste kaitsealasse ning kolmandaks andmekaitseõigus seostub otseselt privaatsusõigusega EIÕK-i artikli 8 mõttes, olles samaväärne õigusega eraelu puutumatusele. Eelnimetatud kolmanda põhjuse aspektist lähtudes võib julgelt väita, toetades konventsiooni nr 108 eesmärki, et andmekaitse reeglid on jõustatud selleks, et säilitada midagi määramatut nagu seda on privaatsus.[67]

Konventsioon nr 108 näeb ette isikuandmete töötlemisega seotud tagatisena kasutada õiguskaitsevahendeid juhul kui üksikisiku taotlust oma andmete säilitamise, parandamise, edastamise või kustutamise kohta ei rahuldata. Õiguste piiranguid saab kohaldada juhul, kui selleks on olemas ülekaalukas avalik huvi, näiteks riigi julgeolek või –kaitse.[68]

2010. aastal võttis Euroopa Nõukogu vastu konventsiooni nr 108 soovituse nr (2010) 13[69], mis koostati täiendamaks andmete töötlemise põhimõtteid seoses profileerimistehnikate aina päevakajalisemaks muutumisega. Eelnimetatud dokument sarnaneb magistritöö autori hinnangul teiste andmekaitseseadustega, sätestades isikuandmete töötlemise üldised põhimõtted, kuid ainult selle erinevusega, et nimetab töötlemistoiminguna sõnaselgelt profileerimist.

Euroopa Nõukogu mõju andmekaitse valdkonnas on tõusnud seoses faktiga, et paljud Euroopa Liidu andmekaitse ametnikud võtavad osa Euroopa Nõukogu tööst ja, et konventsioon nr 108 loob miinimumi tasemel isikuandmete kaitse reeglid, millele Euroopa Liidu andmekaitseseadused peavad vähemalt vastama.[70] Konventsiooni nr 108 otsustati ajakohastada ning 2011. aastal kinnitati avaliku konsultatsiooni tulemuste põhjal selle protsessi kaks peamist eesmärki: eraelu puutumatuse kaitse tugevdamine digitaalajastul ja konventsiooni järelevalvemehhanismi täiendamine.[71]

[67] G. G. Fuster (viide 65), lk 88-89.
[68] Euroopa Liidu Põhiõiguste Amet ja Euroopa Nõukogu (viide 46), lk 16.
[69] Council of Europe. Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling. Arvutivõrgus: https://wcd.coe.int/ViewDoc.jsp?id=1710949, 18.03.2015.
[70] C. Kuner. European Data Protection Law. Corporate Compliance and Regulation. Second edition. Oxford: Oxford University Press 2012, lk 49.
[71] Euroopa Liidu Põhiõiguste Amet ja Euroopa Nõukogu (viide 46), lk 17.

1.2.2. Euroopa õigus

Euroopa endine andmekaitseinspektor Peter Hustinix on seisukohal, et IKT suurendab tohutult võimalusi peaaegu igas eluvaldkonnas, mis on tänapäeval infomajanduses ja ühiskonnas määrava tähtsusega ning tunnistab IKT-ga kaasnevat kasu ja on nõus, et Euroopa Liit peaks tegema kõik võimaliku IKT arengu ja laialdase kasutamise toetamiseks. Euroopa Liit on võtnud eesmärgiks püsida maailmas esirinnas kõrgetasemelise IKT valdkonnas, milleni plaanitakse jõuda Euroopa digitaalse arengukava[72] abil. P. Hustinix' i arvates peaksid sellise digitaalse keskkonna keskmes olema üksikisikud, kellel peaks olema võimalik toetuda IKT suutlikkusele tagada nendega seotud andmete turvalisus. Samuti peaks üksikisikul olema võimalik kontrollida temaga seotud teabe kasutamist ning olla seejuures kindel, et tema eraelu puutumatus ja andmekaitseõigus on austatud. Teadmine, et andmeid ei kuritarvitata, loob isikutes usaldust. Usaldus omakorda on vajalik selleks, et inimesed võtaksid omaks uued teenused.[73] Euroopa Komisjon tegi pärast isikuandmete kaitset käsitlevate Euroopa Liidu õigusaktide toimimise hindamist järelduse, et vajalik on tagada, et Euroopa Liidu kõigis poliitikavaldkondades kaitstakse alati põhiõigust isikuandmete kaitsele ja vajalik on luua tugevam isikuandmete kaitse raamistik, et tänapäeva tehnoloogia tingimustes tagada digitaalmajanduse areng ja tugevdada isikute võimalusi kontrollida oma isikuandmetega tehtavaid toiminguid.[74]

1.2.2.1. Euroopa Liidu põhiõiguste harta

Euroopa Ühenduste asutamislepingutes ei käsitletud mingilgi viisil inimõiguseid ega nende kaitset. Üksikisikute kaitsmiseks toodi Euroopa õiguse üldpõhimõtetesse põhiõigused siis, kui tekkis vajadus hakata õigust mõistma inimõiguste väidetava rikkumise asjades Euroopa Liidu õiguse kohaldamisalasse kuuluvates valdkondades. Tunnistades Euroopa poliitika võimalikku mõju inimõigustele ja püüdes lähendada kodanikke Euroopa Liidule, kuulutati 2000. aastal välja Euroopa Liidu põhiõiguste harta[75] (edaspidi harta), millega omistati isikuandmete kaitsele Euroopa Liidu õiguses sõnaselgelt põhiõiguse staatus.[76]

---

[72] Euroopa Komisjoni teatis Euroopa Parlamendile ja nõukogule. Euroopa digitaalne tegevuskava. KOM (2010) 245 (lõplik). Brüssel: 19.05.2010. Arvutivõrgus: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:ET:PDF, 09.03.2014, lk 20.
[73] Euroopa andmekaitseinspektor (viide 5), lk 1.
[74] Isikuandmete kaitse üldmääruse seletuskiri. Arvutivõrgus: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_et.pdf, 18.03.2015, lk 2.
[75] Euroopa Liidu põhiõiguste harta. - ELT C 83, 30.03.2010.
[76] Euroopa Liidu Põhiõiguste Amet ja Euroopa Nõukogu (viide 46), lk 21.

Algselt oli harta kõigest poliitiline dokument, kuni 1. detsembril 2009. aastal jõustus Lissaboni leping, millega harta muudeti liikmesriikidele õiguslikult siduvaks.[77] Teise innovatsioonina harta õigusliku siduvuse sätestamise kõrval võib nimetada Euroopa Liidu toimimise lepingu (edaspidi ELTL) artiklit 16, mille kohaselt on igaühel õigus oma andmete kaitsele, mis hõlmab Euroopa Liidu esmase õigusaktina Euroopa Liidu üldpädevust võtta vastu andmekaitsealaseid õigusakte.[78] Seega annab Lissaboni leping eraldi õigusliku aluse isikuandmete kaitse eeskirjade vastuvõtmiseks. Ka isikuandmete kaitse üldmäärus esitati ELTL-i artikli 16 alusel.[79] Tulenevalt harta artiklist 47 on igal isikul isikuandmete kaitse reeglite rikkumise korral õigus tõhusale õiguskaitsevahendile ja õiglasele kohtulikule arutamisele.[80]

Harta artikkel 8 tagab Euroopa Liidus igaühele õiguse oma andmete kaitsele. Harta kohaselt tuleb isikuandmeid töödelda asjakohaselt ja kindlaksmääratud eesmärkidel ning igaühel on õigus tutvuda tema kohta kogutud andmetega ja nõuda nende parandamist. Harta artiklis 8 sätestatud nõuete täitmist kontrollib sõltumatu järelevalveasutus.[81] Artikli 8 sõnastamisel on võetud aluseks erinevad rahvusvahelised õiguslikud instrumendid, olgugi, et need ei tunnusta isikuandmete kaitset eraldiseisva õigusena. Harta artikkel 8 on inspireeritud EIÕK-i artiklist 8 ja selle ümber arenenud kohtupraktikast. Harta sätestab üldised isikuandmete kaitse põhiõiguslikud printsiibid. Hartat kohaldatakse koos andmekaitsedirektiiviga, mis täiendab hartat detailsete sätetega, näiteks defineerib „isikuandmete“ mõiste. Isikuandmete kaitse kontseptsiooni, nii nagu teistegi põhiõiguste, tõlgendamisele tuleb läheneda pigem laiemalt kui kitsalt.[82] Põhiõigusekspertide poolt koostatud harta kommentaarides kinnitatakse, et artikkel 8 on kohaldatav manuaalse andmetöötluse kõrval ka automatiseeritud andmetöötlusele, arvestades suurenenud andmete kogumist eelkõige rahvusliku julgeoleku tagamise ja organiseeritud kuritegevuse ennetamise eesmärkidel.[83] Magistritöö autor on arvamusel, et kui hartat ja andmekaitsedirektiivi kohaldatakse koosmõjus, siis andmekaitsedirektiivi tehnoloogianeutraalsus ei omagi erilisemat rolli, sest harta on juba niikuinii kohaldatav tehnoloogilises kontekstis.

---

[77] *Op.Cit.*, lk 20-21.
[78] Euroopa Liidu Põhiõiguste Amet ja Euroopa Nõukogu (viide 46), lk 20.
[79] F. B. Romano. The Right to the Protection of Personal Data: A New Fundamental Right of the European Union. Rooma: 2013. Arvutivõrgus: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2330307, 22.03.2015, lk 6.
[80] Harta art 47.
[81] Euroopa Liidu põhiõiguste harta art 8.
[82] EU network of indipendent experts on fundamental rights. Commentary of the Charter of Fundamental Rights of the EU. Arvutivõrgus: http://ec.europa.eu/justice/fundamentalrights/.../networkcommentaryfinal_en.pdf, 22.03.2015, lk 90-93.
[83] *Op.Cit.*, lk 90.

Lissaboni reformi mõju isikuandmete kaitsele demonstreerivad kaks hiljutist Euroopa Kohtu otsust. Aprillis 2014 tehtud lahendiga *Digital Rights Ireland* kaasuses tunnistati kehtetutuks direktiiv 2006/24/EÜ, mille eesmärgi kohaselt säilitatakse isikute kohta üldkasutatavate sideteenuste tarbimisel saadud andmeid raskete kuritegude uurimiseks, avastamiseks ja kohtus menetlemiseks.[84] Tegemist on põhiõiguste riivega, mis nõuab proportsionaalsuse kontrolli, mille tulemusel otsustas kohus, et kuna direktiiv 2006/24/EÜ ei sätesta selgeid ja täpseid reegleid hartas sätestatud eraelu puutumatuse ja isikuandmete kaitse õiguste põhiõiguste riive ulatuse reguleerimiseks, siis toob see kaasa põhiõiguste väga ulatusliku ja raske riive. Kohus otsustas, et direktiiv 2006/24/EÜ on kehtetu, olenemata üllast eesmärgist kaasa aidata raske kuritegevuse vastasele võitlusele ja seeläbi avaliku julgeoleku tagamisele.[85] Kriitikat on tekitanud aga lahendi osa, mis sedastab, et sõltumatul järelevalveasutusel ei ole võimalik kontrollida andmekaitse ja andmeturbega seotud nõuete täitmist, sest direktiiv 2006/24/EÜ ei nõua andmete säilitamist Euroopa Liidu territooriumil.[86] Eelnimetatud järelduse kriitika seisneb selles, et lahendis ei ole edasi arendatud Euroopa järelvalveasutuste võimalusi kontrollida Euroopa Liidu andmete töötlemist väljaspool Euroopa Liidu territooriumi, arvestades, et liikmesriigi järelevalveasutuste jurisdiktsioon lõpeb liikmesriigi riigipiiriga.[87] Magistritöö autori arvates avaldab *Digital Rights Ireland* otsus olulist mõju liikmesriikide õigusele. Kohtuotsuse jõustumisega muutus direktiiv 2006/24/EÜ kehtetuks direktiivi jõustumise hetkest, kuid liikmesriigid on direktiivi 2006/24/EÜ oma õigusesse üle võtnud, mis tähendab, et liikmesriigid peavad tegema vajalikke õiguslikke samme, et tagada siseriikliku õiguse vastavus Euroopa Kohtu otsusele.

Euroopa Liidu andmekaitseõiguse kohaldamist väljaspool Euroopa Liidu piire illustreerib Euroopa Kohtu lahend maist 2014 suurkorporatsiooni *Google* kohta. Google' i kaasuses vajas vastamist küsimus, kas Euroopa õigus on kohaldatav, kui äriühing (antud juhul *Google Spain*) omab füüsilist tegevuskohta Euroopa Liidus, aga tema tegevused on seotud interneti otsingumootoriga, mis on küll suunatud liikmesriigi elanikele, kuid isikute andmeid töödeldakse reaalselt emafirmas, mis asub väljaspool Euroopa Liidu territooriumi. Euroopa Kohus järeldas siinkohal, et andmekaitsedirektiivis sätestatud kohaldamisala tuleb tõlgendada laiendavalt. Lisaks leidis kohus veel, et õigus unustusele (*right to be forgotten*) ehk isiku

[84] C. Kuner (viide 45), lk 62.
[85] EKo 08.04.2014, C 293/12 ja C 594/12, *Digital Rights Ireland Ltd jt. v* Iirimaa, p 65.
[86] *Op.Cit.*, p 68.
[87] C. Kuner (viide 45), lk 63.

õigus oma andmete kustutamisele on kohaldatav ka internetikeskkonnas.[88] Siinkohal tekib magistritöö autoril küsimus, kas õigus unustusele internetis on võimalik? Ann Cavoukian ja Christopher Wolf on seisukohal, et ei eksisteeri *online* õigust olla unustatud. Kohus ei selgitanud oma otsuses, millal õiged andmed isiku kohta aeguvad selliselt, et need ei oleks enam internetist otsingumootori vahendusel leitavad. Kohus ei märkinud ära ka seda, kas lisaks keegi teine peale otsingumootorite peaks omama kohustust puhastada internetikeskkonda isikut ebasoodsas valguses näitavatest, kuid tõestest andmetest. Euroopa Kohus küll ütles, et õigus unustusele rakendub internetikeskkonnas, kuid ei andnud juhist, mismoodi peaks selle õiguse kohaldamine praktikas toimuma.[89]

Magistritöö autori hinnangul viitavad eeltoodud Euroopa Kohtu lahendid otseselt probleemile, mis puudutab Euroopa Liidu õiguse kohaldamise territoriaalseid piire, arvestades asjaolu, et internetis ei eksisteeri riigipiire. Euroopa õiguse territoriaalse kohaldamise küsimuse kõrval tõusetub küsimus veel kohtualluvuses. Lepingute puhul saab kohaldatavas õiguses ja kohtualluvuse kokku leppida, kuid mis saab siis, kui lepingut ei ole? Samad küsimused sedastati ka 20. märtsil 2015. aastal Eesti Juristide Liidu 26. aastapäeva konverentsil „Kaasaegne õigusloome ja õiguse arengusuunad. IT seadusandluse hetkeseis ja kitsaskohad“.

1.2.2.2. Euroopa Ühenduse direktiiv 95/46/EÜ üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta

Uute info- ja kommunikatsioonitehnoloogiate areng on tõstatanud küsimusi praegu kehtivate andmekaitsealaste õigusaktide ajakohasuse ja kohaldatavuse jätkusuutlikkuse kohta tänases infoühiskonnas ja seda eriti 1995. aasta Euroopa Ühenduse direktiivi 95/46/EÜ (andmekaitsedirektiiv) osas.[90] Andmekaitsedirektiiv on peamine Euroopa Liidu õigusinstrument, mis sätestab üldised reeglid isikuandmete kaitse tagamiseks. Andmekaitsedirektiivi koostamisel tugineti konventsioonis nr 108 sätestatud printsiipidele, mida täpsustati ja mille tähendust laiendati eesmärgiga tagada Euroopa Liidu kodanikele kõrgel tasemel isikuandmete kaitse ja andmete vaba liikumine.[91] Andmekaitsedirektiivi artikkel 1 kohustab liikmesriike isikuandmete töötlemisel kaitsma füüsiliste isikute põhiõigusi ja –vabadusi, eelkõige isikute õigust eraelu puutumatusele. Andmekaitsedirektiivi eesmärk on

[88] *Op.Cit.*, lk 63.
[89] A. Cavoukian, C. Wolf. Sorry, but there's no online 'right to be forgotten'. Arvutivõrgus: https://www.privacybydesign.ca/index.php/ann-cavoukian-christopher-wolf-sorry-theres-online-right-forgotten/, 03.04.2015.
[90] J. C. Buitelaar. Privacy: Back to the Roots. – German Law Journal 2012, nr 13 (3), lk 171.
[91] Euroopa Liidu Põhiõiguste Amet ja Euroopa Nõukogu (viide 46), lk 18.

viia isikuandmete töötlemisega seotud üksikisikute põhiõiguste ja –vabaduste kaitse kõigis liikmesriikides samale tasemele. Kuivõrd isikuandmete töötlemine on tegevus, mis võib üksikisikute õigusi ja vabadusi piirata, siis andmekaitsedirektiivi kohaselt ei või liikmesriigid erinevalt sisustada isikuandmete õiguspärase töötlemise juhtusid, tagamaks kooskõla andmekaitsedirektiivi eesmärgiga.[92]

Andmekaitsedirektiiv on olnud väga mõjuvõimas õigusinstrument. Esiteks on andmekaitsedirektiiv sätestanud standardi isikuandmete mõiste kui õigusmõiste sisustamiseks ning muutnud selgemaks andmekaitsereeglite kohaldamisala. Teiseks on andmekaitsedirektiiv määratlenud isikute õigused ja sätestanud nõuded seoses delikaatsete isikuandmete töötlemisega. Kolmanda olulise aspektina võib nimetada, et andmekaitsedirektiiv on loonud järelevalveasutused ja rahvusülesed koostöökogud nagu „artikli 29 alusel asutatud andmekaitse töörühm".[93] Kui andmekaitsedirektiiv, mis oma printsiibipõhise ülesehituse tõttu on väga paindlik, kehtestab üldised reeglid, siis andmekaitsedirektiiviga hõlmatud valdkondi täpsustab direktiiv 2002/58/EÜ (eraelu puutumatust ja elektroonilist sidet käsitlev direktiiv), mida omakorda muudab direktiiv 2006/24/EÜ (üldkasutatavate elektrooniliste sideteenuste pakkujate tegevusega kaasnevate või nende töödeldud andmete säilitamist käsitlev direktiiv). Eelnimetatud direktiiv tunnistati kehtetuks 8. aprillil 2014. aastal.[94] Andmekaitsedirektiiviga hõlmatud valdkondi täpsustavad direktiivid on vajalikud, sest andmekaitsedirektiiv on tehnoloogia-neutraalne. „Isikuandmete" ja „isikuandmete töötlemise" mõiste definitsioonid ongi väga üldised seetõttu, et andmekaitsedirektiivi oleks võimalik kohaldada erinevates tehnoloogilistes kontekstides.[95]

Andmekaitsedirektiiv paneb liikmesriikidele kohustuse, et kõikidel isikutel peab olema võimalus kasutada õiguskaitsevahendeid, kui on rikutud isiku õiguseid. Andmekaitsedirektiiv sätestab isiku õiguse saada kompensatsiooni ebaseadusliku isikuandmete töötlemise tagajärjel tekkinud kahju eest.[96] Kuna andmekaitsedirektiivis on arendatud konventsioonis nr 108 artiklis 11 ettenähtud võimalusi kasutada muid kaitsemeetmeid, siis rakendati sõltumatut järelevalvet, mis on tõhusalt kaasa aidanud andmekaitsereeglite järgimisele ja parandanud seega andmekaitseõiguse tulemuslikkust.[97]

[92] EKo 16.12.2008, C-524/06, *Heinz Huber v* Saksamaa, p 47, 50, 52.
[93] J. C. Buitelaar (viide 90), lk 175.
[94] Euroopa Liidu Põhiõiguste Amet ja Euroopa Nõukogu (viide 46), lk19-20.
[95] J. C. Buitelaar (viide 90), lk 175.
[96] 95/46/EÜ art 22-23.
[97] Euroopa Liidu Põhiõiguste Amet ja Euroopa Nõukogu (viide 46), lk18.

Euroopa Kohus on märkinud, et andmekaitsedirektiivi sätteid, mis puudutavad isikuandmete töötlemist, mis võib riivata põhiõiguseid, eriti isiku õigust eraelu puutumatusele, tuleb ilmtingimata tõlgendada põhiõiguste valguses.[98] Euroopa Kohtu jaoks on andmekaitsedirektiivi mõte tagada ühtsel tasemel üksikisiku õigus isikuandmete kaitsele kõikides liikmesriikides. Rahvuslikul tasandil kehtestatud õigusaktid ei tohi kaasa tuua isikuandmete kaitse vähenemist võrreldes andmekaitsedirektiiviga, vaid peavad olema ühtlaselt kõrge tasemega terves Euroopa Liidus.[99] Seega siseriiklike õigusaktide ühtlustamine ei piirdu ainult minimaalse ühtlustamisega, vaid viib põhimõtteliselt täieliku ühtlustamiseni. Kõikide liikmesriikide kohtute ülesandeks on tagada Euroopa Liidu õiguse nõuetekohane rakendamine. Sellega kaasneb aga oht, et liikmesriikide kohtud tõlgendavad Euroopa Liidu õigust erinevalt. Seda ohtu aitab vältida eelotsusemenetlus, mis on Euroopa Liidu õiguse põhimehhanism eesmärgiga tagada Euroopa Liidu õiguse ühetaoline tõlgendamine ja kohaldamine. Siseriiklikud kohtud võivad Euroopa Kohtusse pöörduda eelotsusemenetluse raames, küsides Euroopa õiguse tõlgendamist läbi konkreetsete küsimuste. Kõige levinumad küsimused, mida eelotsusetaotlusega Euroopa Kohtult küsitakse, seonduvad isikuandmete avalikustamisega (sh korduv avalikustamine) ja edastamisega ning isikuandmete töötlemisest teavitamisega.[100] Magistritöö autori hinnangul on tegemist andmete töötlemise toimingutega, mis võivad kõige enam riivata isiku õigust eraelu puutumatusele.

Andmekaitsedirektiivi kohaldamisalast on välja jäetud andmete töötlemine, mis on seotud riigi julgeoleku ja turvalisuse tagamisega ning kriminaalmenetlusega. Siinkohal on kõige rohkem vaidlusi tekitanud lennureisijate andmete (*Passenger Name Record* või *PNR*) edastamine lennufirmade poolt Ameerika Ühendriikide võimudele. Ameerika Ühendriikide õigus, mis kohustas lennufirmasid *PNR* andmeid edastama, sattus Euroopa Liidu õigusega konflikti. Seetõttu sõlmisid Euroopa Komisjon ja USA kokkuleppe, mille kohaselt edastatakse algselt USA õiguses sätestatud edastatavate andmete kogusest andmeid väiksemas mahus ning USA rakendab *PNR* andmete kaitseks konkreetseid kaitse meetmeid. Euroopa Kohus kuulutas eelnimetatud kokkuleppe kehtetuks, sest kokkuleppe eesmärgiks oli seatud terrorismi ja teiste ohtlike kuritegude ennetamine, mis ei lange andmekaitsedirektiivi rakendusalasse.[101] Euroopa Liidu regulatsiooni puudumise asemel loovad liikmesriigid rahvuslikud *PNR* süsteemid siseriikliku õiguse alusel. Euroopa Andmekaitseinspektor, artikli 29 alusel asutatud andmekaitse töörühm ja Euroopa Liidu Põhiõiguste Amet on sedastanud, et lennureisijate

[98] C. Kuner (viide 70), lk 19.
[99] Euroopa Liidu Põhiõiguste Amet ja Euroopa Nõukogu (viide 46), lk 18.
[100] E. Rohtmets. Riigikohtu analüüs isikuandmete kaitse kohta Euroopa Kohtu eelotsustes. Tartu: 2013, lk 7-8.
[101] C. Kuner (viide 45), lk 22.

andmed on isikuandmed ning nende töötlemine mõjutab isiku põhiõiguseid, mis tulenevad Euroopa Liidu põhiõiguste hartast, sh õigust isikuandmete kaitsele, õigust eraelu puutumatusele, õigust ettevõtlusvabadusele ja õigust mittediskrimineerimisele. *PNR* andmete töötlemine peab tagama isikule eelnimetatud õigused, mille piiramine on lubatud ainult seaduse alusel ning olema proportsionaalne.[102] Ka Eesti on rakendamas oma *PNR* andmete süsteemi nimega „Broneeringuandmete infosüsteem". *PNR* andmete töötlemine aitab kaasa Eesti riigi siseturvalisuse tagamisele, võimaldades sisejulgeolekut tagavatel asutustel täita paremini nendele seadusega pandud ülesandeid riiki saabuvate või riigist lahkuvate reisijatega kaasnevate riskide ennetamiseks ning piiriületuse efektiivseks korraldamiseks. Teiseks on broneeringuinfo vajalik, et terroriakte ja raskeid kuritegusid tõhusalt ennetada, avastada, uurida ja nende eest vastutusele võtta. Broneeringuinfot on võimalik võrrelda ka tagaotsitavate isikute ja esemete andmeid sisaldavate andmebaasidega, koguda tõendeid ning vajaduse korral tuvastada kurjategijate kaasosalisi ja paljastada kuritegelikke võrgustikke.[103]

Teatises „Terviklik lähenemisviis isikuandmete kaitsele Euroopa Liidus"[104] märkis Euroopa Komisjon kokkuvõtvalt, et Euroopa Liit vajab ulatuslikku ja terviklikku lähenemisviisi, millega oleks tagatud isiku andmekaitseõiguse kui põhiõiguse austamine. Praegune raamistik on jätkuvalt asjakohane eesmärkide ja põhimõtete seisukohast, kuid paraku ei ole see takistanud Euroopa Liidus isikuandmete kaitse rakendamisviisi killustumist, õiguslikku ebakindlust ning üldsuse levinud arusaama, et eelkõige internetis tegutsemisega on seotud olulised ohud. Seetõttu on Euroopa Komisjon seisukohal, et on aeg luua Euroopa Liidus tugevam ja sidusam raamistik isikuandmete kaitsele. 25. jaanuaril 2012. aastal avaldaski Euroopa Komisjon isikuandmete kaitse üldmääruse eelnõu (üldmäärus), mis vastuvõtmise korral asendab praegu kehtiva andmekaitsedirektiivi, kuigi EIK sedastas juba aastatel 1998[105] ja 2000[106], et isikuandmete töötlemiseks IKT abil on vaja selgeid ja detailseid reegleid, arvestades tehnoloogia keerulist iseloomu.

---

[102] Euroopa Liidu Põhiõiguste Amet. Twelve operational fundamental rights considerations for law enforcement with processing PNR data. Arvutivõrgus: http://fra.europa.eu/sites/default/files/fra-2014-fundamental-rights-considerations-pnr-data-en.pdf, 21.03.2015, lk 1.

[103] Riigipiiri seaduse, tolliseaduse ning politsei ja piirivalveseaduse muutmise seaduse eelnõu seletuskiri. Arvutivõrgus: http://www.riigikogu.ee/?op=emsplain&page=pub_file&file_id=ba652ab6-5f14-461c-8724-effb4e6e5e8d&, 22.03.2015, lk 1-2.

[104] Euroopa Komisjoni teatis Euroopa Parlamendile ja nõukogule. Terviklik lähenemisviis isikuandmete kaitsele Euroopa Liidus. KOM (2010) 609 (lõplik). Brüssel: 4.11.2010. Arvutivõrgus: http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0009:FIN:ET:DOC, 09.03.2014.

[105] EIK 25.03.1998, 13/1997/797/1000, *Kopp v* Šveits, p 72.

[106] EIKo 16.02.2000, 27798/95 *Amann v* Šveits, p 56.

1.2.3. Eesti õigus

Eestis on isikuandmete kaitse õiguse ajalugu teiste riikidega võrreldes lühike. Eestis on isikuandmete kaitset reguleerivaks üldaktiks isikuandmete kaitse seadus (IKS)[107], kuid lisaks on isikuandmete kaitse reegleid sisse kirjutatud ka erinevatesse eriseadustesse, mille üheks näiteks on elektroonilise side seadus (ESS)[108]. ESS-iga on üle võetud direktiiv 2006/24/EÜ. Andmekogudega seonduvat reguleerib avaliku teabe seadus (AvTS)[109]. OECD, Euroopa Nõukogu ja Euroopa Liidu liikmena on Eestile isikuandmete kaitse valdkonna reguleerimisel siduvad ka eelnimetatud institutsioonide instrumendid. Eestis ei ole isikuandmete kaitset tunnustatud eraldiseisva põhiõigusena, vaid isikuandmete kaitse on tuletatav õigusest informatsioonilisele enesemääramisele ja õigusest eraelu puutumatusele, mida tagab Eesti Vabariigi põhiseadus (PS)[110].

1.2.3.1. Eesti Vabariigi põhiseadus

Kui paljud riigid on isiku õigust oma andmete kaitsele tunnustanud privaatsusõigusest eraldiseisva õigusena ja toonud selle eraldi välja ka oma põhiseadustes, siis Eesti ei ole seda teinud. Eestis on isikuandmete kaitse õigus hõlmatud isiku informatsioonilise enesemääramise õigusega, mis paigutub PS-i § 19 kaitsealasse. Põhiseaduse § 19 sätestab igaühe õiguse vabale eneseteostusele, mis hõlmab ka isiku informatsioonilise privaatsusõiguse, mille kohaselt on tegemist igaühe õigusega ise otsustada, kas ja kui palju tema kohta andmeid kogutakse ja salvestatakse.[111] Põhiseaduse § 19 näol on tegemist üldise vabaduspõhiõigusega, mis kaitseb isikut enesemääramisõiguse tagamisega.[112]

Robert Alexy hinnangul on informatsiooniline enesemääramise õigus moodsa andmetöötluse tingimustes eriti tähtis, sest isegi suhteliselt tähtsusetud andmed võivad elektroonilise andmetöötluse abil väga kergesti ja palju isiku kohta tema eraelulist infot paljastada. Õigus informatsioonilisele enesemääramisele kui üldise isiksusõiguse osa ei ole piiramatult tagatud. Riik võib teha enda jaoks vajalikke andmete kogumisi, kui need on proportsionaalsed. Teisalt

[107] Isikuandmete kaitse seadus. - RT I 2007, 24, 127… RT I, 30.12.2010, 11.
[108] Elektroonilise side seadus. – RT I 2004, 87, 593 … RT I, 30.12.2014, 7.
[109] Avaliku teabe seadus. - RT I 2000, 92, 597 … RT I, 12.07.2014, 33.
[110] Eesti Vabariigi põhiseadus. - RT 1992, 26, 349 … RT I, 27.04.2011, 2.
[111] M. Ernits. PõhiS § 19/3.1.2.1 (viide 54).
[112] U. Lõhmus. PõhiS § 26/4 (viide 54).

peab aga isikut kaitsma nende ohtude eest, mille uued elektroonilised infotöötluse süsteemid isiksuse vaba eneseteostuse idee realiseerimisel endaga kaasa toovad.[113]

Lisaks sellele, et isikuandmete kaitse on hõlmatud informatsioonilise enesemääramisõigusega, on isikuandmete kaitse üheks oluliseks valdkonnaks ka eraelu kaitse. Eestis tagab igaühe õigust perekonna ja eraelu puutumatusele PS-i § 26. Riigikohtu halduskolleegium on märkinud, et „eraelu puutumatuse riivena käsitatakse muu hulgas isikuandmete kogumist, säilitamist, kasutamist ja avalikustamist"[114], mis kinnitab, et isikuandmete kaitse on osa õigusest eraelu kaitsele. Siinkohal ei tohi ära unustada, et EIK on pidanud EIÕK-i artiklis 8 sätestatud eraelu riiveks ka pelgalt juba seda, kui riigivõim andmeid kogub. EIK-i seisukohalt ei ole riive olemasolu jaatamiseks oluline see, mida nende andmetega hilisemalt tehti, kui üldse tehti.[115]

Kuna õigus isikuandmete kaitsele ei ole Eestis iseseisev põhiõigus, vaid kahest eraldiseisvast põhiõigusest tuletatav õigus, siis tekib siinkohal õigustatult küsimus, millal siis isikuandmete kaitse valdkonda puudutav küsimus langeb PS-i § 19 ja millal § 26 kaitsealasse. Eesti Vabariigi õiguskantsler leiab, et otsustus, kas isikuandmeid kaitsta PS § 26 või § 19 alusel, tuleb vajadusel teha konkreetse üksikjuhtumi asjaolusid silmas pidades. Ent isegi kui isikuandmete töötlemine ei lange PS § 26 kaitsealasse, tulenevad piirangud andmetöötlusele informatsioonilise enesemääramise õigusest PS § 19 alusel.[116] Eeltoodust järeldub, et isikuandmete kaitse reeglite rikkumise korral isik ei jää põhiõigusliku kaitseta, sest on nii või teisiti hõlmatud ka õigusega eraelu puutumatusele või õigusega informatsioonilisele enesemääramisele. Lisaks sätestab PS-i § 15 igaühe põhiõiguse pöörduda oma õiguste kaitseks kohtusse.[117] Õigust eraelu puutumatusele tagatakse eeskätt kriminaal-, haldus- ja tsiviilõiguslikus korras.[118]

Magistritöö autor teeb järelduse, et kuigi Eestis isikuandmete kaitse õiguse näol ei ole tegemist eraldiseisva põhiõigusega, siis muutuvas ajas on isikule tema andmete kaitse siiski tagatud põhiõigushüvena. Tulenevalt väljakujunenud praktikast ei ole praeguses Eesti

[113] R. Alexy. Põhiõigused Eesti Põhiseaduses. - Juridica 2001/eriväljaanne, p 6.1.2.2.
[114] RKHKo 3-3-1-3-12 p 19.
[115] EIK 25.03.1998, 13/1997/797/1000, *Kopp v* Šveits, p 53.
[116] Õiguskantsleri 05.03.2015 märgukiri nr 6-2/141070/1501002 Siseministeeriumile. Isikut tõendavate dokumentide andmekogu põhimääruse § 18 põhiseaduspärasus. Arvutivõrgus: http://oiguskantsler.ee/sites/default/files/field_document2/6iguskantsleri_margukiri_isikuandmete_sailitamise_tahtaeg.pdf, 13.03.2015.
[117] Eesti Vabariigi põhiseadus § 15.
[118] U. Lõhmus. PõhiS § 26/23 (viide 54).

õigusruumis vajadust kehtestada isiku õigust oma andmete kaitsele sõnaselgelt eraldiseisva põhiõigusena, sest isikuandmete kaitse on juba tagatud põhiõigushüvena. Lisaks on Riigikohus selgelt välja öelnud, et Euroopa õigusruumis üldtunnustatud põhiõigused kehtivad ka Eestis[119] ja õigus isikuandmete kaitsele on Euroopas põhiõigus.

1.2.3.2. Isikuandmete kaitse seadus

1996. aastal võeti Eestis vastu esimene isikuandmete kaitse seadus[120] ja see kehtis kuni 2007. aastani. Seoses Eesti Euroopa Liiduga liitumisega jõustus 2007. aastal uus isikuandmete kaitse seadus, mis harmoneeris Eesti õigusesse andmekaitsedirektiivi.

Praegu kehtiva IKS-i koostamisel võeti aluseks Euroopa andmekaitsedirektiiv ning Eesti isikuandmete kaitse raamistik on üles ehitatud andmekaitsedirektiivis sätestatud andmete töötlemise põhimõtetele.[121] Kuivõrd isikuandmete kaitse eesmärk on tagada eraelu puutumatus[122], siis sellest lähtuvalt on seatud ka IKS-i eesmärk kaitsta isikuandmete töötlemisel füüsilise isiku põhiõigusi ja -vabadusi, eelkõige õigust eraelu puutumatusele.[123] Seega tulenevalt IKS-i eesmärgist käsitletakse ka IKS-is isikuandmeid põhiõigushüvena.

Isikuandmete mõiste sisustamisel IKS-is on järgitud andmekaitsedirektiivi abstraktset eeskuju. IKS-i kohaselt on isikuandmed mistahes andmed tuvastatud või tuvastatava füüsilise isiku kohta, sõltumata sellest, millisel kujul või millises vormis need andmed on. Isiku tuvastatavuse hindamisel tuleb igal üksikjuhtumil arvesse võtta kõiki vahendeid, mida andmete töötleja võib isiku tuvastamiseks tõenäoliselt kasutada. IKS-i regulatsiooni laienemiseks ei ole oluline, kas isik on tuvastatav otse või kaudselt ehk üldiste tunnuste või omaduste põhjal või andmete kasutamise kontekstist tulenevalt. Seega ei pea IKS-is kehtestatud nõudeid rakendama anonüümsete andmete töötlemisel, kui isikut ei ole ka muul viisil võimalik tuvastada.

Isikuandmete töötlemine on tegevus, mis võib riivata isikute põhiõigust. Isikuandmete töötlemine IKS-i § 5 kohaselt hõlmab igasugused isikuandmetega tehtavad toimingud ning

[119] RKPJKo 3-4-1-5-94, RKPJKo 3-4-1-1-03 p 14; RKÜKo 3-4-1-6-12 p 131.
[120] Isikuandmete kaitse seadus. - RT I 1996, 48, 944 … RT I 1998, 59, 941.
[121] Isikuandmete kaitse seaduse seletuskiri. Arvutivõrgus: http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/IKS%20SELETUSKIRI%20(1).rtf., 10.03.2015, lk 1.
[122] T. Ilus. Isikuandmete kaitse olemus ja arengusuunad. – Juridica 2002, nr 7, lk 438.
[123] IKS § 1 lg 1.

nimetab ka avatud näidisloetelu andmetöötlustoimingutest. Andmetöötlustoimingute loetelus toodud toimingutest on IKS-is eraldi regulatsioon isikuandmete avalikustamise kohta, mis rõhutab, et isikuandmete avalikustamise näol on tegemist töötlemistoiminguga, mis võib isiku eraelu puutumatust ilmselt kõige ulatuslikumalt kahjustada. Avalikustamise kui töötlemistoimingu eraldi väljatoomine näeb andmesubjektidele ette senisest avaramad võimalused oma avalikustatud andmete ebasoovitava töötlemise kaitseks.[124] Avalikustamine IKS-i § 11 kohaselt hõlmab igasuguse andmete määratlemata isikute ringile kättesaadavaks tegemise, sõltumata kasutatud vahenditest ja viisidest.[125]

IKS ei kaitse isikut ainult esmakordse, vaid ka korduva isikuandmete avalikustamise eest. Riigikohus on öelnud järgmist: „Ainuüksi sellest, et andmed on isiku nõusolekul või seaduse alusel ilma tema nõusolekuta varem mingis vormis avalikustatud, ei saa järeldada, et täiendaval avalikustamisel ei pruugi andmesubjekti jaoks olla olulisi tagajärgi. Andmete esialgne ja korduv avalikustamine võivad toimuda väga erinevas vormis ja väga erineva intensiivsusega, sõltuvalt andmete edastaja isikust, infokanalist, kontekstist, auditooriumist jne. Näiteks kohtuistungil avaldatud andmete uus avaldamine trükiväljaandes avardab reeglina oluliselt teavitatavate isikute ringi.“.[126]

IKS-i üldine kohaldatavus ei olene isikuandmete töötlemise viisist. IKS kohaldub isikuandmete nii automatiseeritud kui ka manuaalsele töötlemisele. Arvestades tänapäevase IKT võimalusi ning elektroonilist töötlemist isikuandmete töötlemise praktikas, ei tagaks selline kitsendus isikute õiguste kaitset piisavalt. Seetõttu on nii andmekaitsedirektiivis kui ka IKS-is ettenähtavad isikuandmete kaitse nõuded põhjendatult oluliselt kõrgemad võrreldes konventsioonis nr 108 sätestatuga.[127] Eestis on eriliseks järelevalveorganiks Andmekaitse Inspektsioon, kes valvab isikuandmete töötlemise seaduslikkuse üle ning omab õigust teha andmete töötlejatele ettekirjutusi ja vajadusel algatada väärteomenetlusi. Isikandmete hulk, töötlemisviiside mitmekesisus ning isiku nõusolekuta töötlemisvõimaluste ulatus nõuab tõhusamat kontrolli isikuandmete töötlemise üle.[128] Magistritöö autori hinnangul toetavad eelnimetatud vajadust veel asjaolud, et andmed on piiriülese iseloomuga ning loodud järelevalveasutus on sellise ulatusliku kontrolli teostamiseks liiga väike ja arvestada tuleb ka

[124] Isikuandmete kaitse seaduse seletuskiri (viide 121), lk 6.
[125] IKS § 11.
[126] RKHKo 3-3-1-3-12 p 24.
[127] Isikuandmete kaitse seaduse seletuskiri (viide 121), lk 2.
[128] U. Lõhmus. PõhiS § 26/21.4 (viide 54).

asjaolu, et järelevalveasutuse jurisdiktsioon lõpeb riigipiiriga. Avaliku teabe seaduse kohaselt teostab andmekogude osas järelevalvet Riigi Infosüsteemi Amet.[129]

Magistritöö autor, töötades avaliku sektori infotehnoloogia asutuses, puutub igapäevaselt kokku erinevate isikuandmete kaitse alaste probleemidega, mis ilmnevad tavaliselt infosüsteemide toimimise tagamiseks vajalike tehniliste tööde teostamise käigus. Riigi infotehnoloogiaasutused üldjuhul tagavad infosüsteemide, milles andmeid töödeldakse, riist- ja tarkvara nõuetekohase ning tõrgeteta toimimise ehk käituvad volitatud andmetöötlejatena neile antud pädevuse piirides. Magistritöö autori arvates on kõige sagedasemaks probleemiks see, et tehnilise töö tegijad on oma valdkonna spetsialistid, kes sageli ei pruugi mõelda, et oma töö käigus omatakse kokkupuudet isikuandmetega sh delikaatsete isikuandmetega, mille töötlemise reeglid kehtestab seadus. Tehnilist tööd tegev isik ei mõtle oma tegevusi teostades õigusnormide peale, mis seab piirid andmete töötlemisele. Kuna infotehnoloogia on oma iseloomult väga keeruline, siis ei ole võimalik iga kord ette näha, milline tegevus võib põhjustada reaalset ohtu isikuandmete turvalisuse tagamisele. Näiteks andmetöötleja töötaja võib enesele teadmata tekitada isikuandmetele volitamata juurdepääsu, näiteks teisele sama asutuse töötajale või kolmandatele isikutele, kellel juurdepääsuõigus puudub. Isik, kelle andmetele volitamata juurdepääs tekitati, ei saa aga kunagi teada, et tema andmeid nägi keegi, kes ei oleks pidanud neid nägema. Ja kui isik ei tea, et tema õiguseid on rikutud, siis ei ole võimalik tal ka oma õiguste kaitset teostada. Andmetöötlejana on IKS-i väga keeruline kohaldada, sest see on väga üldine – puuduvad konkreetsed normid konkreetsete juhtumite kohta, kuid norme on vajalik jällegi konkreetsete asjaoludega seostada. Andmetöötlejale on jäänud väga suur kaalutlusõigus, mis võimaldab iga juhtumit eraldi analüüsida ja tõlgendada, kuna IKS ei anna konkreetseid juhtnööre tegutsemiseks. Andmekaitse Inspektsioon annab andmetöötlejale soovitusi ning andmetöötlejal on võimalik neid soovitusi seaduse rakendamisel kasutada. Andmekaitse Inspektsiooni soovitused ei ole andmetöötlejale õiguslikult siduvad, vaid on üksnes nendepoolne seaduse tõlgendus. Magistritöö autori hinnangul on IKS juristile hea proovikivi. Abstraktsed normid, mis võimaldavad laia tõlgendust, annavad võimaluse seisukohtade tõhusaks põhistamiseks.

[129] AvTS § 44 p 2.

2. Isikuandmete kaitse ning info- ja kommunikatsioonitehnoloogia

2.1. Info- ja kommunikatsioonitehnoloogiast tulenevad õiguslikud probleemid

Infoühiskonna arenedes on isikuandmete kogumise viisid muutunud väga keeruliseks ja neid ei ole kerge tuvastada. Majandustegevuses osalejad saavad keeruliste tehnoloogiliste vahendite abil jälgida üksikisikute käitumist ja kujundada selle alusel oma tegevust. Ka ametiasutused kasutavad e-valitsuse rakenduste abil isikuandmeid aina enam, näiteks nakkushaiguse puhangu korral üksikisiku jälgimiseks, terrorismi ja kuritegevuse ärahoidmise ja nende vastase võitluse tõhustamiseks, maksustamise eesmärgil jne.[130] Teenuste kasutamisest, sealhulgas internetis, saadav kasu on majandusarengu alus. Kasutajad peavad teenust usaldama. Usalduse puudumine tekitab isikutes kahtlusi interneti teel ostude sooritamisel ja uute teenuste, sealhulgas avalike e-valitsuse teenuste kasutuselevõtmisel. Kahtluste korral jätavad inimesed internetiostud pigem tegemata ja e-teenused kasutamata. Kui usalduse loomise probleem jääb tähelepanuta, siis on tulemuseks majanduse kasvu aeglustumine, mille tingib uute, innovaatiliste ja tarkade tehnoloogiliste lahenduste vähene kasutusele võtmine. Aeglustuv majanduskasv on aga tõkkeks avalikule sektorile, takistades võimalikku kasu saamist teenuste digitaliseerimisest.[131] Informatsiooniuputus, mis on infoühiskonna üheks tunnuseks, on ohuks isikute privaatsusele, sh isikuandmete kaitsele, mis on paljude rahvuste hulgas tunnistatud põhiõiguseks.[132] Isikuandmete kaitse põhiõigusena aga väärib *erga omnes* kaitset.[133]

Magistritöö autor nendib siinkohal, et infoajastul on tekkinud uute tehnoloogiate kasutamise tulemusel informatsiooni üleküllus, mistõttu on ka isikuandmete kaitse pälvinud suuremat tähelepanu. Uuema aja tehnoloogiatrendidest eristuvad asjade internet (*internet of things*), suurandmed (*big data*) ja pilvetehnoloogiad (*cloud computing*) on juba põhjalikult maailma muutnud ja veel muutmas ning tekitanud isikuandmete kaitse valdkonnas rohkesti uusi õiguslikke küsimusi. Tänapäeva globaliseerunud maailmas seisneb andmete innovatsioon nende töötlemise võimalustes[134], mida pakuvad erinevad tehnoloogiad. Magistritöö autor

---

[130] *Op.cit.*, lk 1.

[131] Euroopa Komisjon. Komisjoni talituste töödokument. Mõjuhinnangu kommenteeritud kokkuvõte. SEK (2012) 73 (lõplik). Brüssel: 25.01.2012. Arvutivõrgus: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=SEC:2012:0073:FIN:ET:PDF, 10.03.2014, lk 2.

[132] M. Cunningham. Next Generation Privacy: The Internet of Things, Data Exhaust, and Reforming Regulation by Risk of Harm. – Groningen Journal of International Law 2014, nr 2 (2), lk 120.

[133] P. De Filippi, L. Belli. Law of the Cloud v Law of the Land: Challenges and Opportunities for Innovation. – European Journal of Law and Technology 2012, nr 3 (2), lk2.

[134] Euroopa Ülemkogu järeldused, milles keskendutakse digitaalmajandusele, innovatsioonile ja teenustele ning rõhutatakse ühtse digitaalse turu välja kujundamise vajadust. EUCO 169/13. Brüssel: 25.10.2013. Arvutivõrgus:

analüüsib alljärgnevates alapunktides riske, mis kujutavad endast ohtu isikute andmekaitseõiguse tagamisele ning tulenevad populaarsematest privaatsustrendidest[135], milleks on asjade internet, suurandmed ja pilvandmetöötlus.

2.1.1. Asjade internet – uus generatsioon privaatsuses

Arvuti ja side ulatuvus kõikjale on tehnoloogiliste megatrendide tulemusel üheks aina jõudu koguvaks suunaks. Tänu jõudsale arengule sensorite, andmetöötluse ja traadita side vallas ühendatakse igapäevaselt internetiga üha enam füüsilise maailma esemeid nagu külmikud ja telerid jmt. Seetõttu ollakse arvamusel, et tulevikus on igal internetti ühendatud esemel oma IP-aadress. Kõikjale ulatuva ühenduse olulisim nähtus on asjade internet.[136] Asjade internet tähendab lihtsustatult seda, et inimest ümbritsevad esemed elustuvad, mis väljendub esemetevahelises kommunikatsioonis internetis. Kui ühendada esemeid mobiiltelefoniga või juhtmega andmesidevõrku, siis esemetevaheline suhtlus hakkab toimuma automaatselt inimese sekkumiseta. Asjade internetti illustreerib muuhulgas ka see, et raamatukogud märgistavad ja jälgivad iga kogus olevat raamatut ning õllekannudesse paigaldatud kallutussensorid edastavad infot tarbimishulkade kohta. Aastaks 2020 on prognoositud ülemaailmselt üle 200 biljoni internetiga suhtleva masina.[137]

Internetti ühendatud asjad ühest küljest võivad inimeste elu teha palju lihtsamaks, kuid teisest küljest võivad inimese kohta paljastada väga isiklikke detaile nende tegemiste kohta.[138] Asjade interneti rakendusi ja teenuseid pakutakse isikute kohta andmete kogumise ja hilisema kombineerimise kaudu, olenemata sellest, kas kasutaja andmeid kasutatakse kindlal spetsiifilisel eesmärgil või ainult isiku harjumuste kaardistamiseks ja analüüsimiseks. Eelnimetatud informatsiooni põhjal on isikud tuvastatud või tuvastatavad, mistõttu on tegemist isikustatud andmetega, mis kuuluvad isikuandmete kaitse alasse.[139] Ka 36. rahvusvahelisel isikuandmete kaitse konverentsil osalenud andmekaitse inspektorid tõdesid, et

---

http://www.riigikogu.ee/?op=emsplain&page=pub_file&file_id=5e49dedb-09a1-479b-acbf-09ef47bf0897&., 08.03.2014, lk 1.

[135] Ernst & Young Global Limited. Privacy trends 2014. Privacy protection in the age of technology. Arvutivõrgus: http://www.ey.com/Publication/vwLUAssets/EY_-_Privacy_trends_2014:_Privacy_protection_in_the_age_of_technology/$FILE/EY-Insights-on-GRC-Privacy-trends-2014.pdf, 05.02.2015, lk 4.

[136] Majandus- ja kommunikatsiooniministeerium (viide 181), lk 12.

[137] M. Cunningham (viide 132), lk 116.

[138] J. Kohnstamm. Mauritius Declaration on the Internet of Things. Arvutivõrgus: http://www.privacyconference2014.org/media/16421/Mauritius-Declaration.pdf, 04.03.2015, lk 1.

[139] Article 29 Data Protection Working Party. Opinion 8/2014 on the Recent Developments on the Internet of Things. WP223. Brussels: 16.09.2014. Arvutivõrgus: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf, 05.02.2014, lk 4.

internetti ühendatud seadmete sensorite kaudu saadavaid andmeid tuleb käsitleda isikuandmetena. Eelnimetatut toetab asjaolu, et kogutavate andmete põhjal on võimalik isikuid identifitseerida. Kogutavaid andmeid on palju ning need on piisavalt kvaliteetsed ja tundlikud, mis tähendab, et inimese kohta järelduste tegemise tõenäosus on suurem, kui see, et järeldusi ei tehta.[140] Eeltoodut arvestades tekib magistritöö autoril küsimus, kas asjade internetti ühendamisega ja sellisel teel inimeste kohta andmete kogumisega liiale ei minda. Kas on üldse nii suures koguses igasuguseid isikustatud andmeid vaja? Magistritöö autor on arvamusel, et tänasel päeval ületab eluliselt mittevajaliku andmete hulk koguseliselt eluliselt tähtsate andmete hulka. Andmed muudkui kogunevad, olenemata kehtivast minimaalsuse printsiibist. Vaatamata tehnoloogilistele võimalustele peab isikuandmete töötlemine jääma kindlatesse raamidesse, mille juures tuleb kindlasti vältida tarbetu isikulise informatsiooni kuhjumist. Eelnimetatut peavad tagama ka isikuandmete kaitse valdkonda reguleerivad õigusaktid.

Andmete töötlemine saab alguse andmete kogumise momendist, mis tähendab, et kõik kaitsemehhanismid isikute andmete kaitseks peavad olema rakendatud juba andmete töötlemise alguses. Parim võimalus andmete turvalise töötlemise tagamiseks asjade interneti puhul on IKT tootjatel rakendada privaatsuslõimet juba uute tehnoloogiate väljatöötamisel.[141] Magistritöö autor analüüsib privaatsuslõime võimalusi magistritöö käesoleva peatüki punkti 2.2 alapunktis 2.2.1. Arvestades asjaolu, et ühiskonna noorem generatsioon ja ka pealetulevad põlvkonnad ei kujuta elu ühenduses olemata ette, siis ei peaks isikuandmete kaitse olema ainult inimeste endi probleem. See on ühiskonna liikmete ühine kohustus, et säiliks usaldus ühendatud seadmete vastu. Usalduse tagamise vahendiks on aga läbipaistvus, mis asjade interneti kontekstis tähendab seda, et asjade interneti seadmete pakkujad peavad konkreetselt ära näitama, milliseid andmeid ja mis eesmärkidel kogutakse ja kui kaua neid andmeid säilitatakse. Informatsioon andmete töötlemise kohta peab olema isikule kättesaadav ja arusaadav juba asjade interneti seadme ostmisel. Tänasel päeval on ettevõtete privaatsuspoliitikad sõnastatud mittearusaadavalt ja selliste privaatsuspoliitikate põhjal antud nõusolekuid andmete töötlemiseks ei saa kindlasti lugeda nõusolekuks isikuandmete kaitse kontekstis.[142] Artikli 29 alusel asutatud andmekaitse töörühm on oma arvamuses samuti välja toonud eelnimetatud kvaliteetsuses nõusoleku ühena asjade internetist tuleneva riskina isikuandmete kaitses. Olukord, kus isik ei tea, et tema isikuandmeid töötlevad internetti

[140] J. Kohnstamm (viide 138), lk 1.
[141] *Op.Cit.,* lk 2.
[142] *Op.Cit.,* lk 2.

ühendatud objektid, annab aluse tõsiseks kahtluseks isikuandmete töötlemiseks antud nõusoleku kehtivuses.[143] Magistritöö autor on siinjuures samasugusel arvamusel, et eelnimetatud kontekstis on isiku poolt antud nõusolekul andmete töötlemiseks eluline tähtsus. Inimene peab aru saama mismoodi asjade interneti seadmed toimivad ehk milliseid andmeid need tema kohta koguvad ja millistel eesmärkidel kogutud isikuandmetega internetikeskkonnas toimetatakse.

Asjade internet paneb isikuandmete töötlemisel proovile ka rakendatavad turvameetmed. Tänapäeva IKT maailmas ei ole tavaline tulemüür enam tõhus vahend andmete turvalisuse tagamiseks. Üheks lahenduseks riskide maandamisel isikute jaoks on töödelda andmeid ainult seadmesiseselt (*local processing*) ja kui see ei ole võimalik, siis ettevõtted peavad tagama isikute andmete töötlemisel andmete krüpteerimise terve protsessi jooksul, et kaitsta andmeid volitamata töötlemise eest.[144] Asjade interneti seadmetelt ja platvormidelt oodatakse, et need võimaldaksid andmevahetust ja majutust teenuse pakkuja infrastruktuuris, mistõttu ei peaks asjade interneti turvameetmed kujutama endast ainult seadmete endi turvameetmeid, vaid ka turvameetmete rakendamist kommunikatsiooniühendustele, majutuse infrastruktuurile ning muudele andmesisenditele selles süsteemis.[145] Magistritöö autori hinnangul on IKT nii nagu iga teinegi tehnoloogia väga keeruline, mille tegelikku toimimist mõistavad ainult valdkonna spetsialistid. See, milliseid turvameetmeid andmete töötlemisel rakendatakse, ei ütle tavalise inimese jaoks midagi. Tavaline inimene saab oma õiguste rikkumisest teada üldjuhul siis, kui toimub tema andmete mitte õiguspärane avalikustamine. Asjade interneti puhul toimub andmete edastamine internetikeskkonda, mistõttu on andmete avalikuks tulemise oht reaalne.

Asjade internet on siin, et jääda ning selge on, et paneb ka õigusloome proovile isikuandmete kaitse valdkonnas. Asjade internet toob kokku väga suures koguses andmeid, mida ühiselt nimetatakse suurandmeteks ja mis ise eraldi on juba tohutuks väljakutseks seadusandjale isikute õiguste tagamisel, kuid asjade interneti seadmete poolt kogutud andmete tulemusena saadud suurandmestik muudab selle proovikivi keerulisemaks ja olulisemaks.[146]

[143] Article 29 Data Protection Working Party (viide 139), lk 7.
[144] J. Kohnstamm (viide 138), lk 2.
[145] Article 29 Data Protection Working Party (viide 139), lk 9.
[146] J. Kohnstamm (viide 138), lk 1.

2.1.2. Suurandmed ja profileerimine – uus proovikivi isikuandmete kaitses

Termin „suured andmed“ põhineb sotsiaaltehnoloogilisel arengul, mis sai alguse arvuti leiutamisega ning millest on viimaste aastakümnete jooksul välja kujunenud kiiresti kasvav dünaamiline jõud.[147] Suurandmed ei tähenda midagi muud, kui koguda võimalikult palju andmeid, eriti inimeste ja nende harjumuste kohta, ja leida uusi ning võimsamaid viise kogutud andmete analüüsimiseks.[148] Suurandmeteks võib nimetada andmemassi, mis tuleneb miljonist allikast (nt interneti otsingumootorite kaudu saadud informatsiooni andmelaod või *Wikipedia* andmebaas tema veebilehtedega seotud muudatustest), mida ei ole võimalik analüüsida tavapäraste tehnikatega, kasutades ainult ühte serverit või arvutit.[149] Suurandmed on küll vähemnähtav tehnoloogiline trend, kuid omab ometigi samasugust ühiskonda ümberkujundavat jõudu nagu internet. Kui internet vormis ümber inimkonna suhtlemisvõimalused, siis suurandmestik kujundab ümber viisid, kuidas ühiskond andmeid töötleb.[150] Suured andmed toovad kokku mitte ainult suures koguses, vaid ka väga erinevat tüüpi andmeid, mille käsitlemist koos ei ole mitte kunagi varem isegi kaalutud. Suur kogus andmeid nõuab üha suurenevat töötlemise kiirust.[151] Mida kiiremini aga andmeid töödeldakse, seda kiiremini need kogunevad. Sellise kasvava andmete massi mahutamiseks on vaja üha rohkem vaba ruumi. Kui kakskümmend aastat tagasi mõõdeti andmete mahtu megabaitides, siis täna seisavad suurandmed vastamisi terabaitide, petabaitide ja isegi eksabaitidega.[152] Sajandeid tagasi usuti, et Aleksandria raamatukogu mahutab terve inimkonna koguteadmised. Tänapäeval on maailmas aga nii palju informatsiooni, et igale elavale isikule saaks anda 320 korda nii palju infot, kui palju ajaloolaste poolt usuti olevat Aleksandria raamatukogu kogukollektsioonis, mille hinnanguline väärtus on 1200 eksabaiti. Kui kõik need andmed pakkida kokku ja salvestada CD-le, siis kokku tuleks viis kuhja CD-sid, mis kõik ulatuksid kuuni. Kui 2000. aastal moodustas digitaalselt salvestatud informatsioon veerandi kogu

[147] F. Bosco, N. Creemers, V. Ferraris, D. Guagnin, B.-J. Koops. Profiling Technologies and Fundamental Rights and Values: Regulatory Challenges and Perspectives from European Data Protection Authorities. – Reforming European Data Protection Law. Dordrecht: Springer 2015, lk 4.
[148] J. Reno. Big Data, Little Privacy. – CA Technology Exchange. Insights from CA Technologies. Ameerika Ühendriigid: 2012, nr 3 (2), lk 28-32.
[149] Privacy International, UK. Big Data. - An introduction to Data Protection. The European Digital Rights papers 2013, nr 6. Arvutivõrgus: https://edri.org/files/paper06_datap.pdf, 01.03.2015, lk 10.
[150] K. Cukier, V. Mayer-Schoenberger. The Rise of Big Data. How It's Changing the Way We Think About the World. – Foreign Affairs 2013, nr 92 (3), lk 28-29.
[151] K. Michael, K. W. Miller. Big Data: New Opprtunities and New Challenges. – IEEE Security & Privacy. IEEE Computer Society 2013, lk 22-24.
[152] M. Waschke. Introduction to the Big Data. - CA Technology Exchange. Insights from CA Technologies. Ameerika Ühendriigid: 2012 nr 3 (2), lk 1.

maailma salvestatud infost, siis 2013. aastal on veel vaid vähem kui 2% kogu maailma salvestatud infost on mitte digitaalne.[153]

Suurandmete töötlemine tekitab terve rea andmekaitselisi küsimusi, mis puudutavad salvestatavate andmete kogust, andmete turvalist käitlemist ja andmete säilitamise aega.[154] Mida rohkem andmeid kogutakse, seda raskem on eraldada kasulikku informatsiooni tarbetust informatsioonist, sest eksisteerivad andmehulgad ületavad igasugused inimmõistuse piirid. Seega on suurte andmehulkade töötlemiseks vaja kasutada spetsiifilist tehnoloogiat ehk andmekaevet. Profileerimine on spetsiifiline automatiseeritud andmekaeve meetod, mis on mõeldud suurte andmehulkade analüüsimiseks, eesmärgiga moodustada võimalikult sarnaste tunnuste kategooriaid, mida on võimalik kasutada muuhulgas üksikisikute, grupeeringute, ürituste profiilide loomiseks. Profileerimise käigus struktureeritakse andmeid selliselt, et andmetest oleksid leitavad mustrid ja tõenäosused. Loodavate profiilide pinnalt on võimalik teha prognoose, et näha ette võimalikke trende, käitumisi, protsesse ja arenguid tulevikus. Eesmärk on arendada strateegiaid selleks, et olevikus oleks võimalik saada hakkama tuleviku ebamäärasustega.[155]

Kui andmekaeve meetodid loovad ühiskonnale kasu mitmesuguste eeliste nagu näiteks varase pandeemiaohu avastamise, maksupettuste ennetamise näol, siis andmekaeve tehnoloogiate negatiivseks küljeks on oht isikute põhiõigustele nagu privaatsusõigus, andmekaitseõigus, mittediskrimineerimine ning Euroopa ühiskondade põhiväärtustele nagu demokraatia, õigusriik, autonoomia ja enesemääramisõigus. Hädavajadus eelnimetatud ohtudega tegeleda kasvab, mida enam ühiskonnad toetuvad andmetöötlustehnoloogiatele sotsiaalsete ja tehnoloogiliste protsesside juhtimisel.[156]

Suurte andmete analüüsimisel on peamiseks ülesandeks tagada üksikisiku eraelu puutumatus. Iga päev jätab inimene endast maha digitaalse jalajälje, mille kombineerimise tulemusena võib avastada isikute kohta unikaalseid aspekte, mis muidu jääksid märkamatuks. Näited hõlmavad keelekasutust logides, riietust erinevates kontekstides, külastatavaid kohti, üritustel osalemist jmt. Isegi see, kuidas inimesed oma kodus elektrit kasutavad, võib isikute kohta paljastada ootamatut infot. Väljaspool kodusid võivad inimesi *ad hoc* edukalt jälgida droonid, mis märgates ebatavalisi maakasutuse mustreid, edastavad andmed andmekeskustele

[153] K. Cukier, V. Mayer-Schoenberger (viide 150), lk 28.
[154] K. Michael, K. W. Miller (viide 151), lk 22.
[155] F. Bosco, N. Creemers, V. Ferraris, D. Guagnin, B.-J. Koops (viide 147), lk 4.
[156] *Op.Cit.,* lk 5.

eriolukordade puhul. Suurandmete analüüs põhineb aspektidel inimeste kodu, töö ja sotsiaalelu kohta ning oletusi tehes süveneb küsimusse: „Kes sa oled?“. Eelnimetatu omab metafüüsilist mõju – inimesed teadlikult muudavad oma käitumist internetis ja jälgitavates kohtades, et ise oma privaatsust kaitsta.[157] Suurandmete tehnoloogiaid kasutades on võimalik avalikest andmetest eraldada andmeid, mis võivad olla ootamatud või isegi kahjustavad.[158] Informatsiooni mitmekordistumise ja laiaulatuslikuma jagamise võimaluste tingimustes muutub andmete turvalisuse ja eraelu puutumatuse tagamine üha keerulisemaks ülesandeks. Kui informatsioon isikute tervise, asukoha, elektrikasutuse, *online* tegevuste kohta on avatud põhjalikuks uurimiseks, siis tõusetuvad küsimused profiili loomise, diskrimineerimise ja andmete üle kontrolli kaotamise kohta. Isegi kui organisatsioonid kasutavad töödeldava informatsiooni mitteisikustamiseks erinevaid vahendeid (anonümiseerimine, pseudonümiseerimine, krüpteerimine, võtmekodeerimine, andmete killustamine), siis privaatsusega seotud probleemid ei kao, sest ka anonümiseeritud andmeid on tihti võimalik taasidentifitseerida ja konkreetsete isikutega seostada. Andmete taasisikustamine kõigutab tugevalt privaatsuspoliitikamaastikku, õõnestades usku isikustatud informatsiooni anonümiseerimisse.[159] Anonümiseerimise üheks suureks eeliseks on, et see võimaldab teha uuringuid, mida tavaliselt privaatsusnõuete pärast ei ole võimalik läbi viia. Kasutades kõigi inimeste terviselugusid haigusmustrite leidmiseks on võimalik parandada tervishoiuteenuste valdkonda, kuid samas võib selle tegevusega omakorda riivata isikute privaatsust. Kuigi siiani väidetakse, et anonümiseerimine on võimalik ka üksikisikute privaatsust riivamata, siis on vastupidine juba teadlaste poolt ära tõestatud 1997. aastal, kui patsiendid reidentifitseeriti isikuliselt suurtest anonümiseeritud meditsiinilistest andmetest, mida iseloomustasid ainult isikute sünnikuupäevad ja elukoha sihtnumbrid. Efektiivne anonümiseerimine ei sõltu mitte ainult otseste identifikaatorite eemaldamisest, vaid oluline on siinjuures anonüümsushulk – üksikisikute arv, kellega andmed võivad seostuda. Probleemi ei lahenda ka pseudonümiseerimine, mis on isikut identifitseerida võimaldavate andmete asendamine näiteks unikaalse numbriga. Ka pseudonümiseeritud isikut on võimalik identifitseerida, olenemata sellest kui hästi on pseudonüüm krüpteeritud.[160]

[157] K. Michael, K. W. Miller (viide 147), lk 23.
[158] M. Waschke (viide 152), lk 2.
[159] O. Tene, J. Polonetsky. Privacy in the Age of Big Data: A Time for Big Decisions. – Stanford Law Review Online. 2012, nr 64(63). Arvutivõrgus: http://www.stanfordlawreview.org/sites/default/files/online/topics/64-SLRO-63_1.pdf, 15.03.2014, lk 65.
[160] Foundation for Information Policy Research , UK. Anonymisation. – An introduction to data protection. The European Digital Rights papers 2013, nr 06. Arvutivõrgus: https://edri.org/files/paper06_datap.pdf, 01.03.2015, lk 6-7.

Profileerimise juures on oluline ära mainida, et enamusel juhtudel isikud ei tea, et hakatakse profiile looma andmetest, mis on kogutud mitte profileerimise eemärgil, vaid muudel konkreetsetel eesmärkidel. Profileerimiseks isiku nõusoleku küsimine ei ole aga mõistlik, sest ei ole võimalik ette kujutada, kuidas ja millisteks toiminguteks tuleks nõusolekut küsida. Profiile on võimalik luua ka andmetest, mis ei kuulu isikule ja see muudaks nõusoleku küsimise tarbetuks. Kui andmeid töödeldakse seaduse alusel, näiteks kriminaalmenetluse läbiviimisel, siis tõusetub omakorda küsimus andmete töötlemise proportsionaalsuse kohta, sest profileerimise protseduur ei ole läbipaistev, mis tähendab, et isik ei saa oma andmete töötlemise vajalikkuse osas vastuväiteid esitada. Läbipaistvuse puudumine tähendab isiku jaoks omakorda, et piiratakse individuaalse osaluse põhimõtet. Praegusel hetkel kestavad diskussioonid eesmärgiga garanteerida tulevikus isikule õigus olla informeeritud profileerimisest ja selle tagajärgedest.[161]

Mida rohkem suurandmestikke tekib, seda enam suureneb ka tõenäosus identifitseerida anonümiseeritud andmetest üksikisikuid, kasutades informatsiooni teistest suurtest andmehulkadest. Kaasaja tehnoloogiate juures võib julgelt väita, et anonümiseerimise tehnika ei toimi enam, sest uutest pealetulevatest andmehulkadest on võimalik leida identifitseerijaid, mis võimaldavad üksikisikut tuvastada.[162] Profileerimine kujutab endast demokraatlikus ühiskonnas ohtu põhiõiguslikele väärtustele nagu õigusriik, kodanike ja valitsusevahelised suhted ning klientide ja ettevõtete vahelised suhted.[163] Magistritöö autor teeb siinkohal järelduse, et tänapäeva tehnoloogiaid kasutades ei ole isikul võimalik säilitada internetikeskkonnas anonüümsust ega omada täielikku kontrolli oma isikuandmete töötlemise üle, eelkõige seetõttu, et andmete töötlemine uute tehnikatega on muudetud läbipaistmatuks ja piiratud on isiku individuaalset osalust andmetöötluses.

Isikuandmete edastamine on Euroopa Liidu ja Ameerika Ühendriikide vaheliste suhete oluline ja vajalik osa kaubandussuhete lahutamatu osana uute kasvavate digitaalettevõtete jaoks, kes tegutsevad näiteks sotsiaalmeedia või pilvandmetöötluse vallas ja edastavad Euroopa Liidust Ameerika Ühendriikidesse suuri andmehulki. Isikuandmete edastamine moodustab samuti olulise osa Euroopa Liidu ja Ameerika Ühendriikide õiguskaitsealasest koostööst, aga ka

[161] V. Ferraris, F. Bosco, E. D'Angelo. The impact of profiling on fundamental rights. Arvutivõrgus: http://www.unicri.it/special_topics/citizen_profiling/PROFILINGproject_WS1_Fundamental_1110.pdf, 02.03.2015, lk 14.
[162] Foundation for Information Policy Research , UK (viide 160), lk 7.
[163] Foundation for Information Policy Research, UK. Profiling. – An introduction to data protection. The European Digital Rights papers 2013, nr 06. Arvutivõrgus: https://edri.org/files/paper06_datap.pdf, 01.03.2015, lk 17.

liikmesriikide ja USA vahelisest koostööst riikliku julgeoleku vallas. Elektroonilise side ja andmetöötlusteenuste, sh pilvandmetöötluse üha ulatuslikum kasutamine, on oluliselt suurendanud atlandiülese andmete edastamise ulatust ja tähtsust. Inimesed kasutavad iga päev üha rohkem elektroonilise side teenuseid. Isikuandmed on muutunud väga väärtuslikuks. 2011. aastal oli ELi kodanike andmete hinnanguline väärtus 315 miljardit eurot ning see võib kasvada 2020. aastaks peaaegu 1 triljoni võrra aastas. Suurte andmehulkade analüüsi turg kasvab maailmas 40% aastas. Pilvandmetöötlusega seotud tehnoloogiline areng paneb jälle rahvusvahelise andmeedastuse mõiste perspektiivi, sest piiriülestest andmevoogudest saab meie igapäevaelu osa. Isikuandmete töötlemise uute meetoditega seoses tekivad tähtsad küsimused nii uute vahendite kohta, millega eraettevõtted töötlevad ärilistel eesmärkidel suures mahus tarbijaandmeid kui ka luureteenistuste suurema suutlikkuse suhtes teostada andmevahetuse laiaulatuslikku jälgimist.[164]

2.1.3. Pilvetehnoloogiad – uus ja arenev paradigma

Pilvetehnoloogia näol ei ole iseenesest tegemist uue tehnoloogiaga, vaid suhteliselt uue viisiga teha kättesaadavaks arvutiteenuseid.[165] Pilvetehnoloogia teeb võimalikuks ligi pääseda arvutiressurssidele ja teenustele üle võrgu.[166] Pilvandmetöötlus tekkis tänu suurtele ettevõtetele nagu *Google*, *Amazon*, *Microsoft* ja *eBay*, kes ehitasid algselt iseenda tarbeks massiivseid andmekeskuseid koos väga kiire internetiühendusega, kuid hiljem märgati tulupotentsiaali ka andmete majutus- ja arvutiteenuste pakkumises teistele ettevõtetele. Andmekeskused võivad paikneda nii Euroopa Liidu riikides kui ka väljaspool Euroopa Liidu riike.[167] Pilvetehnoloogiate aina kasvava leviku tõttu on pilvandmetöötlus põhjendatult muutunud moesõnaks. Kui varasemad samalaadsed tehnoloogiad hääbusid suuremat populaarsust saavutamata, tingituna oma liiga varajasest ajastusest, siis pilvarvutus on hakanud levima just tänasel ajahetkel, mida iseloomustavad andmesidekiiruste suurenemine, protsessorivõimsuste ja mälumahtude odavnemine ning üldine usalduse kasv.[168] Pilvandmetöötlust kasutades salvestatakse, varundatakse või töödeldakse andmeid kaugarvutites ehk serverites, millele kasutaja pääseb ligi interneti kaudu spetsiaalse tarkvara

[164] Euroopa Komisjoni teatis Euroopa Parlamendile ja nõukogule. Usalduse taastamine EL-is Ameerika Ühendriikide vaheliste andmevoogude vastu. KOM (2013) 846 (lõplik). Brüssel: 27.11.2013 Arvutivõrgus: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2013:0846:FIN:ET:PDF, 09.03.2014, lk 2-3.
[165] Privacy International, UK. Cloud Computing. - An introduction to data protection. The European Digital Rights papers 2013, nr 06. Arvutivõrgus: https://edri.org/files/paper06_datap.pdf, 01.03.2015, lk 16.
[166] Majandus- ja kommunikatsiooniministeerium (viide 136), lk 13.
[167] Privacy International, UK (viide 165), lk 16.
[168] Tallinna Tehnikaülikool. Arenguanalüüs „IKT TTÜ tasemeõppes“. Arvutivõrgus: http://www.ttu.ee/IKT-uuring/, 18.02.2014, lk 13.

abil. Tarkvara kasutusliideseks on reeglina veebilehitseja. Lisaks andmete salvestamisele ning edasisele töötlemisele võimaldab pilvetehnoloogia kasutada ka pilves paiknevaid teenuseid nagu internetipõhised e-postiteenused ja suhtlusvõrgustikud. Samuti saab pilveteenusena kasutada tekstitöötluslahendusi, ajaplaneerijaid, kalendreid või dokumentide failihaldussüsteeme. Andmetöötlusvõimsuse tagavad andmekeskused, mis koosnevad sadadest serveritest ja andmesalvestussüsteemidest. Isikuandmete töötlemise seisukohalt on pilveteenuse kasutaja vastutav töötleja ja pilveteenuse osutaja volitatud töötleja. Pilveteenuse osutaja võib kaasata ka erinevaid lepingupartnereid, kes sellisel juhul tegutsevad volitatud töötleja rollis.[169] Kõikide eelnimetatud rollide puhul tuleb teha kindlaks nende konkreetsed kohustused vastavalt kehtivatele andmekaitsealastele õigusnormidele.[170] Magistritöö autori hinnangul tuleb arvestada ka asjaolu, et kuna pilvetehnoloogiate kasutamine ei ole määratud riigipiiriga ja andmeid on võimalik paigutada pilve, mis võib asuda ükskõik millise riigi territooriumil, siis lisaks turvalisuse küsimusele tekivad küsimused kohaldatava õiguse ja kohtualluvuse osas. Eelnimetatud probleemid nimetas ära ka Justiitsministeeriumi õiguspoliitika valdkonna asekantsler Kai Härmand Eesti Juristide Liidu 26. aastapäeva konverentsil.

Pilveandmetöötluse puhul võib võrreldes teiste tehnoloogiatega välja tuua erinevaid eeliseid, milleks on tasuta või minimaalse hinnaga suur salvestusmaht, ajast ja asukohast sõltumatu ning mugav juurdepääs ja kulude kokkuhoid. Pilvandmetöötluse kasutamine aitab kaasa innovatsiooni arengule uute ja odavate IKT lahenduste või teenuste teostamise kaudu.[171] Lõppkasutaja perspektiivist vaadatuna on pilvtehnoloogia kasutamise peamiseks eeliseks juurdepääs andmetele igal ajal ja igast asukohast internetiühenduse olemasolu korral. Tänu pilvetehnoloogiale on pilve ühendatud nutitelefon sama võimas kui personaalarvuti.[172] Pilvetehnoloogia eeliseid arvesse võttes tõmbab pilvandmetöötlus aina rohkem tähelepanu, tõotades pakkuda suuremat majanduslikku tõhusust, väiksemat keskkonnamõju, lihtsamat kasutamist ning suuremat kasutajasõbralikkust. Vaatamata pilvandmetöötluse poolt

[169] Andmekaitse Inspektsioon. Pilvandmetöötlus. Arvutivõrgus: https://www.aki.ee/et/pilvandmetootlus, 06.02.2015, lk 1.
[170] Artikli 29 alusel loodud andmekaitse töörühm. Arvamus 05/2012 pilvandmetöötluse kohta. WP196. Brüssel: 01.07.2012. Arvutivõrgus: http://ec.europa.eu/justice/dataprotection/article29/documentation/opinionrecommendation/files/2012/wp196_et.pdf#h2-2, 27.02.2014, lk 7.
[171] Andmekaitse Inspektsioon (viide 169), lk 1.
[172] P. De Filippi, L. Belli. Law of the Cloud v Law of the Land: Challenges and Opportunities for Innovation. – European Journal of Law and Technology 2012, Vol 3 No 2, lk2.

pakutavatele paljudele eelistele, esineb seoses pilvarvutusega endiselt ka ebakindlust ja seda eriti andmekaitsealastes küsimustes.[173]

Direktiivi 95/46/EÜ artikli 29 alusel loodud sõltumatu andmekaitse töörühm nimetab isikuandmete töötlemisel pilvandmetöötluse teenuste kasutamise puhul kaks peamist riski, milleks on kontrolli puudumine andmete üle ja ebapiisav teave töötlustoimingute kohta ehk läbipaistvuse puudumine. Olles sisestanud isikuandmed pilveteenuse pakkuja hallatavasse süsteemi, ei pruugi pilveteenuse kasutaja enam olla ainus, kes nende andmete üle kontrolli omab. Samuti ei pruugi pilveteenuse kasutajal olla võimalust juurutada tehnilisi ja korralduslikke meetmeid, et tagada andmete käideldavus, terviklus, konfidentsiaalsus, läbipaistvus, isoleeritus, sekkumisvõimaluste olemasolu ja porditavus.[174] Lisaks sellele, et pilveteenuse kasutajad kaotavad kontrolli tehnoloogilise infrastruktuuri, tarkvara rakenduste ja pilve talletatud andmete üle, ei suuda kasutajad enam kontrollida, kes eelnimetatud ressurssidele juurde pääsevad ja mis eesmärkidel neid kasutatakse. Omades kontrolli pilve arhitektuuri üle, omavad pilveteenuse pakkujad võimalust jälgida kasutajate tegevusi ja kommunikatsiooni ning samuti pilve salvestatud andmetega manipuleerida.[175] Eksperdid väidavad, et ei ole võimalust olla täiesti kindel andmete turvalisuses, kui see on juba pilve salvestatud. Turvaekspert Bruce Schneier'i[176] sõnul ei ole võimalustki tõde teada saada, sest kõik valetavad ja mitte kedagi ei saa usaldada. Samamoodi ei ole võimalik teada, milliseid tehnoloogiates kasutatavaid platvorme võib usaldada. Teenuse pakkujad võivad tõde moonutada või valetada isegi seetõttu, et on selleks valitsusorganisatsioonide poolt sunnitud.[177]

Tänu arenenud IKT-le saavad üksikisikud interneti kaudu hõlpsalt jagada teavet oma isiklike tegevuste kohta ning teha see üldsusele kättesaadavaks ennenägematus ulatuses. Kõige sagedamini kasutatakse informatsiooni ulatuslikuks avaldamiseks suhtlusvõrgustikke, kuid seda võimaldab ka pilvandmetöötlus, mille puhul üksikisikud võivad salvestada kellegi teise serverites olevatesse programmidesse delikaatseid isikuandmeid, kaotades seega nende üle

[173] Rahvusvaheline telekommunikatsiooni andmekaitse töörühm. Pilvandmetöötlus: eraelu puutumatuse ja andmekaitse probleemid - „Sopoti memorandum". Arvutivõrgus: http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/Pilvandmet%C3%B6%C3%B6tlus%20%20Sopoti%20memorandum.pdf, 27.02.2014, lk 2.
[174] Artikli 29 alusel loodud andmekaitse töörühm (viide 170), lk 4.
[175] P. De Filippi, L. Belli (viide 172), lk 2.
[176] Rahvusvaheliselt tunnustatud Ameerika Ühendriikide turvatehnoloog, kes on kirjutanud 12 raamatut ja hulgaliselt artikleid.
[177] L. Mearian. No, your data isn't secure in the cloud. Arvutivõrgus: http://www.computerworld.com/article/2483552/cloud-security/no--your-data-isn-t-secure-in-the-cloud.html, 02.03.2015.

kontrolli. Andmekaitseasutused, ettevõtjad ja tarbijaorganisatsioonid on asunud ühisele seisukohale, et internetis toimuvast tegevusest tulenevad ohud isikuandmete kaitsele aina suurenevad.[178] Kuigi teenuse pakkujad väidavad, et andmed hoitakse pilves krüpteerituna, siis ei ole siiski garantiisid, mis seda väidet toetaksid.[179] Magistritöö autori hinnangul on seega peamisteks põhjusteks, miks inimesed kaotavad internetis kontrolli oma isikuandmete üle, iga päev jagatavate andmete suur hulk ning mitte teadmine, et nende andmeid kogutakse. Digimaailmas on üksikisikutel samasugune õigus oma andmete kaitsele kui digitaliseerimata ühiskondades. Kuna digikeskkondades loob tehnoloogia palju suuremad võimalused andmete kuritarvitusteks, siis peavad üksikisiku õigused olema ka tugevamalt tagatud.

Kehtivad isikuandmete kaitse õiguslikud regulatsioonid ei anna adekvaatseid vastuseid järgmistele küsimustele: Kes täpselt omab andmetele juurdepääsu? Kuidas neid andmeid kasutatakse? Kui lihtne on andmete liigutamine ühest pilvest teise? Kui turvalised on pilved? Kes vastutab andmete väärkasutamise või kadumise korral? Isikuandmete kaitse õiguslikud instrumendid peavad tagama kõikehõlmava, tõhusa ja tulevikukindla regulatsiooni, mis kataks ära teemad seoses pilveteenuse pakkuja õiguste ja kohustuste kindlaksmääramisega, Euroopa Liidu õiguse kohaldatavusega, andmete liikumisega väljapoole Euroopa Liitu ning isikuandmetele juurdepääsuga välisriikide võimude poolt. Niikaua, kui eelnimetatud küsimustega ei tegeleta, ei ole võimalik efektiivselt üksikisikutele tagada Euroopa Liidu põhiõiguste hartast tulenevat põhiõigust isikuandmete kaitsele.[180]

Pilvandmetöötlus on ka Eestis akuutne teema. Nimelt on Eestis alustatud riigipilve ehitamist andmesaatkondade (*Data Embassy)* kontseptsiooni loomise nimetuse all. Eesti infoühiskonna arengukava 2020 kohaselt tagatakse virtuaalsaatkondade rakendamisega Eesti riigi järjepidevus ja riigi infosüsteemi toimepidevus, mis tähendab riigi jaoks oluliste registriandmete säilitamist teistes riikides asuvates virtuaalsetes keskkondades.[181] Magistritöö autori hinnangul riigi jaoks strateegilist tähtsust omavate andmete majutamine võõrriikide virtuaalsetes keskkondades ei ole turvaline ei kodanikele ega ka Eesti riigile tervikuna. Säilitatavad andmed sisaldavad magistritöö autori hinnangul muu riigi jaoks olulise informatsiooni hulgas ka isikustatud andmeid. Võõra riigi, isegi sõbraliku riigi, keskkond võib

[178] Euroopa Komisjon (viide 104), lk 1.
[179] L. Mearian (viide 177).
[180] Privacy International, UK. Cloud Computing. – An introduction to data protection. The European Digital Rights papers 2013, nr 06. Arvutivõrgus: https://edri.org/files/paper06_datap.pdf, 01.03.2015, lk 16.
[181] Majandus- ja kommunikatsiooniministeerium. Eesti infoühiskonna arengukava 2020. Arvutivõrgus: http://www.riso.ee/sites/default/files/elfinder/article_files/infoyhiskonna_arengukava_2020_f.pdf, 03.03.2015, lk 2.

mingil hetkel muutuda mittesõbralikuks ja kujutada ohtu Eesti riigi kodanike põhiõigustele ja julgeolekule. Magistritöö autor on magistritöös välja toonud, et andmete paigutamisel pilve, omab täielikku kontrolli andmete üle vaid teenuse pakkuja mitte teenuse saaja. Andmekaitse eesmärk ei ole iseenesest mitte kaitsta üksnes andmeid, vaid eelkõige isikuid, keda need andmed identifitseerivad või võimaldavad identifitseerida. Seega peaks riigile kuuluvate oluliste andmete pilve paigutamisse suhtuma teatud ettevaatusega.

Magistritöö autor teeb käesolevas alapeatükis analüüsitust järelduse, et tänapäevases infoühiskonnas tõusetunud probleemid seoses isikuandmete kaitsega on tingitud IKT ülikiirest arengust. Läbivateks probleemideks uute andmetöötlustehnoloogiate kasutuses on andmete töötlemise läbipaistmatus ja kontrolli kaotamine andmetega toimuva üle. Ühiskond tervikuna ei ole olnud võimeline tehnoloogiate arenguga sammu pidama, mistõttu ei oma kõik inimesed teadmisi, kuidas uute tehnoloogiatega ümber käia ning millist ohtu need inimese eraelule võivad kujutada. Inimese jaoks puudub sajaprotsendiline garantii, et tema isikuandmeid esialgsetel eesmärkidel kogutakse ja turvaliselt töödeldakse. Isikul on küll võimalus osaliselt kontrollida oma isikuandmete töötlemist, kuid vastuse usaldusväärsuses ei saa mitte kunagi olla täiesti kindel.

2.2. Mittetraditsioonilised võimalused isikuandmete kaitse tagamiseks

Kiiresti muutuvas ühiskonnas, kus uue IKT pealetung on vältimatu ning üheks peamiseks kaitsmist vajavaks põhiõigushüveks on muutunud isiku õigus oma andmete kaitsele, on hädavajalik tagada isikule tõhusad õiguskaitsevahendid juhtudeks, kui isiku õiguseid rikutakse. Isiku õiguste rikkumise korral on kõige tavalisem viis oma õiguseid kaitsta seaduse alusel läbi järelevalveasutuse või kohtu. Kiiresti muutuvas infoühiskonnas tuleb aga mõelda, kas tänaste traditsiooniliste õiguskaitsevahendite kõrval eksisteerib ka alternatiivseid, mittetraditsioonilisi meetmeid isikute õiguste kaitsmiseks. Veelgi tõhusam oleks õiguskaitsevahend, mis omaks ennetavat mõju ja hoiaks õigusrikkumiste toimepanemisest. Kohtusse pöördumise õigus võiks jääda viimaseks võimaluseks, millele eelnevalt tuleks kasutada ära kõik võimalikud muud olemasolevad õiguspärased meetmed.

Usutakse, et andmekaitseseaduse ja –printsiipide kõrval eksisteerib täiendavaid või alternatiivseid meetmeid, mis samamoodi tagavad isikuandmete kaitset. Osad instrumendid on teada juba dekaade ja kauemgi ning osade kasutamist julgustab kehtiv andmekaitsedirektiiv ise, kuid näib, et siiani on andmetöötlejate jaoks puudunud tõhus stiimul

uute meetmete kasutusele võtmiseks.[182] Andmekaitsedirektiivi artikkel 17 lõike 1 ja IKS-i § 25 lõike 1 järgi peab isikuandmete töötleja rakendama isikuandmete kaitseks füüsilisi, organisatoorseid ja infotehnilisi turvameetmeid[183], luues seega kõik võimalused uute täiendavate meetmete loomiseks ja rakendamiseks.

Käesolevas peatükis analüüsib magistritöö autor täiendavaid võimalusi andmekaitsedirektiivi ja isikuandmete kaitse seaduse kõrval, mis võimaldaksid tõhusalt tagada isikute põhiõigust isikuandmete kaitsele.

2.2.1. Eraelu puutumatust soodustav tehnoloogia ja lõimitud andmekaitse

Eraelu puutumatust soodustavat tehnoloogiat võib määratleda kui IKT meetmete ühtset süsteemi, mis kaitseb eraelu puutumatust isikuandmete volitamata töötlemise takistamise kaudu, ilma et see vähendaks infosüsteemi funktsionaalsust. Eraelu puutumatust soodustavate tehnoloogiate kasutamine aitab kavandada info- ja kommunikatsioonisüsteeme ning sideteenuseid selliselt, et need tagavad isikuandmete turvalise töötlemise ning hõlbustavad andmekaitse eeskirjade täitmist. Eraelu puutumatust soodustavate tehnoloogiate kasutamine peaks kaasa tooma selle, et teatavate andmekaitse eeskirjade rikkumine oleks keerulisem ja/või andmekaitse reeglite rikkumisi oleks võimalik lihtsamalt avastada. Eraelu puutumatust soodustavad tehnoloogiad võivad olla kas eraldiseisvad vahendid, mis nõuavad eraldi paigaldamist personaalarvutisse või olla ka juba infosüsteemidesse integreeritud.[184]

Krüpteerimine ja sellega seotud informatsiooni turvamehhanismid on üheks tehnoloogiliseks võimaluseks isikuandmete kaitse nõuete täitmisel. Kui 1990ndatel kasutati krüpteerimist ainult valitsusasutustes ja finantsmajanduses, siis praegu on krüpteerimine tehtud võimalikuks igas veebibrauseris, et tagada internetikeskkonnas tehtavate toimingute (rahaülekanded, e-kirjade saatmine) turvalisus. Maksete teostamise puhul jääb siiski risk, et maksekaartide andmed varastatakse kasutaja enda arvuti poolt seadmes oleva pahavara kaasabil. E-kirjade krüpteerimist kasutatakse aga väga vähe, kui üldse. E-kirjade krüpteerimine osutub tõhusaks ainult siis, kui seda kasutavad nii kirja saatja kui ka saaja. Kõik tavapärased

[182] Euroopa Komisjon. Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments. Arvutivõrgus: http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_en.pdf, 15.03.2015, lk 46.
[183] 95/46/EÜ art 17 lg 1, IKS § 25 lg 1.
[184] Euroopa Ühenduste Komisjoni teatis Euroopa Paramendile ja nõukogule andmekaitse edendamise kohta eraelu puutumatust soodustavate tehnoloogiate kaudu. KOM(2007) 228 lõplik. Brüssel: 2.5.2007 Arvutivõrgus: http://ec.europa.eu/transparency/regdoc/rep/1/2007/ET/1-2007-228-ET-F1-1.Pdf, 15.03.2015, lk 3.

operatsioonisüsteemid (*Microsoft Windows*, *Apple's MacOs*) võimaldavad andmete krüpteerimist, vähendades niimoodi andmetele juurpääsemise võimalusi seadme või andmekandjate varguse korral. Andmete krüpteerimine on eriti oluline mobiiltelefonides ja sülearvutites, sest nende seadmete kadumine või varastamine on suurema tõenäosusega ning mittekrüpteerimise korral oleks andmetele ligipääs ülilihtne. Isegi pilveteenuste puhul on pilves võimalik andmeid krüpteeritult hoida ja töödelda, vältides niimoodi andmetele volitamata juurdepääsu. Selleks, et andmeid volitamata juurdepääsu ja muutmise eest kaitsta, peab krüpteerimine olema lubatud ja õigesti konfigureeritud. Viimaste aastate suuremad isikuandmete kaitse rikkumised ongi olnud põhjustatud ebaõigest andmekaitsemeetmete konfigureerimisest või on turvameetmed üldse puudunud.[185]

Kui andmekaitse rikkumisest teavitamist on peetud üheks õiguskaitsevahendiks, siis täiendavalt võib seda pidada ka üheks osaks turvalisuse printsiibist. Nimelt on teavituse näol tegemist andmetöötleja kohustusega teatud tingimustel teavitada järelevalveasutust ja isikut juhul, kui ilmneb isikuandmete kaitse nõuete rikkumine. Teavitamise nõude rikkumist koos kõigi tagajärgedega tuleb käsitleda andmekaitse printsiibi rikkumisena, mitte õiguskaitsevahendina, milleks seda tavaliselt peetakse. Tõhus teavitus aitaks kehtivad õiguskaitsevahendid veelgi tõhusamaks muuta.[186]

Tavapärane arusaam isikuandmete deidentifitseerimisest või anonüümimisest on see, et nimetatud tehnikate kasutamine vähendab andmete väärkasutamise riske.[187] Andmekaitsedirektiivi põhjendusest 26 leiab anonüümimise mõiste määratluse, mille kohaselt tuleb andmete anonüümimiseks eemaldada neist kõik piisava teabega elemendid selliselt, et isikut ei ole enam võimalik tuvastada. Täpsemalt tuleb andmeid töödelda nii, et isikut ei ole enam võimalik tuvastada, võttes arvesse kõiki vahendeid, mida võidakse isiku tuvastamiseks tõenäoliselt kasutada. Seejuures on oluline tegur, et töötlemine peab olema pöördumatu. Võimalike anonüümimise mehhanismide kehtestamise vahendina viidatakse käitumisjuhenditele ning andmete salvestamisele viisil, mis ei võimalda isikut enam tuvastada. Seega on andmekaitsedirektiiviga selgelt kehtestatud väga ranged nõuded. Aluspõhimõte on, et anonüümimine kui isikuandmete suhtes kohaldatav tehnika peaks praeguse tehnoloogia arengu kontekstis olema sama püsiv kui andmete kustutamine, mis

[185] Euroopa Komisjon (viide 182), lk 47.
[186] *Op.Cit*., lk 47.
[187] *Op.Cit.,* lk 48.

tähendab, et anonüümimise tehnika kasutamise tagajärjel peaks isikuandmete töötlemine muutuma võimatuks.[188]

Privaatsuseelistuste platvorm (*Privacy Preferences Project, P3P*) on tehnoloogia, mis võimaldab isikul analüüsida veebisaitide privaatsuspoliitikat ja võrrelda seda oma eelistusi puudutavate andmetega, mida isik lubab avalikustada. P3P aitab tagada, et isik on oma andmete töötlemiseks andnud teadliku nõusoleku,[189] sest kasutades P3P tarkvara on isikutel palju lihtsam aru saada andmete töötlemise tingimustest, kui lugedes keerulisi privaatsuspoliitikaid. Artikli 29 alusel asutatud andmekaitse töörühm on ära märkinud, et P3P aitab standardida privaatsusteavitused ja kuigi P3P ise ei paku privaatsuse kaitset, siis jõustamise korral P3P tõstab suuresti andmed töötlemise läbipaistvust ning aitab parendada privaatsuse kaitset. Olenemata sellest, et vastased kampaaniagrupid kritiseerivad P3P tarkvara kui keerulist ja segadust tekitavat vahendit, mis muudab interneti kasutajatel raskeks oma privaatsust internetikeskkonnas kaitsta, säilitab P3P siiski oma väärtust kahtlusteta. [190]

Algselt nähti eraelu puutumatuse tagamist ainult läbi eraelu soodustavate tehnoloogiate, kuid praeguseks on jõutud äratundmisele, et eraelu soodustavate tehnoloogiate kasutamist on vaja laiendada lõimitud andmekaitse lahendusega. Lõimitud andmekaitse (*Privacy by Design*) idee on pärit aastast 1990 ja selle töötas välja Ontario teabe- ja andmekaitse volinik Ann Cavoukian. Lõimitud andmekaitse idee sündis tingituna üha suurenevatest süsteemsetest mõjudest, mis tulenesid IKT ning suuremahuliste andmesüsteemide võrgustikest. Lõimitud andmekaitse arendab sellist privaatsuse tagamise aspekti, mille kohaselt eraelu puutumatust ei saa tulevikus tagada ainult lähtudes õigusaktidest, vaid ideaalis peaksid privaatsuse tagamise tingimused olema paika pandud vaikimisi organisatsiooni töökorraldusega. Lõimitud andmekaitse hõlmab infosüsteeme, vastutavaid äritegevusi ning füüsilist ülesehitust ja võrgustatud infrastruktuuri. Lõimitud andmekaitse eesmärgid, milleks on eraelu puutumatuse tagamine ning isiku kontrolli saavutamine oma andmete kasutamise üle, on saavutatavad, kui rakendatakse isikuandmete kaitse algpõhimõtteid, mille kohaselt võib andmekaitse olla ennetav meede, püsiseisund, süsteemi osa, täielikult otstarbekohane, algusest lõpuni turvaline, nähtav ja läbipaistev ning kasutajakeskne.[191]

---

[188] Artikli 29 alusel asutatud andmekaitse töörühm. Arvamus nr 05/2014 anonüümimistehnikate kohta. WP216. Brüssel: 10.04.2014. Arvutivõrgus: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_et.pdf, 15.03.2014, lk 5-6.
[189] Euroopa Komisjon (viide 184), lk 4.
[190] Euroopa Komisjon (viide 182), lk 48-49.
[191] A. Cavoukian. Privacy by Design. The 7 Foundational Principles Arvutivõrgus: https://www.ipc.on.ca/images/resources/7foundationalprinciples.pdf, 15.03.2015.

Euroopa Komisjoni arvates omab lõimitud andmekaitse olulist potentsiaali isikuandmete kaitses. Kõige olulisem on veenda poliitikate kujundajaid ja äriliidreid pöörama vajalikku tähelepanu uute infosüsteemidega seotud privaatsusnõuetele enne infosüsteemide arendama hakkamist. Palju lihtsam on toota privaatsussõbralikke süsteeme, kui andmekaitsereeglid lepitakse kokku juba disainifaasis. Ometigi võib aga esineda olulisi isikuandmete kaitse rikkumisi. Eelkõige võivad andmekaitse rikkumised tuleneda rohkesti delikaatseid isikuandmeid sisaldavatest väga suurtest andmebaasidest, näiteks e-valitsuse andmebaasid, millele omavad volitatud juurdepääsu sajad töötajad.[192] Magistritöö autori arvates on inimene ise üheks ohuallikaks isikuandmete kaitse reeglite mittetäitmisel, kuid seda riski maandavad infotehnoloogilised meetmed (infosüsteemi logimise nõue), mis on infosüsteemides rakendatud, et võimalikke rikkumisi oleks võimalik reaktiivelt kindlaks teha.

Euroopa andmekaitseinspektor nimetab lõimitud andmekaitset eraelu kavandatud puutumatuseks ning märgib ära vajaduse, et juba IKT kavandamisel ja arendamisel võetakse arvesse eraelu puutumatust ja andmekaitset. Seega on äärmiselt oluline, et eraelu puutumatus ja andmekaitse moodustaksid osa tervest tehnoloogia elutsüklist. Kui aga eraelu puutumatuse ja andmekaitsega ei arvestata algusest peale, siis on tihti liiga hilja süsteeme hiljem parandada ning samuti ei ole võimalik hüvitada juba tekkinud kahju. Eraelu kavandatud puutumatuse põhimõtet rakendavat IKT-d kasutamine ei ole aga praktikas eriti levinud. IKT tootjad ega vastutavad andmetöötlejad ei ole suutnud järjepidevalt rakendada või turustada eraelu kavandatud puutumatust. Samas on ka nõudlus eraelu kavandatud puutumatuse järele olnud väike, sest õigusega eeldatakse isikuandmete *de facto* kaitsmist, kuigi paljudel juhtudel see nii ei ole. Mõnedel juhtudel ei ole lihtsalt võimalik turvameetmeid isikuandmete kaitseks rakendada ning paljudel juhtudel ei olda riskidest teadlikud, kas siis osaliselt või täielikult.[193]

Kehtiv andmekaitsedirektiiv ei sisalda selgesõnalist nõuet eraelu kavandatud puutumatuse kohta ja tehnoloogilises kontekstis oleks eriolukordades kohaldatav artikkel 17, kui seda tõlgendatakse konkreetsetest asjaoludest lähtuvalt. Eraelu puutumatust ja elektroonilist sidet käsitleva direktiivi artikkel 14 lõige 3 on aga selgesõnalisem, lubades vajaduse korral vastu võtta meetmeid tagamaks, et lõppseadmete konstrueerimine on kooskõlas kasutajate õigusega kaitsta oma isikuandmeid ja kontrollida nende kasutamist. See säte ei ole aga kunagi kasutamist leidnud. Kuna artikkel 17 kohaldub vastutavatele andmetöötlejatele ja mitte IKT

[192] Euroopa Komisjon (viide 182), lk 50.
[193] Euroopa andmekaitseinspektor (viide 5), lk 1-4.

tootjatele, siis Euroopa andmekaitse inspektor soovitab lisada ühemõtteliselt ja selgesõnaliselt kehtivasse andmekaitse õigusraamistikku eraelu kavandatud puutumatuse põhimõtte.[194] Euroopa Komisjon on arvamusel, et eraelu puutumatust soodustavad tehnoloogiad on välja mõeldud selleks, et tagada andmekaitse seaduste tehnoloogilist jõustamist.[195] Tehnoloogial põhineva andmekaitse kontseptsioon seisneb aga selles, et kui ohtusid andmekaitsele või andmekaitse rikkumisi faktiliselt ei ole, siis ei ole vajalik kohaldada ka õiguslikke piiranguid, sest eraelu puutumatust soodustav tehnoloogia pakub arvestatavaid võimalusi andmekaitseks.[196] Isikuandmete kaitse üldmäärus sisaldab samuti tehnoloogial põhineva andmekaitse kontseptsiooni üldmääruse artiklis 23, mille kohaselt võetakse töötlemisvahendite valikul ja töötlemise käigus kasutusele selliseid tehnilisi ja organisatsioonilisi meetmeid, millega tagatakse töötlemise vastavus määruse nõuetele ja andmesubjekti õiguste kaitsmine.[197] Eelnimetatud artikli sõnastus on oma olemuselt leebe, sest ei sisalda siduvat kohustust, kuid tehnoloogiliste mehhanismide kasutamine andmete kaitsmisel on edukas ainult siis, kui spetsiifilise tehnoloogia kasutamine jõustatakse kohustuslikus korras.[198]

Magistritöö autor põhimõtteliselt nõustub andmekaitseinspektoriga, kuid suhtub eelarvamusega põhimõtte ühemõttelisse sõnastamisesse. Euroopa Kohus ei ole pidanud otstarbekaks mõiste „eraelu“ ammendavat defineerimist, sest eraelu võib hõlmata aspekte, mida ei ole võimalik ette näha.[199] Seetõttu ei ole magistritöö autori hinnangul ka otstarbekas ammendavalt sõnastada eraelu puutumatuse põhimõtet. Eeltoodut toetab ka asjaolu, et suures osas on infosüsteemide tellijaks riik kui vastutav andmetöötleja. Andmete, mida tellitavas infosüsteemis töötlema hakatakse, tundlikkuse tasemest sõltuvad ka infosüsteemile esitatavad andmekaitsenõuded, mis kirjeldatakse tellija poolt tehnilises kirjelduses. Kuigi reeglina kannavad kogu õiguslikku vastutust andmekaitse eeskirjade täitmise eest vastutavad andmetöötlejad, siis jääb ühiskondlikust ja eetilisest vaatepunktist teatav vastutus andmekaitse eest ka teistele osalistele, kelleks on tehniliste kirjelduste koostajad ning rakenduste ja operatsioonisüsteemide loojad ja rakendajad.[200]

---

[194] *Op.Cit*., lk 5-6.
[195] *Op.Cit.,* lk 48.
[196] G. Hornung. Regulating privacy enhancing technologies: seizing the opportunity of the futuure European Data Protection Framework. – The European Journal of Social Science Research 2013, nr 26, lk 182.
[197] Isikuandmete kaitse üldmääruse eelnõu art 23.
[198] G. Hornung (viide 196), lk 187.
[199] EIKo 16.02.2000, 27798/95 *Amann v Šveits*, p 65; EIKo 25.09.2001, 44787/98, *P.G. and J.H. v Ühendatud Kuningriigid* p 56.
[200] Euroopa Komisjon (viide 184), lk 2.

2.2.2. Iseregulatsioon

Euroopa Liit on järjepidevalt arendanud uut regulatiivset poliitikat, mis paneb suurt rõhku meetmetele, mis oleksid alternatiivid või täiendavad vahendid traditsioonilistele „käsin ja kontrollin“ seadustele. Euroopa Liidu regulatiivsete instrumentide mitmekesistamine on peamiselt tingitud vajadusest tõsta toimingute tõhusust, seaduslikkust ja läbipaistvust. Seaduse täiendavaid või alternatiivseid regulatiivseid instrumente, milleks võivad muuhulgas olla soovitused ja vabatahtlikud kokkulepped, nimetatakse iseregulatsioonideks. Iseregulatsioonides nähakse mehhanismi, mis viiks vähesema ja kvaliteetsema õigusliku reguleerimiseni ning mitmekesistaks euroopalikku valitsemise mehhanismi. Iseregulatsioonide populariseerimine on Euroopa Komisjoni pannud rääkima iseregulatsioonidest kui uuest seadusandlikust kultuurist.[201]

Iseregulatsioon ei ole tänapäeva ühiskonnas midagi uut, kuigi see alguses nii võib tunduda. Iseregulatsiooni võib mõista kui vaikepositsiooni, millest lähtuvalt ühiskonnas probleeme lahendatakse. Kui seadus ei sekku, siis on iseregulatsioon just see võimalus, läbi mille isikud ja organisatsioonid oma huvisid kaitsevad. Privaatsuse ja andmekaitse iseregulatsiooni kontseptsiooni on rohkem kasutatud strateegilistel eesmärkidel. Algselt oli iseregulatsioon kasutuses seadusandlust ennetava või edasilükkava meetmena. Iseregulatsioone on võimalik kasutada eksperimendi meetmena, et seaduste ettevalmistamine oleks võimalikult paindlik. Kolmas võimalus on, et valdkonnapõhised iseregulatsioonid täiendavad seaduseid, et seadustes vältida liiga detailset reguleerimist. Neljanda võimalusena pakuvad iseregulatsioonid lahendusi küsimustes, mis on jäänud seaduse reguleerimisalast välja ja millest võib sõltuda uus poliitikakujundus.[202] Magistritöö autori hinnangul on iseregulatsioon selline meede, millega on võimalik detailselt reguleerida organisatsioonide sisest töökorraldust (nt infovara kasutamise kord, mis hõlmab ka isikuandmete töötlemise põhimõtteid), teavitades isikuid läbi iseregulatsioonide kaudu nende õigustest ja kohustustest.

Vaatamata aina kestvatele andmekaitse ekspertide aruteludele seoses privaatsuse säilitamisega internetikeskkonnas, on iseregulatsioon siiski peamiseks vahendiks kasutajate andmete kaitse tagamisel. Iseregulatsioon sobitub ühiskonda paremini kui seadus, sest iseregulatsiooni

[201] L. Senden. Soft-law, self-regulation and co-regulation in European law: Where Do They Meet? – Electronic Journal of Comparative Law 2005, nr 9.1, lk 1-2.
[202] P. J. Hustinix. Co-regulation or self-regulation by public and private bodies – the case of data protection. Freundesgabe Büllesbach 2002. Arvutivõrgus: http://www.alfred-buellesbach.de/PDF/27_Hustinx.pdf, 16.03.2015, lk 2-3.

loomise ja jõustamise aeg on tunduvalt lühem kui seaduste vastuvõtmise aeg. Iseregulatsioonid pakuvad lahendusi tegelikele probleemidele. Lubades tööstusel isereguleerida, panustatakse koos andmekaitsega ka innovatsiooni tehnoloogias. Iseregulatsioonid soodustavad organisatsioonide edukust. Ettevõtted, mis pakuvad parimaid tooteid ja teenuseid, on reeglina ka kõige vastutustundlikumad oma klientide andmete kaitse osas. Iseregulatsioonid sobituvad väga hästi lõimitud andmekaitsega, majutades privaatsuse tehnoloogiasse juba algfaasis, võimaldades sel viisil kasutajatel omada kontrolli oma andmete üle. Iseregulatsioonidega saab reguleerida ka juhtusid, mis on seotud juba avaldatud andmetega, mistõttu organisatsioonid peavad säilitama teatud ettevaatlikuse, kui andmeid kasutatakse tundlikel eesmärkidel nagu näiteks töötajate värbamine.[203] Kui iseregulatsioon on õigesti koostatud, siis see on seadusele mitte ainult täienduseks, vaid ka tunnustuseks. Iseregulatsioon aitab luua tööstuses parimaid praktikaid ja on dünaamiliseks vahendiks isikute usalduse kasvatamisel organisatsioonide vastu. Iseregulatsioonid vastupidiselt seadusele on piisavalt paindlikud, soodustades uute tehnoloogiate, millest seaduse jõustamisel ei teatud veel unistadagi, kiiret kasutusele võtmist ja kohanemist ühiskonnas.[204]

Iseregulatsioonid laiemas tähenduses on seadusel põhinevad käitumisjuhendid konkreetsele subjektide ringile nende eesmärkide paremaks saavutamiseks ja huvide kaitseks. Kitsamas tähenduses mõistetakse iseregulatsioonide all aga ühte õigusloome viisi juhul, kui seadusloome vahenditest ei piisa õigusprobleemide lahendamiseks. Kõige tavalisemad iseregulatsiooniinstrumendid on käitumisjuhendid, mis kehtestatakse nii rahvusvahelisel, valdkondlikul kui ka üksiktasandil.[205] Magistritöö autori arvates on organisatsioonides muude käitumisreeglite hulgas kõige levinumaks iseregulatsiooniinstrumendiks töökorralduse reeglid. Tänapäeva digitaalühiskonnas üksikisikute privaatsusõiguste tagamise paremaks korraldamiseks on organisatsioonides soovitatav kehtestada infovarade kasutamise reeglid ning samuti ka privaatsuspoliitika. Iseregulatsioon tagab isikule oma õiguste teadvustamise, sest isik ei pruugi teada oma seadusest tulenevaid õiguseid, kui seadust ei tunta, kuid asutuse tööd korraldavate dokumentidega tuleb isikul igal juhul tutvuda. Iseregulatsioonid kaitsevad üheaegselt nii tööandja kui ka töötaja õiguseid. Magistritöö autori hinnangul on iseregulatsiooni positiivseks küljeks veel see, et iseregulatsioone on võimalik koostada sellises kirjakeeles, millest isik ka aru saab. Seaduste sõnastused on tavaliselt väga keerulised

[203] J. Adler. When Self-Regulation Works, Your Privacy Is In Good Hands. Arvutivõrgus: http://www.truste.com/blog/2012/07/27/when-self-regulation-works-your-privacy-is-in-good-hands/, 16.03.2015.
[204] T. Ruback. A Brief Look at Self-Regulation and European Data Protection. Arvutivõrgus: https://privacyassociation.org/news/a/a-brief-look-at-self-regulation-and-european-data-protection/, 16.03.2015.
[205] E. Tikk. A.Nõmper (viide 33), lk 173.

ja kõik isikud ei pruugi seaduseid seetõttu mõista. Magistritöö autor, tuginedes oma kogemusele julgeb väita, et infotehnoloogia teemalised iseregulatsioonid on isikutele samuti keerulised mõista oma valdkonnaspetsiifiliste terminite tõttu. Eelnimetatu on aga omakorda proovikiviks organisatsioonide juristidele, et panna spetsiifiline sõnakasutus tavainimesele mõistetavasse keelde.

Magistritöö autori hinnangul annab iseregulatsiooni kontseptsioon suurepärase võimaluse reguleerimaks sellist spetsiifilist valdkonda nagu seda on IKT, arvestades kõiki neid eeliseid, mida iseregulatsioon seaduse ees omab. Kuna IKT on pidevas muutumises, siis ei olegi võimalik seadusega kõiki juhtusid andmekaitseõiguse valdkonnas ette näha. Abstraktselt sõnastatud seadus jätab rakendajatele tõlgendamisruumi ja aitab seega kaasa igapäevase valdkondliku praktika kujunemisele ning pretsedendiõiguse arengule.

Euroopa andmekaitseinspektor kiidab heaks Euroopa Komisjoni lähenemisviisi kasutada iseregulatsiooni instrumente, kuid juhib tähelepanu sellele, et vaja on alternatiivseid meetmeid ka iseregulatsioonile juhuks, kui see ei too oodatud tulemusi. 2009. aastal võttis Euroopa Komisjon vastu soovituse eraelu puutumatuse ja andmekaitse põhimõtete kohaldamise kohta raadiosagedustuvastust kasutavates rakendustes[206], mille kohaselt tuleb raadiosagedustuvastust kasutavates rakendustes deaktiveerida müügihetkel isikuandmeid salvestav märgis, välja arvatud juhul kui isik on andnud nõusoleku töötava märgise allesjätmiseks. Nimelt muretseb andmekaitseinspektor, et jaemüügis raadiosagedustuvastuse rakendusi kasutavatele organisatsioonidele võib jääda märkamatuks, et raadiosagedustuvastuse märgiseid jälgivad kolmandad isikud. Kui müügihetkel rakendustes märgist ei deaktiveerita, siis pääsetakse ligi märgises salvestatud isikuandmetele. Samuti on kolmandal isikul võimalik aja jooksul isikut jälgida või tuvastada, kasutades selleks märgises sisalduvaid kordumatuid tunnuskoode ja seda isegi keskkonnas, mis jääb raadiosagedustuvastuse rakenduse piirkonnast väljapoole. Sellises olukorras võib olla liiga hilja leevendada riske seoses isikuandmete kaitse ja eraelu puutumatusega. Siinjuures võib lahenduseks olla, et raadiosagedustuvastuse märgised on juba müügihetkel vaikimisi deaktiveeritud.[207] Eeltoodud näide illustreerib väga ilmekalt juhtu, millal iseregulatsioon ei toiminud, mistõttu peab ka iseregulatsioonidele ette nägema alternatiivsed instrumendid.

[206] Euroopa Ühenduste Komisjoni soovitus eraelu puutumatuse ja andmekaitse põhimõtete kohaldamise kohta raadiosagedustuvastust kasutavates rakendustes. Brüssel: 12.5.2009. (K(2009) 3200 (lõplik)). Arvutivõrgus: http://www.europarl.europa.eu/RegData/docs_autres_institutions/commission_europeenne/sec/2009/0586/COM_SEC(2009)0586_ET.pdf, 15.03.2015.

[207] Euroopa andmekaitseinspektor (viide 5), lk 9.

Magistritöö autori hinnangul ei tasu iseregulatsioone karta, sest autorile teadaolevalt ei eksisteeri ühiskonnas ühtegi sajaprotsendiliselt tõhusat vahendit. Nii nagu seadustes on lüngad, võib puuduseid ette tulla ka muudes regulatiivsetes instrumentides. Kui ühiskonnale on loodud võimalus iseregulatsioone kasutada, siis tuleks seda aina rohkem teha, arvestades hetkelist vähest aktiivsust iseregulatsioonide kasutamisel.

3. Isikuandmete kaitse perspektiivid - uue regulatsiooni vajadus?

Informatsioon on toormaterjaliks tänapäeva infoajastule, millesse jõudsime 1990ndate alguses. Kui agraarajastul õigus arenes, et määrata kindlaks käitumisjuhised maa kui kõige olulisema väärtuse kasutamiseks, siis infoajastul ootame õiguselt informatsiooni kasutamise reguleerimist.[208] IKT on juba oma arenemise algusajast olnud igapäevaseks proovikiviks andmekaitse seadustele.[209] Enamus riigid seisavad silmitsi IKT-st tingitud küsimustega isikuandmete kaitse valdkonnas, kuid ühtse õigusliku lahenduseni ei ole senini jõutud. Kui Euroopa riikides reguleeritakse andmekaitseõigust üldseaduste tasandil, üritades katta kõik andmete töötlemisega seotud aspektid, siis Ameerika Ühendriikides eelistatakse valdkondlikke eriseaduseid reguleerimaks spetsiifilisi informatsiooni käsitlemise vorme.[210] Põhiõiguste ja –vabaduste kataloogid, mis on ära nimetatud konkreetsetes mitmepoolsetes kokkulepetes, annavad palju normatiivseid aluseid andmekaitse seaduste ja poliitikate loomiseks.[211]

Magistritöö autori hinnangul elati dekaade tagasi ühiskonnas, kus kõike tuli teha käsitsi. Selles ajas ja ruumis oligi see nn tavaline elu. Tänapäeval on tehnoloogia arengu tulemusel jõutud ühiskonnani, kus inimesed elavad küberruumis virtuaalset elu, automatiseeritud e-elu, mis on praeguses ajas ja ruumis nn tavaline elu. Tulevikus elatakse samuti ajas ja ruumis, mis vastab tulevikutingimustele ja on samuti tavaline elu. Mõisted on ajas ja ruumis muutuvad nähtused, mille tõestuseks on mõiste „tavaline elu“ tähenduse muutumine. Tehnoloogia abil progresseeruvas ühiskonnas sündis isikuandmete kaitse, mille tähendus on samuti ajas ja ruumis vastavalt asjaoludele muutunud. IKT hoogsa arengu tõttu näitab isikuandmete kaitse olulisus maailmas jätkuvat tõusutrendi. Euroopa andmekaitsereform, millega alustati 2012. aastal, ei ole magistritöö kirjutamise hetkel veel lõppenud, kuigi eesmärgiks oli seatud saavutada see 2014. aastaks. Andmekaitsereformiga kavandatavate muudatuste tulemusena tagatakse isikule lihtne juurdepääs oma isikuandmetele ning vabadus kanda isikuandmeid üle ühelt teenusepakkujalt teisele takistusteta esimese teenusepakkuja poolt, kehtestatakse nn õigus olla unustatud ja selgesõnalise nõusoleku nõue. Andmekaitsereformi tulemusel kehtestatav isikuandmete kaitse üldmäärus on liikmesriikidele otsekohalduv, mis tagab terves

[208] C. Rees, S. Chalton. Database Law. Bristol: Jordan Publishing Limited, 1998, lk 1.
[209] A. Kiss, G. L. Szoke (viide 35), lk 312.
[210] I. J. Lloyd (viide 36), lk 21-22.
[211] L. A. Bygrave (viide 49), lk 247-248.

Euroopa Liidus ühtsete andmekaitse eeskirjade kohaldamise.[212] Täna on Euroopa Liidus 27 liikmesriiki ja 27 erinevat andmekaitse seadust, sest siseriiklikku õigusesse üle võetud andmekaitsedirektiiv sätestab ainult minimaalsed andmekaitsereeglid. Isikuandmete kaitse üldmäärus on sõnastatud sama üldiselt kui andmekaitsedirektiiv ning ei sisalda spetsiifilisi andmekaitse sätteid. Isikuandmete kaitse üldmäärus mitte ainult ei tühista liikmesriikide andmekaitseseaduseid, vaid avaldab ka otsest mõju liikmesriikide spetsiifilistele andmekaitsereeglitele. Kuid milline see mõju täpselt on, ei ole veel teada. Isikuandmete kaitse üldmääruses sätestatud üldised reeglid praktikas ilma valdkonna spetsiifiliste reegliteta ei toimi.[213] Magistritöö autori hinnangul ei ohusta see siiski isikute õiguskaitsevahendite taotlemise võimalusi, sest oma õiguste rikkumise korral kohtusse pöördumise õigus on tagatud kõrgemalseisvate õigusaktidega.

Üha suuremat populaarsust on kogumas tehnoloogilised strateegiad nagu suurandmete haldamine ja pilvandmetöötlus. Suurandmete haldamise ja pilvandmetöötluse ühtse turu jaoks ei ole veel õigeid raamtingimusi, mis eelkõige seisneksid teenuste turvalisuse, usaldusväärsuse ja kvaliteetsuse edendamises. Euroopa Liit peaks eelnimetatud tingimused looma. Euroopa Ülemkogu nõuab ka tugeva riiklike digitaalteenuste koordinaatorite võrgustiku loomist, mis võib pilvandmetöötluses ja suurandmete haldamises omada strateegilist tähtsust.[214]

Magistritöö eelmisest peatükist selgus, et tänasel hetkel on isikuandmete kaitse maastikul eksisteerivad õiguslikud probleemid paljustki tulenenud IKT arengust. Eelnimetatud seisukohta toetab ka Euroopa Liidu Põhiõiguste Ameti uuring, mille kohaselt on kõige sagedasemad andmekaitserikkumised seotud internetiga.[215] Innovaatiliste tehnoloogiate tõttu on isikud kaotanud kontrolli oma andmetega toimuva üle. Isikuandmete kaitse üldmääruse jõustumisega võidakse küll isikule tagada tõhusam kontroll oma andmete üle, kuid magistritöö autori arvates mõjutab uus tehnoloogia kõige enam hoopis isikuandmete

[212] Euroopa Komisjon. Kuidas kohandatakse ELi reformiga andmekaitse-eeskirju uue tehnoloogilise arenguga? Arvutivõrgus: http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/8_et.pdf, 27.03.2015.
[213] W. Kotschy. The proposal for a new General Data Protection Regulation – problems solved? – International Data Privacy Law 2014, nr 4 (4), lk 275.
[214] Euroopa Ülemkogu järeldused, milles keskendutakse digitaalmajandusele, innovatsioonile ja teenustele ning rõhutatakse ühtse digitaalse turu välja kujundamise vajadust. EUCO 169/13. Brüssel: 25.10.2013. Arvutivõrgus: http://www.riigikogu.ee/?op=emsplain&page=pub_file&file_id=5e49dedb-09a1-479b-acbf-09ef47bf0897&.pdf, 08.03.2014, lk 1-2.
[215] Euroopa Liidu Põhiõiguste Amet. Juurdepääs andmekaitse õiguskaitsevahenditele Euroopa Liidu liikmesriikides. Kokkuvõte. Arvutivõrgus: http://bookshop.europa.eu/et/juurdepaeaes-andmekaitse-iguskaitsevahenditele-euroopa-liidu-liikmesriikides-pbTK0113752/downloads/TK-01-13-752-ET-C/TK0113752ETC_002.pdf?FileName=TK0113752ETC_002.pdf&SKU=TK0113752ETC_PDF&CatalogueNumber=TK-01-13-752-ET-C, 30.03.2015, lk 3.

töötlemise põhimõtteid. Isikuandmete töötlemine uute tehnoloogiatega on muutunud läbipaistmatumaks, mida toetab asjade interneti puhul asjaolu, et teenusepakkujate privaatsuspoliitikad on ebaselged. Profileerimise protseduur kriminaalmenetluste korral on samuti läbipaistmatu, sest isikul puudub üldse teave, et tema andmeid sellisel viisil analüüsitakse. Pilvetehnoloogia puhul puudub isikutel täpne teave andmetöötlustoimingute kohta, sest kui kord on juba andmed pilve talletatud, siis on isik kaotanud kontrolli töötlustoimingute üle. Eelnimetatust järeldub, et piiratud on isiku individuaalse osaluse põhimõte, sest kui isik ei tea, siis ei saa ta ka olla osaline. Puutumata ei jää ka eesmärgipärasuse põhimõte, sest kui ei ole konkreetselt selge milleks andmeid töödeldakse, siis ei toimu andmete töötlemine kindlaks määratud eesmärgil nagu seda nõuab eesmärgipärasuse põhimõte. Eesmärgipärasuse põhimõtet mõjutab samuti suurandmestik. Suurandmed on kogunenud muudel kindlatel eesmärkidel ja kindlasti mitte profileerimise eesmärgil. Profileerimise korral on tegemist juba uue eesmärgiga, mis ei ole kooskõlas andmete töötlemise eesmärgipärasuse põhimõttega. Minimaalsuse põhimõtte kohaselt ei koguta isikuandmeid rohkem, kui eesmärgi täitmiseks vajalik. Eelmisest magistritöö peatükist aga selgus, et kogutakse igasuguseid andmeid ja suurtes kogustes ning mitte ainult ei koguta, vaid andmed kogunevad ise tänu arenenud tehnoloogiale. Samuti selgus, et suurandmete töötlemine paneb küsimärgi alla andmete turvalisuse seoses informatsiooni rohkuse ja selle jagamise võimalustega. Suurandmete puhul tuleb teatud ettevaatusega suhtuda ka andmete kvaliteeti. Sellises tohutus koguses informatsiooni kontrollimine on võimatu, puuduvad tagatised, et informatsioon on õige ja vastab viimasele seisule. Eelkirjeldatu tekitab küsimuse, kuidas on siis isikule tagatud tema andmete õiguspärane töötlemine, kui IKT poolt loodud andmetöötlusvõimalused õõnestavad andmekaitse üldpõhimõtteid, mille peamiseks eesmärgiks on kaitsta isiku põhiõiguseid, eelkõige õigust eraelu puutumatusele.[216] Magistritöö autori hinnangul võib andmekaitsereform pikemas perspektiivis oma eesmärgid täita, kuid arvestades selle vastuvõtmiseks kulunud aega ja asjaosaliste vaidlusi, siis saab selle rakendamine olema tõenäoliselt valulik. Magistritöö autor arvab, et seaduste reformimisel tuleb keskenduda rohkem IKT seostele andmekaitse põhiprintsiipidega, mis on andmekaitseseaduste loomisel aluseks võetud. Isikuandmete kaitse üldmäärusesse on lisatud, et lisaks seaduslikule ja õiglasele isikuandmete töötlemisele peab isikutele tagatama läbipaistev andmete töötlemine.[217] Magistritöö autori arvates on läbipaistvuse printsiipi

[216] I. S. Rubinstein. The End of Privacy or a New Beginning? – International Data Privacy Law 2013, nr 3(2), lk 75.
[217] Isikuandmete kaitse üldmäärus art 5.

praktikas väga keeruline rakendada arvestades IKT poolt pakutavaid erinevaid andmete töötlemise võimalusi.

Magistritöö esimeses peatükis selgus, et tegelikult on andmekaitse seadused vaatamata oma tehnoloogianeutraalsele sõnastusele ikkagi kohaldatavad ka tehnoloogilises kontekstis. Tehnoloogianeutraalsus seadustes võimaldab uute tehnoloogiate kasutusele võttu ja paindlikud andmekaitsereeglid võimaldavad vajalikku kaitset olenevalt konkreetsetest asjaoludest.[218] Seetõttu ei ole magistritöö autori arvates ka vajadust seadust muuta, et tagada isikutele õiguskaitset andmekaitse rikkumiste korral. Kõiki juhtusid ei ole võimalik seaduse muutmisega lahendada, sest kõiki juhtusid ei ole lihtsalt võimalik ette näha. Uute vajaduste ilmnemisel on küll võimalik koheselt seadust muuta, kuid õigusloome protsess on aeganõudev ja ei pruugi alati ka kõige otstarbekam olla. Peale seaduse on olemas ka teisi võimalusi vajalike käitumisreeglite kehtestamiseks või kujundamiseks. Seaduseid võiks olla võimalikult vähe, et ei tekiks ülereguleerimist. Ülereguleerimise vältimiseks oleks võimalik, nagu andmete kogumisegi puhul, rakendada minimaalsuse põhimõtet – nii palju kui vajalik ja nii vähe kui võimalik. Magistritöö autori hinnangul on tänapäeva ühiskonnas võetud omaks põhimõte, mille kohaselt lähtutakse ainult kirjutatud reeglitest. Enne ei juhtu mitte midagi, kui kirjas ei ole. Tänapäeva õiguses on loomingulisus kui väärtus hääbumas ja tava on raske sündima, kui ühiskonnas oodatakse ainult kirjutatud õigust. Magistritöö autor nimetas teise peatüki teises punktis ära privaatsust tagava tehnoloogia, privaatsuslõime ja iseregulatsiooni kui isikuandmete kaitse tagamise alternatiivsed võimalused, mille rakendamiseks on kõik eeldused loodud. Ühiskonnas on vaja ainult pealehakkamist ja loomingulisust, et need seadust asendavad ja täiendavad meetmed tööle rakendada. Sageli valitakse probleemide lahendamiseks aga lihtsam ja vähem aeganõudev lahendus.

Euroopa Liidu Põhiõiguste Ameti läbiviidud uuringu kohaselt ei ole juristidel piisavalt andmekaitselisi eriteadmisi. Paljud ohvrid loobuvad õiguskaitsevahendi taotlemisest seetõttu, et ei ole usaldusväärset ja asjatundlikku abi. Professionaalse andmekaitsealase abi olemasolu korral oleks õiguskaitsevahendi rakendamine kättesaadavam ja seetõttu ka tõhusam. Andmekaitsealaste rikkumiste korral loobutakse õiguskaitsevahendi taotlemisest veel keerulise menetluse, vähese teadlikkuse ning suurte kulude tõttu. Samuti ei ole andmekaitse valdkonnale spetsialiseerunud kohtunikke, sest andmekaitse kohtuasju on vähe, mis välistab

[218] J. Miller. D. Hoffman. Sponsoring trust in tomorrow's technology: towards a lobal digital infrastructure policy. - International Data Privacy Law 2011, nr 1(2), lk 75.

andmekaitsealaste oskuste ja kogemuse tekkimise.[219] Eeltoodu põhjal teeb magistritöö autor järelduse, et õigusspetsialistidele on vaja süvateadmisi andmekaitsest seoses tehnoloogiaga, et tekiks vajalikud oskused andmekaitseõiguse rakendamiseks. Nii Tallinna Tehnikaülikoolis kui ka Tartu Ülikoolis on IT-õiguse õppekavad, mis pakuvad juristidele võimalust omandada süvendatult IKT alaseid teadmisi. IT-õiguse õppekavad sisaldavad ka IKT-ga seotud ja ühiskonnas väga olulist positsiooni omavat andmekaitseõigust. Magistritöö autori arvates ei piisa ainult juristidele süvendatud IKT teadmiste pakkumisest, vaid ka IT spetsialistidele tuleb pakkuda vastavat õigusalaste teadmiste omandamise võimalust. IT spetsialist, kes tegeleb isikuandmeid sisaldavate infosüsteemidega peab mõistma, et iga tema tegevus võib andmekaitse seaduse tähenduses põhjustada isikuandmete kaitse alast rikkumist ja tekitada kellelegi kahju, mida ei ole võimalik enam olematuks muuta. Seejuures ei saa ära unustada, et andmekaitseõigus on põhiõigus, mis peab olema igale isikule tagatud. Selleks, et näha tervikpilti õiguse ja IKT koostoimimisest, peaksid IT spetsialistid omandama ka põhjalikuma õigushariduse ja mitte ainult teadmised õiguse üldpõhimõtete tasemel. Õiguse ja IKT puhul peaks tegemist olema kahesuunalise protsessiga, sest nii nagu jurist peab mõistma IKT seoseid õigusega, siis ka IT spetsialist peab aru saama õiguse seostest IKT-ga. Magistritöö autori arvates on lisaks süvateadmisele vaja spetsialistidel ka julgust andmekaitseõiguse rakendamiseks, et andmekaitseõigusel oleks võimalik liikuda teooriast praktikasse.

Magistritöö autori hinnangul ei ole Eestis vajalik kehtestada isikuandmete kaitse õigust eraldi põhiõigusena. Euroopa Liidu põhiõiguste harta tagab isikuandmete kaitse õiguse kui põhiõiguse ja harta kohaldub ka Eestile. Lisaks on Eestis õigus isikuandmete kaitsele tagatud põhiseaduses sätestatud informatsioonilise enesemääramise õigusega või õigusega eraelu puutumatusele. IKS-i eesmärk on samuti tagada isiku põhiõiguste kaitse. Eeltoodust tulenevalt on Eestis isikuandmete kaitse nõuete rikkumise korral põhiõiguslik kaitse täiesti olemas. Seega eraldi põhiõigust isikuandmete kaitsele sätestada ei ole vajalik, kuid kaaluda võiks ulatuslikumaid teavituskampaaniaid, et isikutele teadvustada, et õigus isikuandmete kaitsele on nende põhiõigus. Magistritöö autorile teadaolevalt ei ole selliseid kodanikule suunatud sõnaselgeid teavitusi olnud. Eestis on Andmekaitse Inspektsioon korraldanud isikute informeerimise spetsiifiliste juhendite kaudu. Kõik juhendid isikuandmete kaitse valdkonna reguleerimiseks on toodud ära järelevalveasutuse koduleheküljel. Lisaks tegutseb Andmekaitse Inspektsioon aktiivselt ka sotsiaalmeedias, kus vastab isikute küsimustele ja jagab vajalikku infot seoses erinevatest postitustest tõusetunud küsimustega. Magistritöö autor toetab siinjuures andmekaitsereformiga esitatud ettepanekut tugevdada järelevalveasutuste

[219] Euroopa Liidu Põhiõiguste Amet (viide 215), lk 9.

volitusi. Järelevalveasutuse pädevus praegusel hetkel seisneb üldjuhul andmekaitserikkumiste heastamise nõudmistes või trahvide määramises, kuigi liikmesriigiti on järelvalveasutuste volitused erinevad. Isikuandmete kaitse üldmääruse jõustamine annaks Euroopa Liidu kõikide liikmesriikide järelevalveasutustele õiguse kohaldada halduskaristusi. Andmekaitserikkumiste korral eelistavad isikud kõige sagedamini pöörduda õiguskaitsevahendi taotlemiseks järelevalveasutuse poole, mistõttu peavad järelevalveasutused olema suutelised pakkuma tõhusat ja terviklikku teenust.[220] Eelnimetatule lisaks tuleb veel magistritöö autori hinnangul arvestada asjaolusid, et andmete hulgad kasvavad ja eksisteerib palju erinevaid andmetöötlusvõimalusi, mistõttu peab järelevalveasutustel olema ka reaalselt võimalik oma seadusest tulenevaid ülesandeid täita ja rikkumisi menetleda, sest andmekaitserikkumisi tänapäeva ühiskonnas on palju.

Euroopa Liidu Põhiõiguste Ameti poolt läbiviidud uuringu kohaselt ei tunne inimesed oma andmekaitsealaseid õiguseid. Selleks, et andmekaitsealase rikkumise korral oleks võimalik taotleda õiguskaitsevahendit, tuleb osata andmekaitsealased rikkumised ära tunda. Siinkohal olekski abistavaks vahendiks avalikkuse teavitamine inimeste õigusest andmekaitsele, selle õiguse rikkumiste iseloomust, õiguskaitsevahendi taotlemise mehhanismidest ning nende tõhusast kasutamisest.[221]

Magistritöö autor jõudis magistritöös järeldusele, et tehnoloogianeutraalsus seadustes on hea ja võimaldab ajaga kaasas käia. Tehnoloogianeutraalsus tähendab paindlikkust, mis seaduste puhul võimaldab normide kohaldamist sõltumata seejuures andmete töötlemiseks kasutatavast tehnoloogiast.

[220] *Op. Cit.,* lk 5.
[221] *Op. Cit*., lk 3.

Kokkuvõte

Vajadus tõhusate isikuandmete kaitse meetmete järele sündis üha populaarsust koguva IKT suureneva kasutusele võtmise tulemusena. Infoühiskonnas muutus hädavajalikuks tagada õigust eraelu puutumatusele, millele kujutas ohtu isikuandmete kuritarvitamine. Andmekaitseõiguse tähenduse muutumine ajas on muutnud ka traditsioonilist lähenemisviisi privaatsusõigusele.

Magistritöös analüüsis autor IKT-st tulenevaid andmekaitsealaseid õiguslikke aspekte infoühiskonnas eesmärgiga hinnata kehtivate õiguskaitsevahendite rakendatavust isikuandmete kaitse õiguse rikkumise korral. Andmekaitsealased rikkumised toimuvad tänasel hetkel valdavalt võrgukeskkonnas, sest internetis on saadaval tohutul hulgal informatsiooni, mis on kergesti kättesaadav, kasutatav, levitatav ja allalaaditav erinevatesse seadmetesse. Õigus isikuandmete kaitsele on Euroopa Liidus põhiõigus, mistõttu peavad kehtivad õiguslikud regulatsioonid pakkuma tõhusat kaitsevõimalust selle õiguse rikkumise korral.

Magistritöös püstitatud hüpoteesi kontrollimiseks analüüsis autor esmajärjekorras isikuandmete kaitse õiguse olemust, selle õiguse väljakasvamist privaatsusõigusest seoses IKT arenguga ning seejärel hetkel kehtivat andmekaitse valdkonna õiguslikku raamistikku. Hüpoteesi ümberlükkamiseks analüüsis magistritöö autor populaarsemaid andmetöötlustehnoloogiaid nagu asjade internet, suurandmed, profileerimine ja pilvetehnoloogiad ning nendest tulenevaid ohtusid isikuandmete kaitsele.

Magistritöös püstitatud esimesele uurimisküsimusele vastust otsides jõudis magistritöö autor järeldusele, et infoühiskonnas eksisteerivad isikuandmete kaitsega seonduvad õiguslikud probleemid on otseselt seotud järjepideva IKT arenguga. Uued tehnoloogiad õõnestavad andmetöötluse põhimõtteid, sest andmetöötlustoimingud ei ole läbipaistvad, eesmärgipärased, turvalised, kuid millele toetudes on üles ehitatud andmekaitseseadused. Tänapäeva andmetöötlustehnoloogiad võimaldavad koguda väga suures koguses andmeid ja neid erinevate tehnikatega töödelda, muutes andmetöötlustoimingud läbipaistmatuks ning andmetöötluse esialgseid eesmärke. Suurandmestik ei vasta andmekogumise minimaalsuse põhimõttele. Profileerimistoimingute puhul isikud ei teagi, et otsitakse vastust küsimusele: „Kes ta on?“. Anonümiseerimistehnikad ei loo enam inimeste usaldust, sest uued tehnoloogiad on teinud võimalikuks andmete taasisikustamise, mis on loonud olukorra, kus võrguühiskonnas ei ole võimalik enam anonüümseks jääda. Lisaks läbipaistvuse puudumisele

andmetöötluses on infoühiskonnas veel läbivaks märksõnaks isikuandmete kaitse valdkonnas kontrolli puudumine. Pilveteenuseid kasutades salvestatakse andmed pilve, mille üle omab täielikku kontrolli ainult teenusepakkuja, kellel on võimalik märkamatult pilve talletatud informatsiooniga manipuleerida, mistõttu ei ole võimalik kontrollida kes, mida ja millal andmetega teeb. Kontrolli kaotamine andmete üle on isikuandmete kaitses turvarisk, mis seab ohtu andmete käideldavuse, tervikluse ja konfidentsiaalsuse, mida rakendatavad turvameetmed peavad tagama. Lisaks vajavad vastamist veel küsimused, et millise riigi õigust vaidluse korral kohaldatakse ja millise riigi kohtus asi vaieldakse, sest moodne andmetöötlus ei tunne riigipiire.

Magistritööst selgus vastuseks teisele uurimisküsimusele, et objektiivsest õigusest tulenevad õiguskaitsevahendid isikuandmete kaitse tagamiseks ei peegelda adekvaatselt IKT arenguid, sest olemasolevad meetmed ei ole täielikult rakendatavad ja vajavad tõhustamist. IKT võimalused andmete töötlemiseks tõstsid isikuandmete kaitse olulisust, mistõttu hakati sellest õigusest rääkima kui privaatsusõigusest eraldiseisvast õigusest. IKT revolutsiooniline areng viis lõpuks isikuandmete kaitse õiguse põhiõiguseks tunnistamiseni. Magistritöös selgus, et inimesed ei tea oma andmekaitselisi õigusi ja ei tunne õiguskaitsevahendeid, mille rakendamist on võimalik rikkumiste korral taotleda. Kehtivad õigusinstrumendid sätestavad isiku õiguse tõhusale õiguskaitsevahendile. Kõige traditsioonilisem võimalus oma õiguste rikkumise korral on pöörduda kohtusse. Andmekaitse valdkonnas on tegutsevad ka järelevalveasutused, kes kodanikke oma õiguste kaitsmisel abistavad. Kuigi õigusaktid sätestavad isiku õiguse õiguskaitsevahendile, siis ei tähenda see veel seda, et õiguskaitsevahend isikule kättesaadav on. Magistritöös selgus, et menetlused on pikad ja kulukad ning valdkondlikku nõustamisteenust praktiliselt ei olegi, sest õigusspetsialistidel puuduvad süvateadmised andmekaitsest. Autor tõi magistritöös traditsiooniliste õiguskaitsevahendite kõrval välja ka mittetraditsioonilised meetmed, mida on võimalik isikuandmete kaitseks rakendada. Magistritöö autor nimetab alternatiivsete võimalustena eraelu puutumatust soodustavat tehnoloogiat, lõimitud andmekaitset ja iseregulatsiooni. Alternatiivsete meetmete kasutamiseks on kõik eeldused loodud, kuid praktikas ei ole need leidnud laialdast kasutust. Magistritöö autor toob välja iseregulatsiooni olulisuse andmekaitse valdkonna reguleerimisel andmekaitsedirektiivi kõrval direktiivi sätteid konkretiseerides. Iseregulatsiooni analüüsist selgub, et tegemist on suurepärase võimalusega IKT kui väga spetsiifilise valdkonna reguleerimiseks, mida tehnoloogianeutraalne ja abstraktselt sõnastatud õigusinstrument ei tee. Teadmist iseregulatsiooni kasutamise võimalustest on vaja ühiskonnas populariseerida. Kõiki reguleerimist vajavaid juhtusid ei ole võimalik ette näha, mistõttu ei

ole otstarbekas õigusinstrumenti ammendavalt kinni sõnastada. Abstraktne õigusinstrument jätab tõlgendamisruumi ja aitab kaasa pretsedendiõiguse arengule, mida tõestab juba ka olemasolev kohtupraktika.

Magistritöö autor leidis vastuseks magistritöös tõstatatud kolmandale uurimisküsimusele, et kvalitatiivsed muudatused kehtivates õigusinstrumentides on vajalikud vaatamata sellele, et kehtivad õigusinstrumendid andmekaitse valdkonnas on infoühiskonnas rakendatavad. OECD juhend eraelu kaitsest ja piiriülesest isikuandmete kaitsest on küll soovitusliku iseloomuga, mis ei vähenda selle juhendi olulisust, sest OECD juhendis sisalduvatest põhimõtetest on lähtutud andmekaitse valdkonna õiguslikul reguleerimisel. Konventsioon nr 108 on ainus rahvusvaheliselt siduv õigusinstrument andmekaitse valdkonnas ja vaatamata oma iganenud sõnastusele rakendatav profileerimistoimingutele. Direktiiv 95/46/EÜ seob liikmesriike saavutatava eesmärgi osas, sätestades minimaalsed reeglid andmekaitsele, võimaldades liikmesriikidel siseriiklike õigusaktidega kehtestada vajadustele vastavad nõuded isikuandmete kaitsele. See, et kehtivad õigusaktid on tehnoloogilises kontekstis rakendatavad, ei tähenda, et õigusaktides ei ole vaja teha sisulisi muudatusi isikute õiguste tugevdamiseks. Magistritöö autor toetab Euroopa Komisjoni ettepanekut kehtestada põhimõte, mille kohaselt uue tehnoloogia tootmisel tuleb arvestada eraelu puutumatusega. Kõik võimalused eraelu soodustava tehnoloogia kasutamiseks on loodud, kuid see on leidnud vähest kasutamist. Paraku vastava põhimõtte sätestamisel isikuandmete kaitse üldmääruses ei teki kohustust vaid jääb võimalus sellest põhimõttest tehnoloogia loomisel lähtuda. Nii on see ka seni olnud, olenemata sellest, et siiani ei olnud tegemist kirjutatud põhimõttega.

Olenemata sellest, et kehtiv õigusraamistik on isikute õiguste kaitseks rakendatav ka digimaailmas, toimub siiski tänasel hetkel Euroopas andmekaitse valdkonna reformimine. Kehtestatava isikuandmete kaitse üldmääruse üheks eesmärgiks andmekaitseõiguse harmoniseerimise kõrval on tugevdada isikute õiguseid eelkõige läbi sätete, mis tagavad isiku jaoks läbipaistva andmetöötluse ning õiguse olla unustatud. Magistritööst selgus, et olenemata uute õiguste kehtestamisest on andmekaitse rakendamine praktikas keerulisem kui teoorias. Seadusandja nägi küll ette IKT kiiret arengut ja sellega seotud internetikasutust, kuid mitte seda, et internet muutub selliseks globaalseks nähtuseks, mis võimaldab teha endas sisalduvast digitaliseeritud andmemassist üldist otsingut.

Vastates magistritöös esitatud neljandale uurimisküsimusele jõudis magistritöö autor vastuseni, mille kohaselt andmekaitseseadus peab IKT arengut toetama. Kuna isikuandmete

kaitse õigus on põhiõigus, siis seadus peab kaitsma isikut kui nõrgemat poolt, millele vastavalt on sõnastatud ka andmekaitseseaduste eesmärgid. Andmekaitse ei tohi saada takistuseks tehnoloogia innovatsioonile, kuid isikuandmete kaitset ei tohi ka ületähtsustada. IKT innovatsiooni toetab tehnoloogianeutraalne ja abstraktse sõnastusega seadus. Sellised paindlikud seadused võimaldavad kasutusele võtta uut tehnoloogiat, mis on ühiskonnas vajalik erinevate probleemide lahendamiseks, kuid samas ei tohi jätta tähelepanuta andmekaitse reegleid, mis on vajalikud isikute õiguste tagamiseks. Magistritöö autor leidis, et praegu kehtivad õiguslikud regulatsioonid on piisavalt üldised, et neid on võimalik kohaldada tehnoloogilises kontekstis. Magistritöö autori hinnangul ongi tõenäoliselt 1995. aastast pärit andmekaitsedirektiiv just seetõttu nii kaua muutumatul kujul püsinud ja ainult tehnoneutraalne isikuandmete kaitse regulatsioon võimaldab õigusel infoühiskonnas tehnoloogia arenguga sammu pidada. Magistritöö autor on magistritöös korduvalt rõhutanud, et andmekaitse regulatsioon ei saa olla detailne ja ammendav ning käsitleda ainult konkreetsel ajahetkel moodsast tehnoloogiast tulenevaid aktuaalseid probleeme. Kuna õigusloome protsess on väga aeglane, siis peab õigusinstrument olema kohaldatav pikaaegselt kiiresti muutuvates aja ja ruumi tingimustes. Magistritöö autor on seisukohal, et vajadust „uue õiguse“ järele enam ei eksisteeri, sest see on juba sündinud. Ühiskonna liikmed on selle ise oma käitumisega kujundanud, vaikimisi omaks võtnud ja rakendama asunud.

Magistritöö autor on seisukohal, et magistritöös püstitatud hüpotees ei leia täiel määral kinnitust. Kehtiv andmekaitse õiguslik regulatsioon nii rahvusvahelisel, Euroopa Liidu kui siseriiklikul tasandil omab teatavaid puuduseid, kuid on siiski rakendatav ja täidab oma eesmärki, milleks on kaitsta isiku põhiõiguseid ja –vabadusi, eelkõige õigust eraelu puutumatusele. Andmekaitse seaduste puudused seisnevad selles, et seadusandja ei olnud võimeline ette nägema andmete hulga ja selle töötlemise võimaluste muutust sellises ulatuses, mille tegi võimalikuks info- ja kommunikatsioonitehnoloogia. Seadusandja aga oli piisavalt tark, et nähes arvutite ja interneti kasvavat kasutust, koostas abstraktse õigusakti andmekaitsedirektiivi näol, millele andis laia esemelise kohaldamisala eesmärgiga jõuda järele tehnoloogia arengule. Põhimõistete nagu „isikuandmed“, „isikuandmete töötlemine“ jmt määratlused ei ole ammendavad ja seoses tehnoloogia arenguga hõlmavad uusi tähendusi. 20 aastat tagasi ei oleks keegi arvanud, et IP-aadressid on isikuandmed, kuid pea 20 aastat tagasi vastuvõetud seadus võimaldab kohaldada IP-aadressile isikuandmete mõistet, tagades sellega isikule kaitse tema õiguste rikkumise korral.

Magistritöö autor toetab andmekaitse valdkonnas levinud seisukohta, et andmekaitse peab teooriast praktikasse liikuma ja on ise valmis sellesse oma töö kaudu panustama. Selleks, et praktika sünniks, on meil vaja spetsialiste, kes oskaksid andmekaitseõigust rakendada ja õiguskaitsevahendite kättesaadavust isikuteni viia. Magistritööst selgus, et õigusspetsialistidel, sh kohtunikel, puuduvad süvendatud teadmised andmekaitseõigusest, mistõttu on vaja võimalusi vastavate oskuste ja kogemuste omandamiseks. Magistritöö autor tegi magistritöös ettepaneku, et IT spetsialistidele tuleb pakkuda süvendatud õigusharidust, eelkõige andmekaitseõiguse valdkonnas, arvestades andmekaitse ja tehnoloogia lahutamatuid seoseid. Magistritöö autor põhimõtteliselt toetab andmekaitsereformi ettepanekuid, lootes, et need täidavad oma eesmärki tagada isikute põhiõiguste ja –vabaduste kaitse. Seadusandja ei saa koostada detailseid ja ammendavaid õiguslikke regulatsioone, järgimata tehnoneutraalsuse printsiipi, mis magistritöö autori arvates välistaks õigusakti kohaldatavuse tulevikus ning seda eriti isikuandmete kaitse valdkonnas, mis on tehnoloogia poolt eriti tugevalt mõjutatud. Seadusandja peab uutest tehnoloogiatest tulenevatele riskidele põhjalikku tähelepanu pöörama, sest laiemas mõttes kujutab IKT ohtu põhiseaduslikele väärtustele, eelkõige õigusriigi põhimõttele. Demokraatia riigivalitsemise vormina on ohus, sest valitsused omavad inimeste kohta palju andmeid, millega on võimalik manipuleerida. Info- ja kommunikatsioonitehnoloogia kätkeb endas väga palju erinevaid ohtusid, mille realiseerumise maandamiseks tuleb ette näha tõhusad meetmed.

Arvestades tehnoloogia iseloomu, millest tulenevalt on tehnoloogia võimeline nii mõneski tegevuses inimest asendama, peaks magistritöö autori arvates õiguse loomine siiski inimestele jääma, seda ka juhul kui tehnoloogia ise on kunagi tulevikus võimeline õigust looma. Nii tehnoloogia kui ka õigus on teadused, mis ajaga aina arenevad. Selge on, et tehnoloogia ja õiguse areng ei toimu samal kiirusel, kuid ideaalne oleks selline areng, kus üks oleks võimeline teist ette nägema. Albert Einstein on teadust iseloomustanud järgmiselt: „Teadus ei ole ega hakkagi kunagi olema lõpetatud raamat. Iga tähtis edu toob endaga kaasa uusi küsimusi. Iga areng toob aja jooksul nähtavale üha uusi ja suuremaid raskusi.“. Magistritöö autori hinnangul iseloomustab eeltoodud ütlus väga tabavalt nii tehnoloogiat kui ka õigust.

Implementation of taditional legal remedies of providing the right to the protection of personal data in information society and about their potential developments. Summary

Today peole are living in a world named information society and they can not imagine their lives without digital devices and Internet. The creation of information society was caused of the rapid growth of usage of new information and communication technology (ICT). New technology is having an effect on modern society and social behaviour through considerable benefits to the users. But there are also risks in ICT world that needs to be taken into consideration. Development of ICT have made possible to collect, use and transfer personal data in automated way and in large sets. Processing of personal data both in public and private sector may violate fundamental rights, especially the right to private life. Data protection is regarded as the field with high legal risks in consideration of innovative level of ICT, activities in the Internet and the fact that directive 96/46/EC dates back to the year 1995. Nowadays personal data is a relevant asset which needs legal protection. Rapid development of information society has raised the question – can data protection legislation keep up with development of ICT?

Estonia have had a great success in the field of imposing ICT. Estonia have earned a name of e-state with digital signature, eID, mobile-ID etc. The latest accomplishment is the programm of e-residency that has brought the worldwide fame to Estonia. The legislation of personal data protection affects Estonia in many ways and therefore is essential that it is applicable. Estonia is a full member of EU and must comply with national legislation with the legislation of EU. Estonia has ratified the Convention for the Protection of Human Rights and Fundamental Freedoms and the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention no 108) and therefore these instruments are legally binding for Estonia. Membership of OECD makes OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data recommendable for Estonia.

The purpose of thesis is to estimate if valid legal remedies of data protection can actually be applied in case of violations of personal data protection rules and the possible need for new legal remedies to protect personal data as a fundamental asset in information society. The author of thesis draws a conclusion if there is a need for „new law“.

The author of thesis is of the opinion that law can not be outdated and must stand up to the challenges of innovative technology. The author set the hypothesis that valid legal remedies

securing the right to the protection of personal data as fundamental right can not be substantially implemented in modern information society. The author sets the following research questions:

1) What legal questions related to personal data protection can be associated with the development of ICT in digitalized world?
2) Do the legal remedies providing personal data protection arising from the objective law reflect adequately the progress of ICT?
3) If qualitative amendments are nessecary in legal remedies providing personal data protection?
4) How personal data protection should be regulated in modern information society?

In the first chapter author gives an overview how ICT have influenced the right to the protection of personal data. The author turns back to the history of data protection and observes the course to present day and the relationship between the concepts of right to the respekt for private life and the right to the protection of personal data. The author refers to the guaranty of personal data protection deriving from international, European Union (EU) and national law. The author also mentions EU data protection reform in thesis from the aspect of providing legal measures to protect fundamental rights. First chapter ends with conclusion whether valid legal remedies are efficient enough to protect personal data in the world of ICT.

The second chapter focuses on technology world. The author analyses if reality corresponds to the needs of future indicating to the personal data protection problems arising from the usage of ICT. The author focuses on for technological trends in data processing called cloud computing, big data, profiling and internet of things. The author points out how aforementioned technology is related to personal data and what kind of risks they implicate to the personal data protection. The author brings to notice to the alternative measures beside legislation.

The third chapter is about the analysis of the need of new personal data protection regulation relying on conclusions made in first two chapters of thesis. The author also points out the perspectives of personal data protection in the light of ICT progression.

The author of thesis concludes that set hypothesis is not fully confirmed according to the found answers to research questions. The author concludes that legal problems of personal data protection are strongly connected with the consistent development of ICT. New ICT

undermines the core principles of data processing by altering procedures less transparent, purposeful and secure. Big data is not conforming to the principle of minimalisation. In case of profiling person does not even know that his or her personal data is processed and someone is searching answer to the question: „Who he or she is?“. Anonymisation technique creates no trust because new technology have made possible deidentification – there is no anonymity in networked society. Valid data protection regulation is based on data processing principles and therefore their nature can not be transformed. Besides transparency questions there are discussion about lack of control over data in information society. Using cloud services and storing data in the cloud person loses control over his or her data because the service provider has full power and has possibilities to manipulate with data unknowingly. In addition there are questions about the applicable law and jurisdiction that need to be answered in networked society because modern data processing do not acknowledge state borders.

The author of thesis concludes that legal remedies of providing personal data protection arising from the objective law do not reflect adequately the progress of ICT because existing measures can not be fully applied and need to be supplemented. Development of ICT increased the importance of personal data protection which lead to the recognition of fundamental right. Personal data protection was no more part of privacy right but totally separate fundamental right. The thesis concludes that people do not know their right of data protection as they do not know the legal remedies which can be applied for in case of breaches. Valid legal instruments stipulate the right to effective legal remedy. The most traditional way is to turn to the court. There are data protection institutions who are obliged to perform supervision over fulfilment of data protection rules in national states. Data protection institutions help people to exercise their rights.The existance of legal remedies in legal instruments does not mean that they are available to people. The thesis concluded that proceedings are long and expensive. There is practically no consultation service in the field of data protection because law specialists do not have deep knowledge of data protection related to ICT.

Beside traditional remedies the author of thesis points out nontraditional measures to use for data protection. The alternatives are privacy enhancing technology, privacy by design and self-regulation. Aforementioned are not new measures but they have not found widespread use. The author concludes that self-regulation could very effectively regulate such specific are as data protection related to ICT because the directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the

processing of personal data and on the free movement of such data (directive 95/46/EC) is technology-neutral and abstract legal instrument. Popularising the use of self-regulataion it could turn out to be very effective in daily basis.

The author of thesis concludes that qualitative amendments are nessecary in legal remedies despite of valid legal instruments are applicable to provide personal data protection. OECD Guidelines are recommendable but it does not decrease the importance of the document. Convention no 108 is only legally binding international instrument but despite of outdated wording still applicabe even in case of profiling proceedings. If legal instruments are applicable in the context of technology it does not mean yet that legal instruments do not need amending to provide more effective protection. The author supports the propasal of European Comission to stipulate the principle of privacy enhancing technology in General Data Protection Regulation (GDPR) though it does not oblige but creates a possibility. The aforementioned principle have been existing in practice before but unwrittenly.

As the author of thesis concludes that valid legal instruments are applicable to provide protection against personal data violations in digitalized world. But still there is data protection reform in progress in EU. The purpose of GDPR is to harmonize data protection law and to strengthen the rights of person above all through providing transparent data processing and the right to be forgotten. The thesis concludes that despite of strengthening persons rights data protection in practice is still more complicated than in theory. The legislator did forsee the rapid development of ICT and widespread use of Internet but did not forsee the fact of Internet changing to global phenomenon that allows to perform general search from digital data mass Internet consists of.

The author of thesis concludes that data protection law must support the progress of ICT. Though the right to the protection of personal data is fundamental right then law must protect the person as a weaker party according to the formed data protection purposes. Data protection can not impede the innovation of technology but it also can not be overemphasized. Technology innovation is supported by tecnology-neutral and abstract laws wich means flexibility. Flexible laws enable implement new tchnology needed in society to solve easily different problems. The author concludes that directive 95/46/EC have been so enduring due to the aforementioned reasons and only technology-neutral law makes possible to keep pace with the progress of technology. The author is of the opinion that there is no need for „new law“ in information society because it is already here.

The author of thesis concludes that set hypothesis is not fully confirmed. There are some shortage in valid legal data protection framework but the instruments are still serving the purpose to protect fundamental rights of individuals. Shortcomings of data protection laws are about legislators ability not to forsee the change of data amount and different processing techniques within the scope caused by development of ICT. But seeing the widespread use of computers and internet the legislator was smart enough to enact a legal instrument such as directive 95/46/EC with very wide scope of application to catch up with progress of technology. Basic terms in data protection such as „personal data“ and „data processing“ are not defined exhaustively and have aquired new meanings due to the development of ICT. Almost 20 years ago nobody would have guessed that one day IP address could be treated as personal data as it is done today.

The author of thesis supports the widespread opinion that data protection must move from theory to practice. Society needs data protection specialist with experience who know how to implement the law and how to make legal remedies available to individuals. The thesis concludes that specialists and judges do not have deep knowledge and experience of personal data protection and therefore possibilites are needes to gain such knowledge and experience. The author of thesis proposes to provide comprehensive law education to IT specialists. Educating law specialist in the area of IT is not enough anymore in consideration of the link between data protection and ICT.

The thesis concludes that technology-neutral laws are good. Exhaustively formed legal instruments would not be applicable in future and probably would need amending but legislation is long lasting procedure. Legislator must turn attention to the risks arising from new technology which deeply influences fundamental values, especially the rule of law. Democracy is also in danger because goverments are holding huge amounts of personal data which could be manipulated. Because of the wide range of possible risks there must be very effective measures ro prevent the risks from becoming real.

Kasutatud allikate loetelu

Kasutatud kirjandus:

1. Adler, J. When Self-Regulation Works, Your Privacy Is In Good Hands. Arvutivõrgus: http://www.truste.com/blog/2012/07/27/when-self-regulation-works-your-privacy-is-in-good-hands/, 16.03.2015.
2. Alexy, R. Põhiõigused Eesti Põhiseaduses. - Juridica 2001/eriväljaanne.
3. Buitelaar, J. C. Privacy: Back to the Roots. – German Law Journal 2012, nr 13 (3).
4. Bygrave, L. A. Data Protection Pursuant to the Right to Privacy in Human Right Treaties.- International Journal of Law and Information Technology 1998, nr 6 (3).
5. Cavoukian, A. Privacy by Design. The 7 Foundational Principles Arvutivõrgus: https://www.ipc.on.ca/images/resources/7foundationalprinciples.pdf, 15.03.2015.
6. Cukier, K., Mayer-Schoenberger, V. The Rise of Big Data. How It's Changing the Way We Think About the World. – Foreign Affairs 2013, nr 92 (3).
7. Cunningham, M. Next Generation Privacy: The Internet of Things, Data Exhaust, and Reforming Regulation by Risk of Harm. – Groningen Journal of International Law 2014, nr 2 (2).
8. De Filippi, P., Belli, L. Law of the Cloud v Law of the Land: Challenges and Opportunities for Innovation. – European Journal of Law and Technology 2012, nr 2 (2).
9. DeVries, W. T. Protecting Privacy in the Digital Age. – Berkeley Technology Law Journal 2014, nr 18 (1).
10. Ferraris, V., Bosco, F., D'Angelo, E. The impact of profiling on fundamental rights. Arvutivõrgus: http://www.unicri.it/special_topics/citizen_profiling/PROFILINGproject_WS1_Fundamental_1110.pdf, 02.03.2015.
11. Fuster, G. G. The Emergence of Personal data Protection as a Fundamental Right of the EU. Switzerland: Springer International Publishing 2014.
12. Garson, G. D. Public Information Technology and E-Governance: Managing the Virtual State. London: Jones and Barlett Publishers International 2006.
13. Gutwirth, S., Leenes, R., De Hert, P. (edit) Reforming European Data Protection Law. Dordrecht: Springer 2015.
14. Gutwirth, S., Leenes, R., De Hert, P., Pullet, Y. (edit). European Data Protection: In Good Health?. Dordrecht: Springer 2012.

15. Hornung, G. Regulating privacy enhancing technologies: seizing the opportunity of the futuure European Data Protection Framework. – The European Journal of Social Science Research 2013, nr 26.
16. Hustinix, P. J. Co-regulation or self-regulation by publik and private bodies – the case of data protection. Freundesgabe Büllesbach 2002. Arvutivõrgus: http://www.alfred-buellesbach.de/PDF/27_Hustinx.pdf, 16.03.2015.
17. Ilus, T. Isikuandmete kaitse olemus ja arengusuunad. – Juridica 2002, nr 7.
18. Ilves, T. H. Kõne demokraatiaorganisatsiooni NDI 30. aastapäeva auhinnadineel Washingtonis 10. detsembril 2013. Arvutivõrgus: http://president.ee/et/ametitegevus/koned/9712-2013-12-17-13-28-46/index.html, 26.01.2014.
19. Kohnstamm, J. Mauritius Declaration on the Internet of Things. Arvutivõrgus: http://www.privacyconference2014.org/media/16421/Mauritius-Declaration.pdf, 04.03.2015.
20. Kokott, J., Sobotta, C. The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR. – International Data Privacy Law 2013, nr 3 (4).
21. Koops, B.-J. The trouble with European data protection law. – International Data Privacy Law 2014, nr 4 (4).
22. Kotschy, W. The proposal for a new General Data Protection Regulation – problems solved? – International Data Privacy Law 2014, nr 4 (4).
23. Kuner, C. Privacy, Security and Transparency: Challenges for Data Protection Law in a New Europe. Hague: Kluwer Law International 2005.
24. Kuner, C. European Data Protection Law. Corporate Compliance and Regulation. Second edition. Oxford: Oxford University Press 2011.
25. Kuner, C. The European Union and the Search for an International Data Protection Framework. – Groningen Journal of International Law 2014, nr 2 (1).
26. Lloyd, I. J. Information Technology law. 6th edition. New York: Oxford University Press 2011.
27. Mearian, L. No, your data isn't secure in the cloud. Arvutivõrgus: http://www.computerworld.com/article/2483552/cloud-security/no--your-data-isn-t-secure-in-the-cloud.html, 02.03.2015.
28. Mendel, T. The Public's Right to Know. Principles on Freedom of Information Legislation. – London: Article 19, 1999. Arvutivõrgus: http://www.article19.org/data/files/pdfs/standards/righttoknow.pdf, 05.02.2014.

29. Michael, K., Miller, K. W. Big Data: New Opprtunities and New Challenges. – IEEE Security & Privacy. IEEE Computer Society 2013.
30. Miller, J., Hoffman, D. Sponsoring trust in tomorrow's technology: towards a lobal digital infrastructure policy. - International Data Privacy Law 2011, nr 1(2).
31. Rees, C., Chalton, S. Database Law. Bristol: Jordan Publishing Limited, 1998.
32. Reno, J. Big Data, Little Privacy. – CA Technology Exchange. Insights from CA Technologies. Ameerika Ühendriigid: 2012 nr 3 (2).
33. Rodota, S. Case studies on data protection. Arvutivõrgus: http://www.ictparliament.org/sites/default/files/1pf_RodotaCaseStudies.pdf, 07.03.2015.
34. Rohtmets, E. Riigikohtu analüüs isikuandmete kaitse kohta Euroopa Kohtu eelotsustes. Tartu: 2013.
35. Ruback, T. A Brief Look at Self-Regulation and European Data Protection. Arvutivõrgus: https://privacyassociation.org/news/a/a-brief-look-at-self-regulation-and-european-data-protection/, 16.03.2015.
36. Rubinstein, I. S. The End of Privacy or a New Beginning? – International Data Privacy Law 2013, nr 3(2).
37. Ruiz, B. R. Privacy in Telecommunications. A European and an American Approach. Hague: Kluwer Law International 2005.
38. Romano, F. B. The Right to the Protection of Personal Data: A New Fundamental Right of the European Union. Rooma: 2013. Arvutivõrgus: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2330307, 22.03.2015.
39. Senden, L. Soft-law, self-regulation and co-regulation in European law: Where Do They Meet? – Electronic Journal of Comparative Law 2005, nr 9.1.
40. Teder, I. Kas soovime suletud ühiskonda? Postimees 7.06.2012. Arvutivõrgus: http://arvamus.postimees.ee/868200/indrek-teder-kas-soovime-suletud-uhiskonda, 05.02.2014.
41. Tene, O. Polonetsky, J. Privacy in the Age of Big Data: A Time for Big Decisions. – Stanford Law Review Online. 2012, nr 64(63). Arvutivõrgus: http://www.stanfordlawreview.org/sites/default/files/online/topics/64-SLRO-63_1.pdf, 15.03.2014.
42. Tikk, E., Nõmper, A. Informatsioon ja õigus. Tallinn: Juura 2007.
43. Truuväli, E.-J. jt (toim). Eesti Vabariigi põhiseadus. Komm vlj. 2. vlj. Tallinn: Juura 2012.

44. Tzanou, M. Data Protection as a fundamental right next to privacy? 'Reconstructing' a not so new right. – International Data Privacy Law 2013, nr 3 (2).
45. Waschke, M. Introduction to the Big Data. - CA Technology Exchange. Insights from CA Technologies. Ameerika Ühendriigid: 2012, nr 3 (2).

Kasutatud õigusaktid:

46. Avaliku teabe seadus. - RT I 2000, 92, 597 … RT I, 12.07.2014, 33.
47. Eesti infopoliitika põhialused. – RT I 1998, 47, 700.
48. Eesti Vabariigi põhiseadus. – RT 1992, 26, 349 … RT I, 27.04.2011, 2.
49. Elektroonilise side seadus. – RT I 2004, 87, 593 … RT I, 30.12.2014, 7.
50. Euroopa andmekaitseinspektori arvamus, mis käsitleb usalduse suurendamist infoühiskonnas andmekaitse ja eraelu puutumatuse tugevdamise kaudu. – ELT C 280/01, 16.10.2010.
51. Euroopa Liidu põhiõiguste harta. - ELT C 83, 30.03.2010.
52. Euroopa Parlamendi ja nõukogu 24.10.1995. a direktiiv 95/46/EÜ üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta, EÜT L 281, 23.11.1995.
53. Euroopa Parlamendi ja nõukogu 12.07.2002. a direktiiv 2002/58/EÜ, milles käsitletakse isikuandmete töötlemist ja eraelu puutumatuse kaitset elektroonilise side sektoris (eraelu puutumatust ja elektroonilist sidet käsitlev direktiiv), EÜT L 201, 31.07.2002.
54. Euroopa Parlamendi ja nõukogu 15.03.2006. a direktiiv 2006/24/EÜ, üldkasutatavate elektrooniliste sideteenuste või üldkasutatavate sidevõrkude pakkujate tegevusega kaasnevate või nende töödeldud andmete säilitamist ja millega muudetakse direktiivi 2002/58/EÜ, EÜT L 105/54, 13.04.2006.
55. Inimõiguste ja põhivabaduste kaitse konventsioon. - RT II 2010, 14, 54.
56. Isikuandmete automatiseeritud töötlemisel isiku kaitse konventsioon. - RT II 2001, 1, 3.
57. Isikuandmete kaitse seadus. - RT I 1996, 48, 944 … RT I 1998, 59, 941.
58. Isikuandmete kaitse seadus . – RT I 2007, 24, 127… RT I 30.12.2010, 11.
59. Kodaniku- ja poliitiliste õiguste rahvusvaheline pakt. – RT II 1994, 10, 11.

Kasutatud kohtupraktika:

60. EKo 16.12.2008, C-524/06, *Heinz Huber v* Saksamaa.
61. EKo 08.04.2014, C-293/12 ja C-594/12, *Digital Rights Ireland Ltd jt. v* Iirimaa.

62. EKo 13.05.2014, C-131/12, *Google Spain jt. v Agencia de Protectíon de Datos jt*.
63. EIKo 02.08.1984, 8691/79, *Malone v The United Kingdom.*
64. EIKo 26.03.1987, 9248/81, *Leander v Sweden.*
65. EIKo 07.07.1989, 10454/83, *Gaskin v The United Kingdom.*
66. EIKo 16.12.1992, 13710/88, *Niemietz v* Saksamaa.
67. EIKo 25.03.1998, 13/1997/797/1000, *Kopp v* Šveits.
68. EIKo 16.02.2000, 27798/95 *Amann v* Šveits.
69. EIKo 04.05.2000, 28341/95, *Rotaru v* Rumeenia.
70. EIKo 06.05.2001, 44599/98, *Bensaid v* Ühendatud Kuningriigid.
71. EIKo 25.09.2001, 44787/98, *P. G. and J. H. v* Ühendatud Kuningriigid.
72. RKHKo 3-3-1-3-12.
73. RKPJKo 3-4-1-5-94.
74. RKPJKo 3-4-1-1-03.
75. RKÜKo 3-4-1-6-12.

Muud allikad:

76. Andmekaitse Inspektsioon. Pilvandmetöötlus. Arvutivõrgus: http://www.aki.ee/et/pilvandmetootlus, 06.02.2015.
77. Article 29 Data Protection Working Party. Opinion 8/2014 on the Recent Developments on the Internet of Things. WP223. Brussels: 16.09.2014. Arvutivõrgus: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf, 05.02.2014.
78. Artikli 29 alusel asutatud andmekaitse töörühm. Arvamus nr 05/2014 anonüümimistehnikate kohta. WP216. Brüssel: 10.04.2014. Arvutivõrgus: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_et.pdf, 15.03.2014.
79. Artikli 29 alusel loodud andmekaitse töörühm. Arvamus 05/2012 pilvandmetöötluse kohta. WP196. Brüssel: 01.07.2012. Arvutivõrgus: http://ec.europa.eu/justice/data-protection/article29/documentation/opinionrecommendation/files/2012/wp196_et.pdf#h2-2, 27.02.2014.
80. EDRI. Privacy International, UK. An introduction to Data Protection. The European Digital Rights papers 2013, nr 6. Arvutivõrgus: https://edri.org/files/paper06_datap.pdf, 01.03.2015.
81. Ernst & Young Global Limited. Privacy trends 2014. Privacy protection in the age of technology. Arvutivõrgus: http://www.ey.com/Publication/vwLUAssets/EY_-

_Privacy_trends_2014:_Privacy_protection_in_the_age_of_technology/$FILE/EY-Insights-on-GRC-Privacy-trends-2014.pdf, 05.02.2015.

82. EU network of indipendent experts on fundamental rights. Commentary of the Charter of Fundamental Rights of the EU. Arvutivõrgus: http://ec.europa.eu/justice/fundamentalrights/.../networkcommentaryfinal_en.pdf, 22.03.2015.
83. Euroopa Komisjon. Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments. Arvutivõrgus: http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_en.pdf, 15.03.2015.
84. Euroopa Komisjon. EU study on the Legal analysis of a Single Market for the Informatsion Society. Privacy. The future of online privacy and data protection. Arvutivõrgus: http://ec.europa.eu/information_society/newsroom/cf/newsletter-item-detail.cfm?item_id=7022, 07.03.2015.
85. Euroopa Komisjoni teatis Euroopa Parlamendile ja nõukogule. Usalduse taastamine EL-is Ameerika Ühendriikide vaheliste andmevoogude vastu. KOM (2013) 846 (lõplik). Brüssel: 27.11.2013 Arvutivõrgus: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2013:0846:FIN:ET:PDF, 09.03.2014
86. Euroopa Komisjoni teatis Euroopa Parlamendile ja nõukogule. Euroopa digitaalne tegevuskava. KOM (2010) 245 (lõplik). Brüssel: 19.05.2010. Arvutivõrgus: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:ET:PDF, 09.03.2014.
87. Euroopa Komisjoni teatis Euroopa Parlamendile ja nõukogule. Eraelu puutumatuse kaitsmine ühendatud maailmas. Euroopa isikuandmete kaitse raamistik 21. sajandil. KOM (2012) 9 (lõplik). Brüssel: 25.01.2012. Arvutivõrgus: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0009:FIN:ET:PDF, 09.03.2014.
88. Euroopa Komisjon. Komisjoni talituste töödokument. Mõjuhinnangu kommenteeritud kokkuvõte. SEK (2012) 73 (lõplik). Brüssel: 25.01.2012. Arvutivõrgus: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=SEC:2012:0073:FIN:ET:PDF, 10.03.2014.
89. Euroopa Komisjon. Kuidas kohandatakse ELi reformiga andmekaitse-eeskirju uue tehnoloogilise arenguga? Arvutivõrgus: http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/8_et.pdf, 27.03.2015.

90. Euroopa Nõukogu Parlamentaarse Assamblee resolutsioon nr 1165 (1998) Right to privacy. - In view of the new communication technologies which make it possible to store and use personal data, the right to control one's own data should be added to this definition. Arvutivõrgus kättesaadav: http://assembly.coe.int/main.asp?Link=/documents/adoptedtext/ta98/eres1165.htm, 09.03.2015.
91. Euroopa Liidu Põhiõiguste Amet. Juurdepääs andmekaitse õiguskaitsevahenditele Euroopa Liidu liikmesriikides. Kokkuvõte. Arvutivõrgus: http://bookshop.europa.eu/et/juurdepaeaes-andmekaitse-iguskaitsevahenditele-euroopa-liidu-liikmesriikides-pbTK0113752/downloads/TK-01-13-752-ET-C/TK0113752ETC_002.pdf?FileName=TK0113752ETC_002.pdf&SKU=TK0113752ETC_PDF&CatalogueNumber=TK-01-13-752-ET-C, 30.03.2015.
92. Euroopa Liidu Põhiõiguste Amet. Kodanikud vajavad tõhusat ja kättesaadavat kaitset andmekaitse seaduste rikkumise eest. Arvutivõrgus : http://fra.europa.eu/sites/default/files/fra_press_release_data_protection_remedies_report_et.pdf, 14.03.2015.
93. Euroopa Liidu Põhiõiguste Amet ja Euroopa Nõukogu. Euroopa andmekaitseõiguse käsiraamat. Luxembourg: Euroopa Liidu Väljaannete Talitus 2015.
94. Euroopa Ühenduste Komisjoni teatis Euroopa Paramendile ja nõukogule andmekaitse edendamise kohta eraelu puutumatust soodustavate tehnoloogiate kaudu. KOM(2007) 228 lõplik. Brüssel: 2.5.2007 Arvutivõrgus: http://ec.europa.eu/transparency/regdoc/rep/1/2007/ET/1-2007-228-ET-F1-1.Pdf, 15.03.2015.
95. Euroopa Ühenduste Komisjoni soovitus eraelu puutumatuse ja andmekaitse põhimõtete kohaldamise kohta raadiosagedustuvastust kasutavates rakendustes. (K(2009) 3200 (lõplik)). Brüssel: 12.5.2009. Arvutivõrgus: http://www.europarl.europa.eu/RegData/docs_autres_institutions/commission_europeenne/sec/2009/0586/COM_SEC(2009)0586_ET.pdf, 15.03.2015.
96. Euroopa Ülemkogu järeldused, milles keskendutakse digitaalmajandusele, innovatsioonile ja teenustele ning rõhutatakse ühtse digitaalse turu välja kujundamise vajadust. EUCO 169/13. Brüssel: 25.10.2013. Arvutivõrgus: http://www.riigikogu.ee/?op=emsplain&page=pub_file&file_id=5e49dedb-09a1-479b-acbf-09ef47bf0897&., 08.03.2014.

97. FRA. Twelve operational fundamental rights considerations for law enforcement with processing PNR data. Arvutivõrgus: http://fra.europa.eu/sites/default/files/fra-2014-fundamental-rights-considerations-pnr-data-en.pdf, 21.03.2015.
98. Isikuandmete kaitse seaduse seletuskiri. Arvutivõrgus: http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/IKS%20SELETUSKIRI%20(1).rtf, 10.03.2015.
99. Isikuandmete kaitse üldmääruse seletuskiri. Arvutivõrgus: http://ec.europa.eu/justice/dataprotection/document/review2012/com_2012_11_et.pdf, 18.03.2015.
100. Majandus- ja kommunikatsiooniministeerium. Eesti infoühiskonna arengukava 2020. Arvutivõrgus: http://www.riso.ee/sites/default/files/elfinder/article_files/infoyhiskonna_arengukava_2020_f.pdf, 03.03.2015.
101. OECD. The OECD privacy framework. Arvutivõrgus: http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf, 14.03.2015.
102. Rahvusvaheline telekommunikatsiooni andmekaitse töörühm. Pilvandmetöötlus: eraelu puutumatuse ja andmekaitse probleemid - „Sopoti memorandum". Arvutivõrgus: http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/Pilvandmet%C3%B6%C3%B6tlus%20-%20Sopoti%20memorandum.pdf, 27.02.2014.
103. Riigipiiri seaduse, tolliseaduse ning politsei ja piirivalveseaduse muutmise seaduse eelnõu seletuskiri. Arvutivõrgus: http://www.riigikogu.ee/?op=emsplain&page=pub_file&file_id=ba652ab6-5f14-461c-8724-effb4e6e5e8d&, 22.03.2015.
104. Tallinna Tehnikaülikool. Arenguanalüüs „IKT TTÜ tasemeõppes". Arvutivõrgus: http://www.ttu.ee/IKT-uuring/, 18.02.2014.
105. Õiguskantsleri 05.03.2015 märgukiri nr 6-2/141070/1501002 Siseministeeriumile. Isikut tõendavate dokumentide andmekogu põhimääruse § 18 põhiseaduspärasus. Arvutivõrgus: http://oiguskantsler.ee/sites/default/files/field_document2/6iguskantsleri_margukiri_isikuandmete_sailitamise_tahtaeg.pdf, 13.03.2015.
106. Ühinenud Rahvaste Organisatsioon. Inimõiguste ülddeklaratsioon. Arvutivõrgus: http://www.un.org/en/documents/udhr/, 14.03.2015.

Lihtlitsents lõputöö reprodutseerimiseks ja lõputöö üldsusele kättesaadavaks tegemiseks

Mina Merike Küngas (sünnikuupäev: 29.03.1982)

1. annan Tartu Ülikoolile tasuta loa (lihtlitsentsi) enda loodud teose „Traditsiooniliste õiguskaitsevahendite rakendatavus isikuandmete kaitse õiguse tagamisel infoühiskonnas ja nende võimalikest arengutest“, mille juhendaja on Raul Narits,

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, 04.05.2015.