TALLINNA TEHNIKAÜLIKOOL

Majandusteaduskond

Õiguse instituut

Elizabeth Laan

ISIKUANDMETE KAITSE ÜLDMÄÄRUSE ÜHTLUSTAMINE ISIKUTE PÕHIÕIGUSTEGA

Magistritöö

Eesti avalik ja eraõigus

Juhendaja: Sandra Särav, MA

Tallinn 2018

Deklareerin, et olen koostanud töö iseseisvalt ja
olen viidanud kõikidele töö koostamisel kasutatud
teiste autorite töödele, olulistele seisukohtadele ja andmetele,
ning ei ole esitanud sama tööd varasemalt ainepunktide saamiseks.
Töö pikkuseks on ..... sõna sissejuhatusest kuni kokkuvõtte lõpuni.

Elizabeth Laan ..... (allkiri, kuupäev)

Üliõpilase kood: 162703 HAJM
Üliõpilase e-posti aadress: elizabethlaan@gmail.com

Juhendaja: Sandra Särav, MA: Töö vastab kehtivatele nõuetele

..... (allkiri, kuupäev)

SISUKORD

LÜHIKOKKUVÕTE

Antud magistritöö eesmärgiks on uurida uut andmekaitse üldmäärust, mis muutub kohaldatavaks 2018. aasta maist ning anda ülevaade uutest muudatustest üldmääruses võrreldes eelnevalt kehtinud ning tänapäevaks kehtivuse kaotanud andmekaitse direktiiviga. Käesoleva magistritöö näol on tegemist kvalitatiivse uurimistööga, mille teooria analüüsimisel kasutatakse analüütilist ja tõlgendavat meetodit. Samuti kasutatakse ka teleoloogilist tõlgendamist ja võrdlevat meetodit. Analüüsi koostamiseks kasutatakse nii Euroopa Liidu kui ka Eesti andmekaitsealased õigusakte ning kohtupraktikat, nii esmaseid kui teiseseid allikaid.

Töö käigus jõudis autor järeldusele, et Euroopa Liidu tasandil oli vajalik kehtestada uus õigusakt, mis tagaks parema ja tõhusama isikuandmete kaitse. Samuti jõudis autor järeldusele, et uuendused tagavad tõhusama õiguskaitse, kuna uus üldmäärus on põhjalikum ning koosneb mitmetest põhimõtetest, mis eelnevas direktiivis ei olnud kajastatud, kuid praktikas selgus, et oleks vaja sätestada ka seadusandlikul tasandil. Autor jõudis olulisele tulemusele ka selle osas, et kas "õigus olla unustatud" tagab tõhusama õiguskaitse. Autor on arvamusel, et tänu "õigusele olla unustatud" on saavutatud tõhusam läbipaistvusprintsiibi järgimine ning andmesubjektidel on tõhusam kontroll iseenda isikuandmete üle. Samuti on nad rohkem teadlikud andmete töötlemise protsessist ning isikuandmete kaitse ulatusest.

Antud magistritöö hüpoteesiks on "õigus olla unustatud" tagab isikuandmete kaitse valdkonnas tõhusama õiguskaitse võrreldes eelnevalt kehtinud andmekaitse direktiiviga. Samuti on käesolevas magistritöös kolm uurimisküsimust. Nendeks on:

1. Kas Euroopa Liidu tasandil oli vajalik kehtestada uus õigusakt, mis tagaks isikuandmete kaitset paremini?
2. Kuidas tagavad andmekaitsemääruses kasutatavad uuendused tõhusama õiguskaitse, mis on kooskõlas inimeste põhiõiguste ja vabadustega?
3. Mis on on andmekaitse üldmääruse eeldatav mõju?

SISSEJUHATUS

Interneti näol on tegemist ühe suurima informatsiooni kogumikuga, mis võimaldab ligipääsu mitmetele andmebaasidele ja infokogumitele. Tänu sellele on võimalik koguda erinevat informatsiooni veebist, suhelda sõpradega, saada ligipääsu riigi poolt haldavatele teenustele või saada tulemusi sooritatud teabepäringutele. Tavapärasele informatsiooni otsingule veebist saab sooritada otsingut ka üksikisiku isikuandmete kohta. Selline otsing kujutab ohtu üksikisiku põhi- ja inimõigustele, kitsamalt öeldes nii õigusele privaatsusele kui ka õigusele isikuandmete kaitsele. Isikuandmete kaitse eesmärgiks on kaitsta üksikisiku eraelu ning privaatsuse kaitse on andmekaitse aluseks. Isikuandmete kaitse rohkem tähtsustamine on tingitud sellest, et varasemalt ei olnud võimalik teostada küberrünnakuid nii nagu tänapäeval, luues andmebaase ning automatiseeritult töödelda saadud andmeid.[1]

Internet on suurim informatsiooniallikas, mis siiani loodud on ning me elame maailmas, mis on digitaliseerinud. Seetõttu on raske andmekaitse norme sätestada, kuna ajaga kasvab interneti levik ja internetis olevate veebisaitide keerukus tõuseb.[2] Paljud meediaväljaanded on kolinud internetti ning teinud avalikuks oma võrguväljaanded ja võrguarhiivid. Samuti on tänapäevaks võrguväljaanded populaarsemad kui paberkandjal olevad meediaväljaanded. Ajaga on kasvanud ka interneti otsingumootorite tähtsus ja nende kasutajate arv. Mida rohkem on internet arenenud, seda enam küsitatakse isikute andmeid läbi veebi. Näited viisidest, kuidas läbi interneti üksikisikute andmeid nõutakse, on näiteks veebilehtedel sooritatud ostude kinnitus ankeedil, infopäringutel ning ka teistel erinevatel mehhanismidel, ning seda kõike veebilehe külastuse ajal läbi küpsiste.[3] Tehnoloogia arenguga on privaatsuse kaitse küsimused aktuaalsemad, kuid see ei ole ainult viimasel sajandil nii. Esimesed kirjed isikuandmete privaatsuse teemal ning selle seaduslikul tunnustamisel ulatuvad Ameerika Ühendriikides 1890. aastani, mil *Harvard Legal Law* ajakiri avaldas õigusteadlase Samuel D.Warreni ja Louis D. Brandeisi poolt loodud artikli

[1] Ilus, T. (2002) Isikuandmete kaitse olemus ja arengusuunad. *Juridica*, 7, lk 435-446.
[2] Cooley, R., Mobasher, B. & Srivastava, J. (1999) Data Preparation for Mining World Wide Web Browsing Patterns. – *Knowledge and Information Systems,* Vol. 1, 5-32.
[3] Inglise keeles Cookies.

pealkirjaga "The Right to Privacy" [4]. Antud artikkel on 128 aastat vana, kuid seda artiklit võib pidada üheks mõjuvõimsamaks esseeks maailmas, kuna see on tänase päevani relevantne. Antud artiklis defineerisid autorid privaatsust kui õigust olla üksi jäetud valitsuse poolt. Artikli eesmärgiks oli leida üksikisiku eraelu kaitsele õigusest tulenev alus. Samuti olid nad mures isikute privaatsuse üle, ühiskonnas toimuvate muutuste tõttu. Muutused, mida nad silmas pidasid olid seotud kaasaskantavate fotokaameratega, pressi ning kollase ajakirjanduse tekke ning kiire levikuga.[5] Autorite arvates tingisid sotsiaalsed muutused isiku eraelu tunnustamise vajaduse: „... pressi pealetükkivus ning avalik kuulujuttude levitamine on muutnud privaatsuse ja üksinduse indiviididele vajalikumaks ja olulisemaks, sest selle rikkumine võib isikule kaasa tuua valu ja stressi, mis on palju tõsisem kui mõni kehavigastus."[6]

Warreni ja Brandeis'i arvates peitus privaatsus isiku meelerahus. Privaatsusõiguse nimetasid nad õiguseks jääda rahule jäetud ehk isiku õigus oma isiklikule sisesfäärile. Seda võib pidada üheks esimeseks korraks, kui õiguskirjanduses või üleüldse kirjanduses defineeriti privaatsust kui õigust jääda rahule jäetud.[7] Privaatsusõigus on üks inimõiguste osadest, mis kujutab endast üksikisiku põhiõigusi-ja vabadusi, andes üksikisikule suurema kaitse.

Peale Teist maailmasõda on Euroopas õigus andmekaitsele ja privaatsusele muutunud väga oluliseks ning samuti ka üheks inimõiguste osaks. Andmekaitse arengule panid aluse 1948. aastal vastuvõetud ÜRO Inimõiguste Ülddeklaratsioon ning 1950. aastal loodud Inimõiguste ja põhivabaduste kaitse konventsioon. Osades riikides, ei peeta privaatsust ei inim- ega põhivabaduseks. Üheks näiteks saab pidada Ameerika Ühendriike, kus konstitutsioon ei taga privaatsuse kaitset. Ameerika Ühendriikide Ülemkohus on tõlgendanud mitmeid konstitutsiooni muudatusi, mis tagaksid üksikisiku privaatsuse mitmeid elemente kaitseks valitsuse sissetungivate tegevuste vastu, nende hulka kuuluvad näiteks sõnavabadus ja ebamõistlikud läbiotsimised, kuid üksikisiku privaatsus ei ole siiani konstitutsioonis kaitstud.[8] Isikuandmete töötlemist sätestas aga direktiiv 95/46/EÜ (andmekaitsedirektiiv).[9] Andmekaitsedirektiivi näol ei

[4] Klosek, J. (2000) Data Privacy in the Information Age. Greenwood Publishing Group, United States of America, lk 8.

[5] Solove, D (2009), *Understanding Privacy*, Harvard University press, Cambridge, lk 15-16.

[6] Brandeis, L. Warren, S. *The Right to Privacy* – R. Wacks, lk 4.

[7] Tzanou, M. (2013). *Is Data Protection the Same as Privacy? An Analysis of Telecommunications' Metadata Retention Measures*, *Journal of Internet Law,* Vol 17, nr 3, lk 23

[8] Cate, F. H. (1998) The European Data Protection Directive and European-U.S. Trade. Currents: *International Trade Law Journal*, 7 (1), lk 61-80, lk 66.

[9] Euroopa Parlamendi ja nõukogu direktiiv 95/46/EÜ, 24.10.1995, üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta. EÜT L 281, 23.11.1995.

ole tegemist otsekohalduva õigusaktiga, vaid liikmesriigid peavad tagama direktiivis sätestatud tulemuse, valides selleks ise vahendid või täpsed seaduse sõnastused. Seetõttu on regulatsioonid riigiti erinevad. Teised olulised rahvusvahelised aktid, mis kaitsevad isikuandmeid, on Euroopa Nõukogu konventsioon isiku kaitseks isikuandmete töötlemisel[10] ja Majanduskoostöö ja Arengu Organisatsiooni (inglise keeles lühend *OECD*) soovitused isikuandmete ja privaatsuse kaitseks ning piiriüleseks andmeedastuseks[11]. Kõikide nende dokumentide puhul on oluline märkida, et nendes dokumentides on arvesse võetud üksikisiku privaatsust, kui ka vajadust toetada informatsiooni vaba liikumist riikide vahel.[12]

25. jaanuaril 2012. a tehti ettepanek luua andmekaitsemäärus, mis asendaks direktiivi ning oleks otsekohalduv määrus, tänu millele oleks andmekaitse liikmesriikides ühtne, ning samuti taheti, et andmekaitse kontroll tugevneks ning väheneksid halduskulud. Tänu sellele tekkis andmekaitsereform. 24. mai 2016. aastal määrus jõustus ning seda hakatakse kohaldama 2018. aasta maist. Privaatsuse kaitse alla kuuluvad kõik andmete töötlemise meetmed. Kuna tegemist ei ole kitsa mõistega, siis tuleks kindlasti välja tuua erinevad töötlemise vormid. Nendeks on andmete levitamine, salvestamine, andmete kogumine, andmete muutmine, andmete kohandamine ning nende struktureerimine. Andmekaitse direktiivi artikkel 4 punkt 2 sõnastab isikuandmete töötlemist kui isikuandmete või nende kogumitega tehtavat automatiseeritud või automatiseerimata toimingut või toimingute kogumit, nagu kogumine, dokumenteerimine, korrastamine, struktureerimine, säilitamine, kohandamine ja muutmine, päringute tegemine, lugemine, kasutamine, edastamise, levitamise või muul moel kättesaadavaks tegemise teel avalikustamine, ühitamine või ühendamine, piiramine, kustutamine või hävitamine.[13] Kuna tehnoloogia on arenenud ning internetis saab viibida läbi erinevate nutiseadmete, veedavad inimesed virtuaalmaailmas rohkem aega. Sellest tulenevalt jagavad inimesed kas teadlikult või mitteteadlikult enda informatsiooni, seades sellega ohtu enda privaatsuse. Tegemist on valdkonnaga, mis puudutab meid kõiki ning mis puudutab meid igapäevaselt. Seetõttu on vaja inimesi teadvustada ohtudest, mis kaasnevad internetis aja veetmisega ning tõsta inimeste

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

[11] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 23. 09. 1980.

[12] Ilus (2002), *supra nota 1,* lk 436.

[13] Euroopa Parlamendi ja nõukogu määrus (EL) 2016/679, füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta. ELT L 119, 04.05.2016.

teadlikkust nende õigusele kaitsta oma isikuandmeid. Seetõttu võib märkida, et antud teema on igati aktuaalne käesolevas ühiskonnas ning tänu oma aktuaalsusele sobib ka magistritöö teemaks.

Antud magistritöö eesmärgiks on analüüsida uut andmekaitse üldmäärust ning uurida kuidas antud määrus kaitseb isikuandmeid, kuidas uued muudatused mõjutavad andmete töötlemise protsesse ning millised on võimalikud kitsaskohad. Antud magistritöö hüpoteesiks on "õigus olla unustatud" tagab tõhusama õiguskaitse isikuandmete kaitse valdkonnas võrreldes varasemalt kehtinud seadusandlusega.

Hüpoteesi aitavad kinnitada või ümber lükata järgmised uurimisküsimused. Nendeks on:

1. Kas Euroopa Liidu tasandil oli vajalik kehtestada uus õigusakt, mis tagaks parema isikuandmete kaitse?
2. Kuidas tagavad andmekaitsemääruses kasutatavad uuendused tõhusama õiguskaitse, mis on kooskõlas inimeste põhiõiguste-ja vabadustega?
3. Mis on andmekaitse üldmääruse eeldatav mõju?

Andmekaitsemäärust analüüsides on antud magistritöö jagatud kaheks peatükiks, mis omakorda jagunevad alapeatükkideks. Esimene peatükk keskendub andmekaitse printsiipidele Eestis tänapäeval. Antakse ülevaade olemasolevast õiguslikust raamistikust ning avatakse teema läbi asjakohaste mõistete. Seletatakse olulisi mõisteid nagu isikuandmed ja isikuandmete töötlemine. Samuti tutvustatakse õigusakte, mis on seotud andmekaitsega või mis on loodud selleks, et andmekaitset edendada. Teine peatükk räägib põhjalikult GDPR-st, selle suurimatest muudatustest ja aluspõhimõtetest ning tutvustatakse uusi meetmeid, mida kasutatakse, et seadus oleks tõhus, kuidas muutuvad andmekaitse printsiibid ning mis nende muudatustega kaasnevad. Samuti seletatakse lahti mida need muudatused endast kujutavad. Teises peatükis tutvustatakse ka printsiipe ja põhimõtteid, mis on kõige rohkem seotud andmekaitse direktiiviga ning millest kinnipidamine on andmetöötleja üks igapäevatöödest. Nendeks olulisteks printsiipideks on näiteks läbipaistvusprintsiip, teavituskohustus ja ka termin "õigus olla unustatud". Antud peatükis leitakse vastused ka töö alguses püstitatud küsimustele ning tehakse järeldusi saadud uurimusest ning ka ettepanekuid tulevikuks.

Varasemalt mainitud hüpoteesi paikapidavuse kontrollimine eeldab üksikasjalikku uurimustööd ning mitmete erinevate uurimismetoodite kasutamist. Tegemist on kvalitatiivse uurimistööga, mille teooria leidmiseks põhinetakse analüütilisel ja tõlgendaval meetodil. Samuti kasutatakse nii

teleoloogilist tõlgendamist kui ka võrdlevat meetodit. Töös kasutatakse nii Euroopa Liidu kui ka Eesti õigusakte, nii esmaseid kui teiseseid allikaid. Olulisteks allikateks on ka andmekaitsealased õigusaktid kui ka kohtupraktika antud teemal. Antud allikaid kasutatakse selleks, et koostada põhjalik uurimus ning anda ülevaade teema kohta. Samuti kasutatakse antud töö koostamisel ka erialast kirjandust. Kasutatud on nii eestikeelset kui ka võõrkeelset erialakirjandust, teaduslikku perioodikat ja internetis olevat teavet. Kuna andmekaitse teema on väga lai, siis erialakirjanduse valik on samuti väga lai ja rikkalik.

1. EESTI ANDMEKAITSE TÄNAPÄEVAL

Antud peatükis räägib autor infoühiskonna väljakujunenimisest, privaatsusõigusest, privaatsusest kui põhiõigusest, andmekaitse üldmäärusele eelnevatest õigusaktidest ning andmekaitsega seotud kõige tähtsamatest mõistetest kui ka andmekaitse reformi vajalikkusest. Samuti ka andmekaitse õiguslikust raamistikust nii Euroopas kui ka Eestis. Esimeses peatükis leiab vastuse ka kahele esimesele autori poolt püstitatud uurimisküsimusele. Esimese peatüki eesmärgiks on anta ülevaade andmekaitse õigusest ning sellega seonduvatest komponentidest. Andmekaitse temaatika on vägagi ajakohane, kuna esiteks tänu uuele üldmäärusele, mis hakkab kehtima 2018 aasta maist, kui ka tänu sellele, et internetist on saanud igapäeva osa ning interneti kasutajate arv suureneb iga päev ning tänu sellele suureneb ka internetis tehtavad andmekaitse rikkumised. Oluline on märkida ka seda, et enamus andmekaitse rikkumisi on toimunud just tänu internetile.

1.1. Infoühiskonna väljakujunemine

Tänapäeval oleme jõudnud infoühiskonda, sest informatsioon on saanud oluliseks nii nimetatud käibeobjektiks, aga ka kultuuriväärtuseks ja hüveks.[14] Tänu sellele saab tänapäeval olevat ühiskonda nimetada infoühiskonnaks. Infoühiskonna pakutavad teenused on igapäeva osaks ning kergesti kättesaadavad igas eas olevatele isikutele. Ligipääs internetile on samuti väga kerge ning seda võib pidada üheks osaks inimeste igapäevaeludes. Läbi interneti tehtavad teenused muudavad elu kiiremaks ja mugavamaks. Nendeks võivad olla nii pangateenused kui ka sotsiaalmeedia. Läbi sotsiaalmeedia on võimalik oma arvamust avaldada, informatsiooni jagada oma sõpradega või lihtsalt vestelda. Samuti ka lisada artikleid, pilte või videoid. Erineva informatsiooni jagamine on läbi interneti tehtud võimalikuks vaid ühe nupuvajutusega, muutes sellise info jagamise vormi kõige kiiremaks ja mugavamaks.

Algselt, kui internet loodi, kasutasid seda ainult haritlased, kes jagasid selle vahendusel üksteisega informatsiooni. Tänapäeval on internet peamiseks informatsiooniallikaks ning töövahendiks paljudele erinevatele inimestele. 1960. aastal algas esimene tehnoloogia *boom* ning

[14] Tikk, E. Nõmper, A. (2007) Informatisoon ja õigus. Tallinn: Juura, lk 14.

ka esimene suuremahuline isikuandmete kogumine. Algselt kogusid ettevõtted andmeid iseenda firma jaoks, kuid aja jooksul taibati, et sellega on võimalik enda ettevõtet edendada ning äri teha. Valitsused ja ettevõtted hakkasid kasutama arvuteid, et paremini koguda ja töödelda isikuandmeid.[15] Varsti said ettevõtted ja valitsused kogutud andmete majanduslikust väärtusest aru ning alustasid eurooplaste igapäevaste tegevustest saadud andmete salvestamist. Kuna isikuandmete kogumine muutus aina mahukamaks, siis 1970. aastal tunnistas Euroopa Nõukogu vajadust reguleerida isikuandmete kogumise ja säilitamise prognoositavat arengut, et säilitada isiku eraelu kaitse. Euroopa Nõukogu Ministrite Komitee hakkas vastu võtma otsuseid ja kehtestama põhimõtteid ning juhiseid isikuandmete kaitse ühtlustamiseks liikmesriikide vahel.[16] Esimest korda kehtestati seadusandlikul tasandil andmekaitse sätted 1970. aastal Hesse Liidumaal Saksamaal.[17]

Selleks, et isikute privaatsusõigus oleks laialdaselt tagatud loodi 28. jaanuaril 1981. aastal rahvusvaheline andmekaitset kaitsev konventsioon nr 108[18], mis reguleerib isikuandmete automatiseeritut töötlemist. Tänu sellele dokumendile sätestati esimest korda üksikisiku õigus privaatsusele, mis kujutas endas kaitset isikuandmete kogumise, töötlemise ning formuleeris isikuandmete mõiste ning mis juhtudel on tegemist delikaatsete isikuandmetega. Samuti on regulatsioonis märgitud, mis juhul on isikul õigus teada, mis informatsiooni tema kohta talletatakse ning vajadusel on võimalik seda isikul lasta muuta. Eelnevalt puudus vajadus selliseks õigusaktiks, kuna internet puudus ning seetõttu ei olnud info ka nii kergesti ning nii paljudele inimestele kättesaadav.

Koos tehnoloogia arenguga ning interneti kiire levikuga, tekkis vajadus detailsema regulatsiooni järgi. Tulenevalt vajadusest hakati välja töötama andmekaitsedirektiivi. 1990. aastal tehti ettepanek, et direktiiv vastu võtta, kuid võrreldes tänase päevaga ei olnud olemas sotsiaalseid võrgustikke, pilveandmetöötlusi, asukohapõhiseid teenuseid ja teisi erinevaid programme. Seetõttu oligi vaja andmekaitsereformi. Andmekaitsedirektiivist tulenes, et andmekaitseasutused peaksid ennetavalt mõtlema uue tehnoloogiaga seotud privaatsuse tõrgetest, et reguleerida

[15] Glon, C. (2014) Data Protection in the Europeal Union: A closer look at the current patckwork of data protection laws and the proposed reform that could replace them all. *International Journal of Legal Information*, 42 (3), lk 471- 492.
[16] *Ibid.*
[17] Tzanou, M. (2013) Data Protection as a Fundamental Right Next to Privacy? "Reconstructing" a not so new right. *International Data Privacy Law*, vol. 3, lk 90.
[18] Council of Europe. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. ETS No.108, Strasbourg 28/01/1981 (Convention 108).

tehnoloogiat enne privaatsuse kuritarvitamist. Tänu sellele on direktiiv loonud sõltumatute andmete turvalisuse tagamisega tegelevad asutused.[19] Samuti on suureks probleemiks see, et laialdane andmete kogumine, analoogide salvestamine läbi digiteerimise ning kogu meedia muutmine digitaalvormingusse viib meid ajastusse, kus on olemas "perfektne meelespea" ehk üksikisikutel on võimalus näiteks Google otsingumootorit kasutades näha? enda minevikku läbi interneti.[20]

Aastatega on interneti kasutajate hulk suurenenud ning vastavalt sellele on ka informatsiooni levik suurenenud. Andmete jagamine on muutunud lihtsamaks ja mugavamaks ning inimesed külastavad mitmeid veebilehti, mis koguvad nende teadmata nende andmeid ning seetõttu on ka isikute privaatsust järjest rohkem rikutud. Samuti ei ole inimesed teadlikud sellest, et veebisaidid nende andmeid töötlevad, või et neil on õigus enda isikuandmete kaitsele.

1.2. Privaatsus

Eesti Vabariigi põhiseaduses on sätestatud artiklis 26 õigus perekonna –ja eraelu puutumatusele. Selle sätte näitel on tegemist privaatsusõigusega.[21] Privaatsusõigust hakati ulatuslikult tunnistama peale II maailmasõda. Privaatsusõigus ehk õigust eraelu puutumatusele saab lugeda igaühe õigust enesemääratlemisele, elada oma soovide ja tahtmise järgi minimaalse välise sekkumisega, kontrollida enda kohta käivat informatsiooni ning olla kaitstud eraeluliste sekkumiste eest.[22] Samuti kuulub privaatsusõigus põhiõiguste hulka ning seda saab kirjeldada põhiõiguste tunnuste kaudu.

Privaatsus ja andmekaitse on omavahel seotud seetõttu, et privaatsuse komponentideks on asjad, mille alusel on isik äratuntav ning mille kaudu isik ennast teistele või riigile määratleb. Identiteediks võib pidada unikaalsete tunnuste kogumit, mille alusel isik eristub kõikidest teistest isikutest.[23] Identiteet koosneb aga komponentidest, mille järgi on võimalik isikut tuvastada. Nimi on esimene asi mille järgi inimene eristub teistest isikutest ning see on osa isiku identiteedist.

[19] Heisenberg, D. (2005). Negotiating privacy : The European Union, the United States, and personal data protection, Ipolitics: Global Challenges in the Information Age.

[20] Gutwirth, S, Leenes, R, & Poullet, Y (eds) 2011, Computers, Privacy and Data Protection : An Element of Choice, Springer, Dordrecht.

[21] Eesti Vabariigi põhiseadus. - RT I, 15.05.2015, 2

[22] Maruste, R. (2004) Konstitutsionalism ning põhiõiguste ja -vabaduste kaitse. Tallinn: Juura, lk 429

[23] Männiko, M. (2011). Õigus privaatsusele ja andmekaitse, Tallinn, Juura, lk 18.

Kaasuses *Burghartz vs. Šveits*[24] leidis EIÕK, et füüsilise isiku identifitseerimise ja perekondliku kuuluvuse tunnustamise vahendina puudutab nimi isiku era-ja perekonnaelu.[25] Teiseks privaatsuse komponendiks on isikukood ning koos nimega kasutatakse seda kõige tihedamini isiku identifitseerimisel. Isikukood on osa inimese identiteedist ning selle töötlemine on privaatsusõigusega kaitstav. Kolmandaks privaatsuse osaks võib pidada etnilist kuuluvust. Rassiline, etniline ja rahvuslik kuuluvus moodustab osa üksiksiku identiteedist ning on ka tänu sellele privaatsusõigusega kaitstav. Järgmiseks privaatsuse osaks võib pidada isiku füüsilisi omadusi ning need on isiku identifitseerivateks tunnusteks ning on tänu sellele ka osa inimese identiteedist. EIÕK leidis kaasuses *von Hannover vs. Saksamaa,* et isiku kohta piltide avaldamine on tema füüsilise ja psühholoogilise puutumatuse rikkumine ning sellest tulenevalt vastuolus EIK artikliga 8.[26] Järgmiseks privaatsuse komponendiks saab pidada sotsiaalset kuuluvust, mis on samuti kaitstav privaatsusõigusega. Kaasuses *Odiere vs. Prantsusmaa* leidis EIÕK, et isikul on õigus teada oma geneetilisi vanemaid, sest vanemate informatsioon moodustab osa isiku eraelust ning osa ka isiku identiteedist.[27] Isiku identiteedi moodustavad erinevad isiku iseloomuomadused- ja tunnused ning see on oluline privaatsusõiguse koha pealt seetõttu, et isikul oleks õigus otsustada, et kellele või millisel moel ta enda identiteeti avaldab. Kõik need erinevad komponendid moodustavad isiku identiteedi.

1.3. Kesksed mõisted

Privaatsuse ja andmekaitse mõisted on üksteisega tihedalt seotud, sest privaatsus on andmekaitse aluseks. Privaatsuse puhul on tegemist universaalse ideega, millel on tugev eetiline mõõde ning mis on seotud inimese väärikuse ja autonoomiaga.[28] Samuti on privaatsusega seotud õigus eraelule, mida saab pidada üheks demokraatliku riigi alustalaks, sest see puudutab igaüht. Põhiõigusena on ka õigus isikuandmete kaitsele osa üksikisiku enesemääratlusõigusest.[29] Enesemääramisõigus koosneb mitmetest aspektidest. Nendeks võivad olla rahvuspärane enesemääratlus, kehaline enesemääratlus, seksuaalne enesemääratlus, informatsiooniline enesemääratlus jne. Kõik eelnevalt nimetatud on kaitstavad privaatsusõiguse sätetega. Kuid

[24] EIKo 22.02.1994, 16213/90, *Burghartz vs. Šveits*
[25] *Supra nota* 16, lk 19.
[26] EIKo 24.09.2004, 59320/00, *von Hannover vs. Saksamaa.*
[27] EIKo 13.02.2003, 42326/98, *Odiere vs. Prantsusmaa.*
[28] Hustinix, P (2013). EU Data Protection Law - Current State and Future Perspectives, http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/Hustingx.pdf (15.02.2018)
[29] *Supra nota* 16, lk 41.

andmekaitsega on kõige rohkem seotud informatsiooniline enesemääratlus.[30]

Saksamaa konstitutsioonikohus tunnistas 1983. aastal rahvaloenduse kaasuses (*Volkszählungsurteil),* informatsioonilist enesemääramisõigust kui eraldiseisva õigusena. See oli esimene kord, kui kohus rõhutas isiku informatsioonilisele enesemääramisõigusele kui õigusele. Informatsiooniline enesemääratlus on põhiõigus ja sotsiloogiline norm, mille eesmärgiks on säilitada üksikisiku nii väiksemad kui suuremad väljakutsed millega tagatakse sotsiaalne stabiilsus. Samuti on Saksamaal õigus informatsioonilisele enesemääramisele üheks andmekaitse keskseks põhiõiguslikuks aluseks.[31] Kohtuotsus sätestab, et üksikisiku põhiõigus on ise otsustada oma isikuandmete avalikustamise ja kasutamise üle.[32] Andmekaitse alustaladeks on seega nii õigus privaatsusele kui ka õigus informatsiooni läbi enesemääratlemisele. Antud põhiõigused on kattuvad oma mõistete tõttu, ning leidub seletusi, mille kohaselt privaatsusõigus on enesemääramisõiguse üks osa, seetõttu on kaitstavaks õigushüveks õigus informatsioonilisele enesemääramisele.

Andmekaitsemääruse keskseteks mõisteteks on andmed. Andmed on informatsioon kellegi või millegi kohta.[33] Isikuandmeteks võib siis pidada andmeid, mis annavad informatsiooni isiku kohta.

Isikuandmete mõiste on defineeritud andmekaitsemääruse artikli 4 punktis 1, mis sätestab, et isikuandmed on:

"igasugune teave tuvastatud või tuvastatava füüsilise isiku („andmesubjekti") kohta; tuvastatav füüsiline isik on isik, keda saab otseselt või kaudselt tuvastada, eelkõige sellise identifitseerimistunnuse põhjal nagu nimi, isikukood, asukohateave, võrguidentifikaator või selle füüsilise isiku ühe või mitme füüsilise, füsioloogilise, geneetilise, vaimse, majandusliku, kultuurilise või sotsiaalse tunnuse põhjal."[34]

Samuti on direktiivis kirjas, et füüsiline isik on isik, keda saab otseselt või kaudselt tuvastada.

[30] *Ibid,* lk 41.
[31] M. Albers. (2005) Isikuandmete kaitse põhiõiguslik alus: kas õigus informatsioonilisele enesemääramisele ja/või eraelu austami- sele? – Juridica 8, lk 537–543, lk 537.
[32] DeSimone, C. (2011). Pitting Karlsruhe Against Luxembourg? German Data Protection and the Contested Implementation of the EU Data Retention Directive. - *German Law Journal* 2010/11, No. 3, lk 293.
[33] Eesti keele sõnaraamat ÕS (1999), Tallinn, Eesti Keele Sihtasutus.
[34]Euroopa Parlamendi ja nõukogu määrus (EL) 2016/679, füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta. ELT L 119, 04.05.2016.

Otsene tuvastamine käib isiku nime järgi ning kaudne tuvastamine näiteks telefoninumbri, video või asukoha järgi. Artiklit ei saa kohaldada juriidilisele isikule. Samuti on andmekaitsemääruse preambula punktis 51 mainitud füüsiliste isikute teistsugust tähelepanu vajavad andmeliigid. Nendeks on delikaatsed isikuandmed, mis vajavad rohkem kaitset. Andmekaitsemääruse artikli 9 lõike 1 kohaselt on delikaatsed isikuandmed:

"[...] millest ilmneb rassiline või etniline päritolu, poliitilised vaated, usulised või filosoofilised veendumused või ametiühingusse kuulumine, geneetilisi andmeid, füüsilise isiku kordumatuks tuvastamiseks kasutatavaid biomeetrilisi andmeid, terviseandmeid või andmeid füüsilise isiku seksuaalelu ja seksuaalse sättumuse kohta."[35]

Delikaatsete isikuandmete töötlemisel karmima lähenemise kasutamise nõuet on seadusandja nõudnud seetõttu, et kui kasutatakse ära andmeid valedel eesmärkidel, toob see kaasa suurema kahju ning rikkumise üksikisikute põhiõigustele.[36] Direktiivi artikkel 8 lõike 1 kohaselt on ka kitsam delikaatsete isikuandmete mõiste seletus, milleks on:

„[...] isikuandmeid, mis paljastavad rassilise või etnilise päritolu, poliitilised vaated, usulised või filosoofilised veendumused, ametiühingusse kuulumise, ning tervislikku seisundit või seksuaalelu[37] [...]."

Eelnevast lähtudes võivad olla isikuandmed ükskõik mis vormis, kuna õigusaktides ei ole mainitud konkreetset vormingut. Teave võib olla nii kirjana, pildina, dokumendina, videona või audiofailina. Erinevad andmed ning mitmetes erinevates vormingutes olevad andmed annavad isiku kohta samasugust informatsiooni. Erinevas vormis esinevate andmete puhul on tegemist isikuandmetega siis, kui nende põhjal on võimalik isik seostada. Kui andmed on isiku omad, siis on tegemist isikuandmetega ehk isik on seostatav kuidagi nende andmetega. Isikuandmed, mis on uuesti identifitseeritud või krüpteeritud, kuid mille läbi saab isikut uuesti tuvastada on endiselt isikuandmed ning kuuluvad seaduse reguleerimisalasse. Seadus kaitseb isikuandmeid sõltumata nende andmete töötlemiseks kasutatud tehnoloogiast. Kuna see tehnoloogia on neutraalne ja kehtib nii automatiseeritud kui ka käsitsi töötlemise kohta, tingimusel, et andmed

[35] *Ibid*

[36] Artikkel 29 alusel asutatud andmekaitse töörühm. Advice Paper on Special Categories of Data (sensitive data), 2000. https://ec.europa.eu/info/law/law-topic/data-protection_en (19.02.2018)

[37] Parlamendi ja nõukogu direktiiv 95/46/EÜ, *supra nota* 5.

on korraldatud vastavalt eelnevalt määratletud kriteeriumitele.[38]

Teiseks oluliseks mõisteks on andmesubjekt. Andmesubjektiks on füüsiline isik, kelle isikuandmeid kuidagi töödeldakse.[39] Töötlemiseks nimetatakse igat isikuandmetega tehtavat toimingut, sõltumata selle töötlemise viisist. Erinevad töötlemise viisid on: kogumine, salvestamine, päringu teostamine, korrastamine, üleandmine, kasutamine, levitamine, väljavõtete tegemine, kustutamine, sulgemine, hävitamine ja ühendamine. Samuti on õiguskirjanduses nimetatud üldistavalt andmesubjekti õiguseid andmetöötleja suhtes ning teisalt poolt andmetöötleja kohustusi andmesubjekti suhtes - andmesubjekti osaluse põhimõte.[40] Samuti on üldmääruses sätestatud ka teised mõisted nagu: profiilianalüüs, preudonümiseerimine, andmete kogum, vastutav töötleja, volitatud töötleja, vastuvõtja, kolmas isik, andmesubjekti nõusolek, isikuandmetega seotud rikkumine, geneetilised andmed, biomeetrilised andmed, terviseandmed, peamine tegevuskoht, esindaja, kontsern, siduvad kontsernisisesed eeskirjad, järelevalveasutus, asjaomane järelvalveasutus, isikuandmete piiriülene töötlemine, asjakohane ja põhjendatud vastuväide, infoühiskonnas teenus jne.

1.4. Õiguslik raamistik

1.4.1. Euroopa Inimõiguste ja põhivabaduste kaitse konventsioon

Euroopa Inimõiguste ja Põhivabaduste kaitse konventsioon (EIÕK) võeti vastu aastal 1950, kuid see jõustus 1953 aastal.[41] 1959. aastal asutati Strasbourgis Euroopa Inimõiguste Kohus (EIK), et tagada konventsioonist tulenevaid õigusi. Konventsioonist ei tule sinna sätestatud kaitset isikuandmete kaitsele. Õigus on tuletatav EIÕK sätestatud artiklis 8 õigusest era- ja perekonnaelu kaitsele. Artikkel 8 ei sisalda endas sõnu "informatsioon", "andmekaitse" või "andmed", kuid nagu varasemalt mainiti, siis EIK rohke praktika informatsioonilise enesemääratluse teemal ning sellega seotud õigus isikuandmete kaitsele kuulub artiki 8 alla. Artikkel 8 sätestab, et igaühel on õigus nõuda, et tema era- ja perekonnaelu, kodu puutumatus ja kirjavahetuse saladust austataks ning võimud võivad ainult sellel juhul sekkuda, kui see on

[38] Artikkel 29 alusel asustatud andmekaitse töörühm, *supra nota* 17. (19.02.2017)
[39] Männiko, M. *Supra nota* 16.
[40] Ilus, T. (2005). Andmesubjekti osaluse põhimõte Euroopa Nõukogu konventsioonide ning Euroopa Inimõiguste Kohtu lahendite valguses. – *Juridica,* 8, lk 519.
[41] The Council of Europe. A Convention to protect your rights and liberties. Kättesaadav: http://human-rights-convention.org/, 21.02.2018.

kooskõlas seadusega ning see on demokraatlikus riigis vajalik riigi julgeoleku tagamiseks.[42]

Isikuandmete kaitset artikli 8 ulatuses mainiti esmakordselt 1984. aastal, kui kohtunik Pettiti jäi eriarvamusele otsuses *Malone vs The United Kingdom*. Oma eriarvamuses sõnas ta, et avaliku võimu poolt ilma õigusliku aluseta telekommunikatsioonivahendite mõõtmine rikub üksikisiku õigust informatsioonilisele enesemääramisele.[43] EIK on leidnud, et artikkel 8 alla kuuluvad ka informatsiooni kogumine ning avaldamine ilma isiku ebaõige informatsiooni ümber lükkamiseta[44] ja isiku õigus nõuda ligipääsu temakohta kogutavate andmetele.[45]

EIK kohtupraktika isikuandmete kaitse teemadel on lai ning EIÕK on tänase päevani aktuaalne isikuandmete kaitseks, kuid kahjuks see on liialt üldsõnaline. Kuna EIÕK ei sisalda isikuandmete kaitse keskseid mõisteid või üleüldist viidet isikuandmete kaitsele, siis puudub teadmine, millal isikuandmete töötlemisega seotud küsimused langevad EIÕK kaitsealasse ning millal mitte. EIÕK artikkel 8 sätestatud sõna "eraelu" on liialt lai ning ebaselge ning antud artiklit rakendatakse kõige tihedamini andmekaitse teemadel siis, kui avalik võim on kuidagi sekkunud üksikisiku andmete töötlemisse. Samuti ei ole EIÕK kaitsealas ka isikuandmete töötlemine erasektori poolt, kuid see moodustab ühe suurima osa andmete töötlemisel.

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

1981. aastal võeti vastu Euroopa Nõukogu isikuandmete automatiseeritud töötlemisel isiku kaitse konventsioon (edaspidi konventsioon nr 108). Tegemist on esimese rahvusvahelise õiguslikult siduva dokumendiga andmekaitse valdkonnas. Konventsioonile eelnesid Euroopa Ministrite komitee soovitus – "Üksikisikute andmete kaitsest erasektoris elektroonilistes andmebaasides"[46] ja soovitus – "Üksikisikute andmete kaitsest avaliku sektori elektroonilistes andmebaasides."[47] Konventsiooni nr 108 eesmärgiks on tagada isiku õigus privaatsusele andmekaitse kontekstis ning reguleerida piiriületavate andmete liikumist. Konventsiooni artikkel üks sätestab, et "[...]konventsiooni eesmärk tagada osalisriigi territooriumil igale isikule,

[42] L. A. Bygrave. (1998). Data Protection Pursuant to the Right to Privacy in Human Right Treaties.- *International Journal of Law and Information Technology*, nr 6 (3), lk 255-259.
[43] EIKo 02.08.1984, 8691/79, *Malone v The United Kingdom, kohtunik Pettiti eriarvamus.*
[44] EIKo 26.03.1987, 9248/81, *Leander v Sweden.*
[45] EIKo 07.07.1989, 10454/83, *Gaskin vs The United Kingdom*.
[46] 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, 21.02.2018.
[47] 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, 21.02.2018.

olenemata tema kodakondsusest või alalisest elukohast, tema õiguste ja põhivabaduste austamine. Eriti oluline on isikuandmete automatiseeritud töötlemisel tagada isiku õigus säilitada privaatsus." [48]

Konventsiooni sätestatakse isikuandmete töötlemise põhimõtted, mida kasutatakse tänapäevalgi, võttes aluseks konventsiooni. Samuti reguleerib konventsioon ka andmete piiriülest kandmist. Aastal 2001 koostati konventsioonile lisaprotokoll, mis sisaldas endas piiranguid andmete ekspordiks ning sätestab, et tuleb luua sõltumatu järelevalveasutus ja õigus edasikaebamisele. Oma olemuselt on see väga sarnane andmekaitse direktiivile 95/46/EÜ. Konventsiooniga on liitunud 2018. veebruari seisuga 51 riiki,[49] kuid tänaseks päevaks on antud konventsioon iganenud, kuna see ei arvesta internetikasutajate suureneva arvuga ning nendega kaasnevate riskidega.

1.4.3. Euroopa Liidu põhiõiguste harta

Euroopa Liidu asutamislepingutes ei mainitud mingil viisil inimõiguseid ega ka üksikisikute isikuandmete kaitsmist. Euroopa õiguse üldpõhimõtetesse lisati põhiõigused siis, kui toimusid inimõiguste väidetavad rikkumised valdkondades, mis kuulusid Euroopa Liidu õiguse kohaldamisalasse. Aastal 2000 kuulutati välja Euroopa Liidu põhiõiguste harta.[50] Harta koosneb Euroopa liikmesriikide kodanike tsiviil-, majanduslikke, poliitilisi ja sotsiaalseid õigusi. Hartaga anti isikuandmete kaitsele põhiõiguse staatus. Algselt oli harta poliitiline dokument, kuid 1. detsembril 2009. aastal jõustus Lissaboni leping ning tänus sellele muutus harta õiguslikult siduvaks liikmesriikidele. Harta artikkel 47 sätestab, et igal isikul on isikuandmete kaitse reeglite rikkumise korral õigus tõhusale õiguskaitsevahendile ja õiglasele kohtulikule arutamisel.[51]

Samuti sätestab harta artikkel 8, et isikuandmeid tuleb töödelda asjakohaselt ning kindlatel eesmärkidel ning igal inimesel on õigus tutvuda tema kohta kogutud andmetega ning nõuda nende parandamist, kui on vaja. Sellest artiklist kinnipidamist kontrollib sõltumatu järelevalveasutus.[52] Artikkel 8 koostamisel võeti eeskujuks EIÕK artikkel 8 ning sellest põhinevast rohkest kohtupraktikast. Hartast tulevad üldised ning põhiõiguslikud printsiibid isikuandmete kaitsel. Üldjuhul kohaldatakse hartat koos andmekaitsedirektiiviga, kuna

[48] The Council of Europe. Treaty Office. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data CETS No.:108. Arvutivõrgus: http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=108&CM=&DF=&CL=ENG, 28.04.2014.
[49] *Ibid.*
[50] Euroopa Liidu põhiõiguste harta. - ELT C 83, 30.03.2010.
[51] *Ibid*, artikkel 47.
[52] *Supra nota* 35, artikkel 8

andmekaitsedirektiivis on põhjalikult lahti seletatud kesksed mõisted nagu näiteks "isikuandmed". Kuid sellest olenemata ei lahendanud harta andmekaitsedirektiivi probleeme, kuna koosnedes ainult põhiõigustest, ei näe see ette kindlaid reegleid isikuandmete töötlemiseks.

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

Antud direktiiv võeti vastu 1995 aastal. Direktiivi eesmärk oli ühtlustada ja harmoniseerida liikmesriikide vahel isikuandmete töötlemisega seotud õigusakte.[53] Direktiivi loomisel sooviti tagada andmete vaba liikumine, efektiivne siseturu toimimine ning tagada isikute põhiõiguste kaitse. Direktiiv loodi sellel eesmärgil, et täiendada ning täpsustada olemasolevaid õigusakte. See on sätestatud ka direktiivi preambulas. Preambula 10 kohaselt on direktiivi eesmärk kaitsta EIÕK artiklis 8 tunnustatud põhiõigusi. Mitmeid aastaid hiljem jõuti järeldusele, et direktiiv on sobilik eesmärkide ja põhimõtete seisukohast, kuid see ei ole piisavalt efektiivne, et lahendada isikuandmete kaitse probleeme. Aastaks 2010 oli selgunud, et direktiivi rakendamisel on tekkinud andmekaitse õiguse laialivalgumine, kuna liikmesriikides andmekaitsele kohaldatava õiguse tasemed olid erinevad ning seetõttu puudus õiguskindlus selle direktiivi rakendamisel. Lisaks ei olnud antud direktiiviga andmekaitse õiguse kokku sulamine liidu tasandil toimunud oodatud tasemel.

16. septembril 2010. aastal pidas Euroopa Liidu õigusvolinik ning Euroopa komisjoni asepresident Viviane Reding Brüsselis toimunud Digitaalse ühisturu konverentsil kõne, kus ta teatas, et soovib läbi vaadata kehtivat andmekaitse direktiivi, et tugevdada üksikisikute õigusi ja siseturu toimimist. Viviane Reding soovitas, et kui üksikisik ei soovi enam, et tema andmeid töödeldakse või salvestatakse vastutava töötleja poolt ning nende andmete säilitamiseks ei ole ühtegi õigustatud põhjust, et neid säilitada, tuleks vastavad andmed nende süsteemist kustutada. Viviane Reding ja Euroopa Komisjon olid eestvedajaks, et tuvastada direktiiviga kaasnevaid probleeme. Selleks, et probleeme tuvastada korraldas Euroopa Komisjon arutelusid, huvigruppe ning teisi erinevaid konsulteerimisi.[54] Aastal 2010 väljastas Euroopa Komisjon teatise "Tervislik lähenemisviis isikuandmete kaitsele Euroopa Liidus".[55] Antud teatisega selgus, et direktiiviga

[53] Carey, P. (2004) Data protection: a practical guide to UK and EU law. Oxford: Oxford University Press, lk 3.
[54] Euroopa Komisjoni eelnõu seletuskiri „Euroopa Parlamendi ja nõukogu määrus üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta." KOM(2012) 11. Brüssel: 25.01.2012, lk 3. Arvutivõrgus:http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_et.pdf, (26.02.2018)
[55] Euroopa Komisjoni teatis Euroopa Parlamendile, nõukogule, majandus- ja sotsiaalkomiteele ning regioonide komiteele. Terviklik lähenemine isikuandmete kaitsele Euroopa Liidus. KOM(2010) 609 lõplik. Brüssel: 04.11.2010. Arvutivõrgus: http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_et.pdf, (26.02.2018)

seotud probleeme ei olnud selleks ajaks suudetud lahendada. Andmekaitsereformiks valmistudes korraldas Euroopa Komisjon 2011. aastal andmekaitse direktiivi tõhususe hindamise.[56] Korraldatud andmekaitsedirektiivi rakendamise hindamine kinnitas, et ülevõtmisel liikmesriikidele jäetud vorm ja meetodite valik ning riigiti erinevad ühiskondlikud arusaamad on viinud selleni, et direktiivi käsitletakse erinevalt ning selle tulemus on see, et puudub ühtne arusaam direktiivi mõistete kontseptsioonist Euroopa Liidus.[57]

Pärast probleemide selgumist ning nende uurimist tegi Euroopa Komisjon 25.01.2012 ettepaneku isikuandmete kaitse regulatsiooni laiaulatuslikuks reformiks ning, et uus loodav üldraamistik peab asendama kehtima andmekaitse direktiivi. Uue reformiga tuleks üldmäärus, direktiiv ja nendele eelnev seletuskiri. Uue direktiivi peamisteks eesmärkideks pidas Euroopa Komisjon üksikisikute õiguste tugevdamist ning siseturu suurendamist. Eesmärgi saavutamiseks tuleb tagada igas olukorras üksikisikutele asjakohane kaitse, suurendada andmesubjektide läbipaistvust, suurenda teadlikkust oma õiguste suhtes andmete kaitsmisel ning tõhustada õiguskaitsevahendeid.[58] Selleks, et tagada üksikisiku isikuandmete kaitse tugev tase tuleb andmete töötlemisel rakendada võimalikult väheste andmete kogumise põhimõtet ning üksikisikul peab olema võimalus tutvuda enda kohta kogutud andmetega ja võimalusel neid parandada või kustutada. Samuti on andmetöötleja kohustatud teavitama andmesubjekti tema andmete töötlemisest.

Pärast pikki läbirääkimisi antud teemal jõudsid Euroopa Komisjon, Euroopa Nõukogu ja Euroopa Parlament ühisele seisukohale ning 14. aprillil 2016. aastal kinnitas Euroopa Parlament andmekaitsereformi, mille hulka kuulusid (EL) 2016/679 - füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise määrus (GDPR) ning andmekaitsemääruse (direktiivi 95/46/EÜ) kehtetuks tunnistamise. 28. Mail 2018. muutub uus üldmäärus (GDPR) täies ulatuses täitmisele pööratavaks kogu Euroopa Liidus olevatele liikmesriikidele.

1.4.5. Eesti õigus

Eestis on isikuandmete kaitse seaduse ajalugu võrreldes teiste euroopa riikidega lühike. Eesti Põhiseaduses ei ole eraldi sätet isikuandmete kaitsele, kuid see õigus on Põhiseadusest tuletatav.

[56] Commision Staff Working Paper Impact Assessment /SEC/2012/0072 final, 25.01.2012.
[57] Tupay, P, K. (2016) Õigusest eraelule kuni andmekaitse üldmääruseni ehk tundmatu õigus isikuandmete kaitsele. Juridica, 4, lk 237.
[58] Euroopa Komisjonis teatis 2010.

Eestis reguleerib Isikuandmete kaitset isikuandmete kaitse seadus (IKS)[59], kuid isikuandmete kaitse sätteid leidub ka elektroonilise side seaduses (ESS).[60] Isikuandmete töötlemine on seotud ka avaliku teabe seadusega (AvTS).[61]

Teised õigusaktid, mis on seotud isikuandmete kaitsega on Eestile rahvusvahelised siduvad õigusaktid. Eesti ratifitseeris 1996 aastal Euroopa inimõiguse- ja põhivabaduse kaitse konventsiooniga ning 2002 aastal ratifitseeris konventsiooni nr 108. Samuti on eelnevalt nimetatud Euroopa Liidu õigusaktid Eestile siduvad, kuna 2004 aastal allkirjastas Euroopa Liiduga liitumislepingu. Eestile on soovituslik ka OECD juhend, kuna Eestis on OECD liige alates 2010. aastast.

1.4.6. Eesti Vabariigi Põhiseadus

Mitmed Euroopa riigid on õiguse isikuandmete kaitsele või privaatsusõiguse tunnustanud eraldiseisvana õigusena ning toonud selle eraldi välja ka enda põhiseaduses, kuid Eesti ei ole seda teinud. Eestis seostatakse isikuandmete kaitset enesemääramisõigusega, kuid see õigus on üks osa põhiseaduse § 26[62] eraelu kaitse osast. Samuti seostatakse isikuandmete kaitset ka põhiseaduse §19, mis sätestab, et igaühel on õigus vabale eneseteostusele ning selle alla kuulub ka informatsiooniline enesemääramisõigusele, mille kohaselt on iga isiku otsus kui palju tema andmeid kogutakse ja salvestatakse.[63] Põhiseaduse §19 on vabaduspõhiõigus, mille eesmärgiks on tagada isikule enesemääramisõiguse olemasolu.

Varasemalt mainitud põhiseaduse §26, mis sätestab igaühe õiguse perekonna- ja eraelu puutumatusele. Riigikohtu halduskolleegium on jõudnud oma kaasuses arvamusele, et eraelu riiveks võib pidada ka isikuandmete kogumist, salvestamist ning ükskõik mis teisel moel andmete töötlemist.[64] Põhiseaduse §26 loomisel võeti eeskujuks Euroopa Inimõiguste ja põhivabaduste kaitse konventsiooni artikkel 8. Eraelu hulka kuuluvad intiimsfääri puutumatus, õigus seksuaalsele enesemääramisele, õigus informatsioonilisele enesemääramisele ja õigus oma sõnale ning pildile.[65]

[59] Isikuandmete kaitse seadus. - RT I, 30.12.2010, 11.
[60] Elektroonilise side seadus. – RT I, 01.07.2017, 2.
[61] Avaliku teabe seadus.- RT I, 04.07.2017, 11
[62] Eesti Vabariigi põhiseadus. - RT I, 15.05.2015, 2.
[63] Lõhmus, U. (2012). PõhiS § 26/9.4. – E. J Truuväli jt (toim) Eesti Vabariigi põhiseadus. Komm vlj. 2. vlj. Tallinn: Juura.
[64] RKHKo 3-3-1-3-12 p 19, 12.06.2012.
[65] *Supra nota* 49, § 26.

Õigusteadlase Robert Alexy arvates on informatsiooniline enesemääramisõigus üheks väga oluliseks osaks moodsas andmetöötluses, sest tavainimese jaoks tähtsusetuna tunduvad andmed võivad andmetöötluse läbi väga palju eraelulist infot paljastada. Õigus informatsioonilisele enesemääramisõigusele kui üldisele vabaduspõhisele õigusele ei ole Eesti riigis piiramatult tagatud. Riik võib ainult siis andmeid töödelda ja koguda, kui need on proportsionaalsed. Proportsionaalsed tähendab seda kui andmeid on töödeldud ainult vajalikus osas ning ei ole liialt töödeldud, kui see ei ole vajalik. Samuti peab ta oluliseks seda, kui informatsiooniline enesemääramis õigus muutub oluliseks olukorras, kus riik üritab läbi põhiseaduse §19 hankida teavet isiku iseloomu kohta.[66] Õigus isikuandmete kaitsele ei ole Eestis eraldiseisev põhiõigus ega ka selgesõnaliselt sätestatud, kuid see on tuletatav põhiseaduse §19 ja §26.

1.4.7. Isikuandmete kaitse seadus

Esimesed siseriiklikud isikuandmete kaitse seadused sätestati Euroopas 1970ndatel ja 1980ndatel aastatel.[67] Eestis võeti vastu esimene isikuandmete kaitse seadus 1996. aastal. [68] Kuna Eesti liitus Euroopa Liiduga, siis 2003. aastal tekkis vajadus viia kehtiv Isikuandmete kaitse seadus kooskõlla Euroopa Liidu andmekaitse üldmäärustikuga, tänu sellele täiendati seadust. Uues redaktsioonis jõustus seadus 2003. aastal, kuid selles tekkis palju sisulisi probleeme. Need parandati ning veel uuem redaktsioon jõustus 1. Jaanuaril 2008. Aastal.[69] Kõige uuem redaktsioon on tehtud 2015. aastal ning see jõustus 16. jaanuaril 2016. aastal ning see on ka hetkel kehtiv.[70]

Isikuandmete kaitse seaduse eesmärk on sätestatud § 1 lg 1, mis ütleb, et isikuandmete töötlemisel tuleb kaitsta füüsilise isiku põhiõigusi- ja vabadusi ning eelkõige õigust eraelu puutumatusele. Isikuandmete töötlemiseks on tegevus, mis võib rikkuda isikute põhiõigust. Isikuandmete töötlemiseks on Isikuandmete seaduse § 5 kohaselt on iga isikuandmetega tehtav toiming, mille hulka kuuluvad isikuandmete kogumine, salvestamine, korrastamine, säilitamine, muutmine ja avalikustamine, juurdepääsu võimaldamine isikuandmetele, päringute teostamine ja väljavõtete tegemine, isikuandmete kasutamine, edastamine, ristkasutamine, ühendamine, sulgemine, kustutamine või hävitamine.[71] Samuti on antud seaduses eraldi regulatsioon

[66] Alexy, R. (2001) Põhiõigused Eesti Põhiseaduses. - Juridica , eriväljaanne, p 6.1.2.2.
[67] Esimesena kehtestas 1970 aastal Saksamaa Liitvabariigi Hesseni liidumaa ning järgmisena Rootsi Kuningriik.
[68] Isikuandmete kaitse seadus. RT I 1996, 48, 944.
[69] Isikuandmete kaitse seadus. RT I 2007, 24, 127.
[70] Isikuandmete kaitse seadus. RT I, 06.01.2016, 10.
[71] Isikuandmete kaitse seadus §5.

isikuandmete avalikustamise näol. Isikuandmete avalikustamisel on tegemist töötlemise toiminguga, mis võib isikut kõige rohkem kahjustada.[72]

Isikuandmete kaitse seaduse eesmärkide loomisel võeti eeskujuks Euroopa Inimõiguste ja põhivabaduste konventsiooni artikkel 8 kui ka harta artikkel 8-st. Samuti tugineb Isikuandmete kaitse seadus oma põhimõtetel konventsioon nr 108-le.

Kuid Isikuandmete kaitse seaduse probleemiks on see, et kuna see põhineb põhimõtetel ning üldosal, siis spetsiifilistes valdkondades jääb selleks väheks. Selleks, et praktikas järgida seda, peab see olema tunduvalt spetsiifilisem. Samuti ei ole loodud eriseadusi. Tulenevalt sellest on Isikuandmete kaitse seadus liialt üldsõnaline ning pealiskaudne, nagu ka direktiiv.[73] Samuti on isikuandmete kaitse üldmääruses artiklis 5 sätestaud peamised põhimõtted isikuandmete töötlemisel:

"Isikuandmete töötlemisel tagatakse, et a) töötlemine on seaduslik, õiglane ja andmesubjektile läbipaistev b) isikuandmeid kogutakse täpselt ja selgelt kindlaksmääratud ning õiguspärastel eesmärkidel ning neid ei töödelda hiljem viisil, mis on nende eesmärkidega vastuolus;

c) isikuandmed on asjakohased, olulised ja piiratud sellega, mis on vajalik nende töötlemise eesmärgi seisukohalt

d) isikuandmed on õiged ja vajaduse korral ajakohastatud ning et võetakse kõik mõistlikud meetmed, et töötlemise eesmärgi seisukohast ebaõiged isikuandmed kustutaks või parandataks viivitamata.[74]"

Ülal toodud põhimõtted on kõige peamised, mis peavad tagatud olema, kui töödeldakse isikute andmeid, kuid üldmääruses on sätestatud ka veidi kitsamalt erinevad põhimõtted, mille tagamine töötlemisel on samuti oluline.

[72] Isikuandmete kaitse seaduse seletuskiri. Arvutivõrgus: http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/IKS%20SELETUSKIRI%20(1).rtf., (28.02.2018).
[73] Rohtmets, E. (2013) Eesti andmekaitse Euroopa Kohtu praktika peeglis. - Riigikogu toimetised 28. Arvutivõrgus: http://www.riigikogu.ee/rito/index.php?id=14437, 28.02.2018.
[74] Isikuandmete kaitse üldmääruse artikkel 5.

2. ISIKUANDMETE KAITSE ÜLDMÄÄRUS (GDPR)

Antud peatükis räägib autor uuest isikuandmete kaitse üldmäärusest, mis on igale euroopa liidu liikmesriigile kohaldatav 2018 aasta maist. Autor selgitab milles seisnevad üldmääruse suurimad muudatused ning milleks olid need muudatused vajalikud või millised suured kohtulahendid neid mõjutasid. Samuti leitakse vastus viimasele uurimisküsimusele. Autor seletab ka üldmääruses sisalduvaid põhimõtteid või printsiipe ning kuidas need on parandanud üksikisikute kontrolli iseenda andmete üle ning parandanud üleüldist isikuandmete kaitset.

Isikuandmete kaitse üldmääruse preambulas on sätestatud määruse eesmärk, milleks on:

"Füüsiliste isikute kaitse põhimõtete ja eeskirjadega nende isikuandmete töötlemisel tuleks nende kodakondsusest ja elukohast sõltumata austada nende põhiõigusi ja -vabadusi, eelkõige õigust isikuandmete kaitsele. Käesoleva määruse eesmärk on aidata kaasa vabadusel, turvalisusel ja õigusel rajaneva ala ning majandusliidu saavutamisele, majanduslikule ja sotsiaalsele arengule, riikide majanduse tugevdamisele ja lähendamisele siseturul ning füüsiliste isikute heaolule."[75]

Samuti on oluline märkida ka seda, et isikuandmete kaitse õiguse näol ei ole tegemist absoluutse õigusega, kuid liikmesriigid on kohustatud seda tasakaalustama muude põhiõigustega, et üldmääruse kohaldamine oleks tagatud proportsionaalsuse põhimõtetega. Samuti on üldmääruses viited era- ja perekonnaelu, kodu ja edastatavate sõnumite saladuse austamisele, isikuandmete kaitsest, mõtte-, südametunnistuse- ja usuvabadusest, sõna- ja teabevabadusest, ettevõtlusvabadusest, õigusest tõhusale õiguskaitsevahendile ja õiglasele kohtulikule arutamisele ning kultuurilisele, usulisele ja keelelisele mitmekesisusele.[76] Autor keskendub kõige enam era- ja perekonnaelu puutumatusele.

[75] Isikuandmete kaitse üldmääruse preambula.
[76] *Ibid*.

2.1. Läbipaistvusprintsiip

Läbipaistvus on väga oluline aspekt isikuandmete töötlemisel. See tähendab seda, et isikul, kelle andmeid töödeldakse on kontroll enda isikuandmete üle. Soovi korral on võimalik neid kustutada, muuta või täiendada. Selle hulka kuulub teavitamiskohustus, mis tähendab seda, et andmetöötleja teavitab andmesubjekti, et tema andmeid töödeldakse. Samuti tähendab see ka seda, et kui isik ei ole teadlik sellest, et keegi tema andmeid kogub ning mis mahus, on tal võimalus enda õigusi kaitsta. Direktiivi artikkel 5 punkt a sätestab, et isikuandmete töötlemisel tagatakse, et töötlemine on seaduslik, õiglane ja andmesubjektile läbipaistev.[77]

Samuti on direktiivi preambulas punktis 37 sätestatud läbipaistvuse põhimõte:

„[...] Läbipaistvuse põhimõte eeldab, et nende isikuandmete töötlemisega seotud teave ja sõnumid on lihtsalt kättesaadavad, arusaadavad ning selgelt ja lihtsalt sõnastatud. Kõnealune põhimõte puudutab eelkõige andmesubjektide teavitamist vastutava töötleja identiteedist ning töötlemise eesmärgist ja täiendavast teabest., et tagada asjaomaste füüsiliste isikute suhtes õiglane ja läbipaistev töötlemine ning nende õigus saada neid puudutavate isikuandmete töötlemise kohta kinnitust ja sõnumeid [78] [...].”

Antud preambula punkt räägib ka teavitamiskohustusest, et füüsilisi isikuid tuleks teavitada töötlemisega seotud ohtudest, kaitsemeetmetest ja õigustest ning kuidas neid õigusi kasutada. Samuti on seal mainitud, et andmeid tuleks töödelda ainult juhul, kui eesmärki ei ole võimalik saavutada teiste vahendite abil. Samuti on oluline isikuandmete töötlemisel tagada turvalisus ja konfidentsiaalsus.

Samuti on preambulas märgitud, et läbipaistvusprintsiibi eesmärgiks on, et andmesubjektile suunatud teave oleks arusaadav oma sõnastuse poolest. Antud printsiibi põhimõtte seletus on sätestatud preambula punktis 54 ning on sõnastatud selliselt:

[77] *Supra nota* 21, §5 a.

[78] *Ibid,* punkt 37.

„[...] Läbipaistvuse põhimõte eeldab, et üldsusele või andmesubjektile suunatud teave on kokkuvõtlik, lihtsalt kättesaadav ja arusaadav ning selgelt ja lihtsalt sõnastatud ning samuti tuleks vajaduse korral täiendavalt kasutada visualiseerimist[79][...].”

Antud punkt on oluline sellises olukorras, kus andmesubjektil on tehnoloogia keerukuse tõttu raske mõista kes ning millisel eesmärgil tema isikuandmeid kogutakse, nagu seda tehakse veebis oleva reklaami puhul. Samuti on keel oluline sellisel juhul, kui töödeldavat andmed on laste andmed. Koostatud lause peab olema nii lihtsalt ja arusaadavalt sõnastatud, et lapsed saaksid sellest aru. Lapse näol on autor pidanud silmas seda, et Eestis võib isikuandmete töötlemiseks anda nõusoleku 14 aastane laps. Kui laps on noorem kui 14 aastane siis lapse eest peab nõusoleku andma tema seaduslik esindaja.

Samuti on läbipaistvusprintsiipi oluline järgida isikul, kes viib läbi andmete töötlemist. See on ka üks õiglase töötlemise osadest. Töötlemise käigus tuleb andmesubjekti teavitada tema andmete töötlemisest. Määruse preambula punkt 60 täpsustab, kuidas vastutav töötaja peab käituma, kui töötleb andmeid. Punkt sätestab, et:

„[...] Vastutav töötleja peaks esitama andmesubjektile igasuguse täiendava teabe, mis on vajalik õiglase ja läbipaistva töötlemise tagamiseks, võttes arvesse isikuandmete töötlemise konkreetseid asjaolusid ja konteksti. Lisaks tuleks andmesubjekti teavitada profiilianalüüsi olemasolust ja sellise analüüsi tagajärgedest [...][80].”

Antud magistritöö autor on arvamusel, et mitmed punktid, mis on esindatud preambulas ning räägivad läbipaistvusprintsiibist, aitavad paremini tagada läbipaistvuse isikuandmete töötlemisel. Samuti on oluline punkt, kus mainitakse, et andmesubjektile esitatav keel peab olema arusaadav ja lihtne, et isik saaks aru, mis eesmärgil tema andmeid kogutakse või töödeldakse. Tihtipeale on andmetöötleja poolt esitatud privaatsustingimused liialt keerukad ning pikad. Seetõttu on raske andmesubjektil aru saada, mida tema isikuandmetega õieti tehakse või kuidas viiakse läbi tema andmete töötlemist. Samuti võib see sama punkt tekitada praktikas probleeme, kuna punkti sõnastus on küllaltki laialdane ning erinevalt mõistetav, kuna kasutatud on lihtsalt sõnastust, et teave oleks “kokkuvõtlik” ja “arusaadav”. Samuti on erinev inimeste teadlikus andmete töötlemisest ning seetõttu võib võime aru saada privaatsuse sätetest olla raskendatud. Eriti võib see probleeme tekitada ettevõtetes, kuna neil on raske aru saada kas nende ettevõttes rakendatud

[79] *Ibid* punkt 54.
[80] Isikuandmete kaitse üldmääruse punkt 60.

privaatsuspoliitika vastab “arusaadava” kriteeriumile või mitte. Samuti on punkt 54 oluline tänu sellele, et ettevõtted peavad esitama andmesubjektile nii arusaadavas keeles, et lapsed saaksid aru, miks nende andmeid töödeldakse. See on oluline tänu sellele, et lapsed ning noored on väga suur osa interneti kasutajatest ning noorte osakaal internetis suureneb iga aastaga. Eestis on alla 14 aastaselt nõutud nõusoleku andmiseks seadusliku esindaja nõusolek, kuid 14 aastane Eesti kodanik võib anda enda andmete töötlemiseks ise nõusoleku.

Üldmääruse artikkel 13 ja 14 sätestavad pika loetelu informatsioonist, mida andmetöötleja peab andmesubjektile esitama, kui töötleb tema andmeid. Samuti tuleb teavitada andmesubjekti sellest, kas tema andmeid kogutakse töötlemiseks vajalike minimaalsest kogust rohkem ning kas andmeid kogutakse mingiks teiseks otstarbeks, kui see, milleks neid algselt koguti. Loetelus on mainitud ka see, kas andmed salvestatakse krüpteeritult ning kaua isikuandmeid säilitatakse, ning et isikul on õigus esitada kaebus vastavasse järelevalveasutusele. Tänu nendele kahele punktile on ettevõtetel võrreldes varasemaga suuremad kulutused. Samuti on üldmääruse artiklis 15 kirjas andmesubjekti õigused tutvuda enda kohta kogutud andmetega.

Töö autor on arvamusel, et mitmed punktid tagavad läbipaistvusprintsiibist kinnipidamise ning tänu nõutavale läbipaistvusele on andmesubjektid rohkem teadlikud andmete töötlemisest ja nendega kaasnevatest õigustest ning privaatsusnõuetest. Samuti on artiklid 13 ja 14 väga tõhusad, et tagada füüsilistel isikutel parem ülevaade nende kohta kogutavatest andmetest ning sellele aitab kaasa ka see, et andmetöötleja peab teavitama andmete töötlemisest andmesubjekti. Üldmäärus on kasulik ka andmetöötlejale oma toimingute läbiviimisel kui ka aitab ettevõtetel mõista, et kas nad on taganud kõik privaatsuspoliitikad, mis on direktiivis ettenähtud. Kokkuvõtvalt võib öelda, et nii preambulas olevad punktid kui mõned üldmääruse artiklid on väga efektiivsed, et tagada korrektne andmete töötlemine ning korrektne teavitamine andmesubjektile.

2.2. Andmetöötleja kohustused

Uue üldmäärusega soovitakse vabaneda ebaselgusest, mis on seotud vastutatava töötlejaga, kes viib läbi andmete töötlemist. Enamik isikuandmete töötlemisest toimub pilveandmetöötlusena (ing. k. *cloud computing).* Pilveandmetöötlus tekkis tänu suurtele infotehnoloogia ettevõtetele nagu Google, Amazon jne, kes ehitasid iseenda firma jaoks suuri andmetöötlus keskus, kus oli väga kiire internetiühendus. Pilveandmetöötlus tähendab seda, et andmeid ei salvestata

füüsilistele andmekandjatele vaid neid salvestatakse ja töödeldakse suures "pilves", mis asub internetis. Pilveandmetöötluse korral kasutaja salvestab või töötleb andmeid serverites, millel on kasutajal interneti vahendusel juurdepääs spetsiifilise tarkvara abil.[81] Pilveteenuste plussiks on see, et see võimaldab suurt salvestusmahtu. Andmetöötluse koha pealt on see kasulik tänu sellele, et avalik- ja erasektor saavad väiksemate kuludega kasutada kaasaegset tehnoloogiat ning osutada paindlikumat info-ja kommunikatsioonitehnoloogia teenuseid.[82] Pilv on infotehnoloogiline teenus, mis võimaldab salvestada ja jagada teenuseid ning neid internetis kiiresti hallata. Selle plussiks on see, et firmad hoiavad kokku enda halduskulude pealt, firmad saavad kiiremini oma rakendusi hallata, parandada nende juhitavust ning nõuab vähem hooldust. Pivli on olemas kolme sorti. Nendeks on privaatne pilv, avalik pilv ja hübriid pilv, mis koosneb nii privaat kui avalikust pilvest. Privaatne pilv on mõeldud ühe isiku või ühe organisatsiooni töö jaoks. Avalik pilv tähendab seda, et pilv asub kohas, kus seda saavad kõik kasutada ning see pilv on tasuta. Samuti on olemas ka suure andme ehk *big data cloud*, kus tehakse esmaklassilisi ning mahukaid it teenuseid.

Üldmääruses on ette nähtud vastutuse printsiip, mis tagab selle, et vastutav töötleja rakendaks meetmeid, mis tagavad andmete töötlemise kooskõla üldmääruses sätestatuga, ning et vastutav töötleja oskaks neid meetmeid demonstreerida, kui järelevalveasutus seda soovib. Antud meetmed on sätestatud üldmääruse artiklis 5, mis ütleb, et:

„[...] isikuandmeid töödeldakse viisil, mis tagab isikuandmete asjakohase turvalisuse, sealhulgas kaitseb loata või ebaseadusliku töötlemise eest ning juhusliku kaotamise, hävitamise või kahjustumise eest, kasutades asjakohaseid tehnilisi või korralduslikke meetmeid („usaldusväärsus ja konfidentsiaalsus");

Lõike 1 täitmise eest vastutab ja on võimeline selle täitmist tõendama vastutav töötleja („vastutus")[...][83].

Üldmääruse preambula punkt 23 sätestab, et:
„[...] Selle tagamiseks, et füüsilise isikud ei jää ilma kaitsest, millele neil on õigus käesoleva määruse alusel, tuleks käesolevat määrust kohaldada väljaspool liitu asuva vastutava töötleja või

[81] Parm, U. (2014) Pilveandmetöötlus:
arvutivõrgus http://www.aki.ee/et/pilvandmetootlus (6.03.2018)
[82] *Ibid.*
[83] Üldmääruse artikkel 5

volitatud töötleja poolt liidus olevate andmesubjektide isikuandmete töötlemise suhtes, kui isikuandmete töötlemise toimingud on seotud kaupade või teenuste pakkumisega kõnealustele andmesubjektidele, sõltumata sellest, kas see on seotud maksega või mitte [...].[84]"

Üldmääruse 4 peatükk keskendub vastutava ja volitatud töötaja kohustustele. Artikkel 24 sätestab vastutava töötleja vastutusega seotud tingimused ning artikkel 26 sätestab, et kes on kaasvastutavad töötlejad. Üldmääruse artikkel 28 sätestab volitatud töötleja kohustused. Üldmääruse 4 jagu, mis on seotud järelevalvega ning andmekaitseametnikega, määravad millal tuleb tööle kaasata andmekaitseametnik. Artikkel 37 sätestab, et:

„[...] Vastutav töötleja ja volitatud töötleja määravad andmekaitseametniku, kui

a) isikuandmeid töötleb avaliku sektori asutus või organ, välja arvatud oma õigust mõistvat funktsiooni täitvad kohtud;

b) vastutava töötleja või volitatud töötleja põhitegevuse moodustavad isikuandmete töötlemise toimingud, mille laad, ulatus ja/või eesmärk tingivad ulatusliku andmesubjektide korrapärase ja süstemaatilise jälgimise, või

c) vastutava töötleja või volitatud töötleja põhitegevuse moodustab artiklis 9 osutatud andmete eriliikide ja artiklis 10 osutatud süüteoasjades süüdimõistvate kohtuotsuste ja süütegudega seotud isikuandmete ulatuslik töötlemine. [...][85]

Magistritöö autor on arvamusel, et uue peatüki lisamine on suur edasiminek parema direktiivi suunas. See tagab parema läbipaistvusprintsiibi tagamise ning sätestab paremini ning selgemini vastutava töötleja ja volitatud töötleja vastutuse ning nende tööülesanded. Samuti on sellega tagatud karmimad sisekontrolli nõuded ja täpsem järelevalve kontroll. Andmesubjektil on ka parem ülevaade sellest, mis andmetöötlejad tema andmetega tegelevad ning samuti on ka arusaadav andmetöötlejate töökohustused. Kokkuvõtvalt tagavad need artiklid läbipaistvusprintsiibi kasutamist kui ühe põhieesmärgi direktiivi põhimõtetest.

[84] Üldmääruse preambula punkt 23
[85] Üldmääruse artikkel 37

2.3. Suurandmed ehk big data töötlemine

Suurandmed on antud magistritööga seotud tänu sellele, et suurandmete kogumise näol on tegemist suuremahulise andmete töötlemisega, tänu sellele on autor pidanud vajalikuks seletada suurandmete olemusest ning nende töötlemisel kaasnevatest ohtudest. Termin "suurandmed" tuleneb sotsiaaltehnoloogilisel arengul, mis sai oma alguse arvuti leiutamiseks ning millest on aastate jooksul tekkinud väga kiiresti arenev dünaamiline jõud.[86] Suurandmeid võib samastada internetiga, kuna mõlema näol on tegemist tehnoloogilise trendiga, mis on tekkinud sellel sajandil. Suurandmed tähendavad seda, et kuidas koguda nii palju kui võimalik andmeid inimeste ning nende igapäevaste harjumuste näol kokku ning kuidas neid saadud andmeid analüüsida.[87] Tegemist on andmemassiga, mis tuleneb erinevatest allikatest ning mida ei saa analüüsida, kasutades ainult ühte arvutit või ühte suurt serverit. Suurandmestik on kujundanud välja viisi kuidas ühiskond erinevaid saadud andmeid töötleb.[88] Suurandmete kogumise teel saavad kokku väga erinevad andmed ning ka väga suures mahus. Tänu sellele on vaja selliste andmete töötlemiseks väga suurt kiirust ning see kiirus aina suureneb.[89] Samuti ka mitmeid arvuteid ning servereid.

Suure kiirusega töötlemisel suureneb aga saadud andmete kogumise maht. Sellise suure andmete mahu kogumiseks on vaja rohkem vaba ruumi. Mitmeid aastaid tagasi mõõdeti andmete mahtu megabaitides, siis tänapäeval aga terabaitide, petabaitide ning eksabaitidega.[90] Suurandmete töötlemine on tihedalt seotud andmekaitsega. Andmete töötlemisel tuleb järgida andmekaitse teemalisi nõudmisi kui andmeid salvestatakse, kogutakse, andmete turvalist käsitlemist ning kui kaua võib suurandmeid serverites säilitada. Kuna suurandmed koguvad igasuguseid andmeid siis nende andmete töötlemiseks on vaja kasutada andmekaevet, et see eristaks kasuliku informatsiooni tarbetust või mitte vajalikust informatsioonist. Andmekaeve meetodit nimetatakse

[86] Bosco, F, Creemers, N. (2015) Profiling Technologies and Fundamental Rights and Values: Regulatory Challenges and Perspectives from European Data Protection Authorities. – Reforming European Data Protection Law. Dordrecht: Springer, lk 4.
[87] Reno, J. (2012) Big Data, Little Privacy. – CA Technology Exchange. Insights from CA Technologies, nr 3 (2), lk 28-32.
[88] Cukier, K. (2013) The Rise of Big Data. How It's Changing the Way We Think About the World. – Foreign Affairs 2013, nr 92, lk 28-29.
[89] Michael, K. (2013) Big Data: New Opportunities and New Challenges. – IEEE Security & Privacy. IEEE Computer Society, lk 22-24.
[90] Waschke, M. (2012) Introduction to the Big Data. - CA Technology Exchange. Insights from CA Technologies. nr 3 (2), lk 1.

profileerimiseks. Profileerimise näol on tegemist automatiseeritud andmekaeve meetodikaga, mis ongi mõeldud ainult suurandmete töötlemiseks. Profileerimise käigus struktureeritakse andmeid, et tekiksid erinevad kategooriad ning need kategooriad koosnevad võimalikult sarnaste tunnustega andmetest. Samuti selle käigus jagatakse andmeid selliselt, et andmetest oleks võimalik leida sarnaseid mustreid ja tõenäosusi. Nende kategooriate pinnalt on võimalik teha erinevaid prognoose, mis ennustavad ette trende, protsesse ja arenguid, mis toimuvad tulevikus ning selle eesmärgiks on see, et tulevikus tuleks tegeleda võimalikult vähe ebamäärasustega.[91]

Suurte andmete kasutamisel või analüüsimisel on kõige olulisem tagada üksikisikute andmete kaitse ning ka üksikisikute eraelu ja kodu puutumatus. Suurandmete tehnoloogiaid kasutades on võimalik eraldada andmeid avalikest andmetest, mis võivad olla kahjustavad.[92] Kuna suurte andmete käsitlemisel on andmeid nii palju, muutub nende andmete turvalisuse tagamine vägagi keerukaks. Samuti on oluline märkida seda, et profileerimise käigus ei tea isikud, et nende andmeid hakatakse koguma või töötlema ning profileerimiseks isiku nõusoleku küsimine ei ole mõistlik, kuna ei teata mis olukordades tuleks nõusolekut küsida ning millal mitte. Profileerimise käigus luuakse ka profiile, mis ei koosne isiku andmetest ning tänu sellele oleks nõusoleku küsimine tarbetu. Tegemist ei ole läbipaistva toiminguga, kuid selleks, et ka profileerimine muutuks läbipaistvaks on vaja väga spetsiifilisi sätteid, mida veel loodud ei ole. Samuti on neid sätteid keerukas luua, kuna profileerimise käigus puututakse kokku nii paljude erinevate kui ka suure hulga andmetega.

2.4. Termin "õigus olla unustatud"

Isiklikud andmed on muutunud väärtuslikuks tooraineks, mis pakuvad suurkorporatsioonidele nagu Google ja Facebook tööd. Ehkki varajases staadiumis oli vaja ühtset lähenemisviisi isikuandmete liikumise reguleerimisel jurisdiktsioonipiirkondade piires, on see kohustus veelgi olulisem isikliku teabe allhangete ja jurisdiktsiooni alla kuuluva isikuandmete haldamise keskkonnas.[93] Üheks viisiks neid isikuandmeid hallata ongi üksikisikute kontroll enda andmete üle, ehk kui on soov Google otsingumootorist enda andmeid kustutada, siis selleks on leidunud ka võimalus. Kuid kuidas seletada antud terminit"õigus olla unustatud"?

[91] *Supra nota* 81, lk 4.
[92] *Supra nota* 85, lk 3.
[93] Gunasekara, G. (2014). Paddling in unison or just paddling? International trends in reforming information privacy law. *International Journal of Law and Information Technology, 22*(2), 141-177, lk 143.

"Õigus olla unustatud" on oma intellektuaalse päritolu saanud Prantsuse õigusest, mis annab "right to oblivion"[94] ehk eesti keeles õigus unustusele, see tähendab ka seda, et süüdimõistetu võib esitada süüdimõistva kohtuotsuse asjaolude avaldamisele vastuväite, kui ta on oma karistuse kandnud.[95] Selle eesmärgiks praktikas oli aidata kurjategijatel uut elu alustada ning ennetada seda, et uuesti ei avaldataks infot varasemalt toime pandud kuritegude kohta. Isikuandmete kaitse valdkond on muutunud järjest päevakohasemaks seoses tehnoloogia arenguga. Avalikkuse suurenenud huvi isikuandmete kaitsmise vastu kinnitab asjaolu, et kohtusse laekub järjest enam kaebusi, mille sisuks on andmesubjekti õigus vaidlustada andmete edasist töötlemist ning õigust olla unustatud.[96] Samuti on Euroopa Komisjon pidanud "õigust olla unustatud" üheks andmekaitsereformi neljaks alussambaks.[97]

"Õigus olla unustatud" idee peamiseks põhjuseks on interneti digitaalmaailma käsitleva teabe kättesaadavuse ja juurdepääsetavuse kiire laienemine.[98] Tänu otsingumootoritele on mälu nüüd perfektne ning lõpmatu. Informatsioon ning selle jagamine on tähtsad komponendid kultuurist arusaamisel ning identiteet kujunemisel ja teistele nähtavaks tegemisel. Kontroll informatsiooni üle tähendab kontrolli läbipaistvuse üle ning tegemist on tähtsa osaga demoktraatlikust süsteemist.[99] Selleks, et mõista teooriat ning praktikat, mis on seotud terminiga "õigus olla unustatud", tuleb kõige pealt seletada, mida antud termin tähendab. Termin "õigus olla unustatud" on märgitud uues andmekaitsemääruses ning see käsitleb õigust andmete kustutamisele. Õigus unustusele on kõigi nii füüsiliste kui ka juriidiliste isikute õigus, ka juriidilisel isikul võib olla huvi, et tema kohta avaldatud informatsioon peale teatavat ajavahemikku kustutatakse.[100] Termin "õigus olla unustatud" on sätestatud määruse artiklis 17:

„[...] Andmesubjektil on õigus nõuda, et vastutav töötleja kustutaks põhjendamatu viivituseta teda puudutavad isikuandmed ja vastutav töötleja on kohustatud kustutama isikuandmed põhjendamatu viivituseta, kui kehtib üks järgmistest asjaoludest:

a) isikuandmeid ei ole enam vaja sellel eesmärgil, millega seoses need on kogutud või muul viisil töödeldud;

[94] Prantsuse keeles - *le droit d l'oubli.*
[95] Walker, R. (2012). The right to be forgotten. *Hastings Law Journal* 64(1), 257.
[96] Hansen, T. (2014) Euroopa Inimõiguste Kohtu praktika kohtuotsustes isikuandmete avaldamisel, J*uridica*, 4, lk 313-324, lk 313.
[97] European Commission MEMO 13.03.2018
[98] McGoldrick, D. (2013). Developments in the Right to be Forgotten. *Human Rights Law Review, 13*(4), 761-776.
[99] *Ibid*, lk 763.
[100] Liiv, E. (2014) Kas eraisikul on õigus unustusele Internetis? J*uridica*, 9, lk 643-651, lk 649.

b) andmesubjekt võtab töötlemiseks antud nõusoleku tagasi vastavalt artikli 6 lõike 1 punktile a või artikli 9 lõike 2 punktile a ning puudub muu õiguslik alus isikuandmete töötlemiseks;

c) andmesubjekt esitab vastuväite isikuandmete töötlemise suhtes artikli 21 lõike 1 kohaselt ja töötlemiseks pole ülekaalukaid õiguspäraseid põhjuseid või andmesubjekt esitab vastuväite isikuandmete töötlemise suhtes artikli 21 lõike 2 kohaselt;

d) isikuandmeid on töödeldud ebaseaduslikult;

e) isikuandmed tuleb kustutada selleks, et täita vastutava töötleja suhtes kohaldatava liidu või liikmesriigi õigusega ette nähtud juriidilist kohustust;

f) isikuandmeid koguti seoses artikli 8 lõikes 1 osutatud infoühiskonna teenuste pakkumisega. [...][101]

Üldmääruse artikkel 17 (2) näeb ette, et vastutav töötleja võtab tarvitusele vajaliku meetmed, et teavitada kõnealuseid isikuandmeid töötlevaid vastutavaid töötlejaid sellest, et andmesubjekt taotleb neilt kõnealustele isikuandmetele osutavate linkide või koopiate kustutamist.[102] Antud muudatustega muudetakse seda, et kui varem pidi andmesubjekt põhjendama, miks antud andmeid ei tohiks töödelda, siis nüüd on see ettevõtte kohustust.

Artikkel, mis oli kolmkümmend kuus sõna pikk, oli see, mis muutis internetti.[103] Tegemist oli *Google vs. Spain* kohtulahendiga. *Google vs. Spain* lahend tõi palju tähelepanu küsimusele, kas andmeid peaks saama internetist kustutada või mitte.[104] Samuti kaasnes selle kohtulahendiga ka see, et tekkis võimalus enda andmeid kustutada.[105] Antud kaasuse sisuks oli, et Hispaanias elav Hispaania kodanik esitas Hispaanias olevale andmekaitseametile suure levikuga meediaväljaannete Google Spain ja Google Inc vastu kaebuse.

Kaebuse sisuks oli, et kui interneti kasutaja sisestab Google'i otsingumootorisse (Google search) kaebaja nime, kuvatakse tulemuste seas lingid ühe 1998.a ajalehe lehekülgedele ning nendel lehekülgedel on koos kaebaja nimega avaldatud arestitud kinnisvara enampakkumiste kohta.[106] Kaebaja soovis, et ajalehe väljaanded eemaldaksid need leheküljed või muudaks neid nii, et tema

[101] Üldmääruse artikkel 17
[102] Üldmääruse artikkel 17 (2)
[103] Shahin, S. (2016). Right to Be Forgotten. *Journalism & Mass Communication Quarterly, 93*(2), 360-382.
[104] EIKo 13.05.2014, c-131/12, *Google vs. Spain*.
[105] Carbone, C. E. (2015) To Be or Not to Be Forgotten: Balancing the Right to Know with the Right to Privacy in the Digital Age. Virginia Journal of Social Policy & the Law, 22 (3), lk 525-560, lk 553.
[106] *Supra nota* 74, lk 647.

isikuandmeid ei ole näha või muutma kuidagi otsingumootorite poolt võimaldatavaid vahendeid, et tema isik ei oleks tuvastatav. Samuti soovis ta, et Google'i äriühingud eemaldaksid tema andmed või peidaksid need, et need ei ilmuks enam otsingutulemustes. See kõik oli kaebaja jaoks oluline tänu sellele, et tegemist oli vana asjaga, mis oli lahendatud juba aastaid tagasi ning tollasel ajal see ei omanud enam tähtsust. Veebruaris 2016. a Google teavitas, et laiendab "õigus olla unustatud" kõikidele ettevõtete domeenidele, mis on lokaliseeritud Euroopa Liidus,[107] kuid ei laiendanud sama õigust Ameerika Ühendriikides olevatele ettevõtetele. Peale antud kohtulahendi jõustumist 2014. a rohkem kui 500 000 inimest esitasid Google'le palve, et kustutada nende andmed Google otsingumootorist.[108] Google esitas 2015.a raporti, mis näitas milliseid interneti lehekülgi on internetikasutajad soovinud kustutada "õigus olla unustatud" raames. Antud raportist selgus, et kõige rohkem on isikud soovinud kustutada otsingumootorist viiteid Facebooki kontole ning top 10 hulka kuulusid ka YouTube ning Twitter.[109]

Termin "õigus olla unustatud" tähendab olukorda, kus andmesubjekt teostab interneti otsingumootorile päringu ning otsingutulemuste seast leiab enda kohta andmeid. Antud tulemuste seast soovib andmesubjekt andmete eemaldamist ning kohustab otsingumootoreid teatud tingimustele vastava andmete eemaldamist. See kohustus rakendub praktikas siis, kui andmesubjekti isikuandmed on nime otsingumootorisse sisestamisel tulemuste seas ning viitavad ka teistele internetilehekülgedele. Praktikas andmete kustutamist ei toimu, vaid selle kohustuse kohaselt kaotatakse isikuandmete puhul seos selle isiku nimega. Informatsioon jääb veebilehele alles, kuid internetikasutaja ei leia seda enam otsingumootorit kasutades. Tänu sellele ei taga antud termin isikule täieliku võimaluse enda kohta käivaid andmeid internetist eemaldada.

Kui eelnevalt sai mainitud, et Google nõustus eemaldama andmed, mis on lokaliseeritud Euroopa Liidu domeenide raames, siis üks kohtulahend on seda praktikat teistsuguseks muutnud. 2015. a veebruaris nõudis Prantsusmaa jurist nimega Dan Shefet, et Google'i filiaal, mis asub Pariisis, eemaldaks kõik internetilehekülјed, mis on seotud tema minevikuga ning laimavad, kuna see on halb praksisele, kus ta töötab. Google nõustus sellega ning eemaldas kõik tulemused Euroopa otsingumootori tulemustest, kuid Dan Shefet ei olnud sellega rahul,,kuna ta väitis, et eemaldamine Euroopa otsingumootoritest ei lahenda sellega kaasnevat probleemi, kuna ta töötab

[107] Byrum, K. (2017). The European right to be forgotten: A challenge to the United States Constitution's First Amendment and to professional public relations ethics. *Public Relations Review, 43*(1), 102-111.
[108] Tirosh, N. (2017) Reconsidering the 'Right to be Forgotten' – memory rights and the right to memory in the new media era. *Media, Culture & Society*, Vol.39(5), lk 644-660.
[109] Kelly, M. J.; Satolam, D. (2017). The right to be forgotten. *University of Illinois Law Review* 2017(1), 1-64.

rahvusvahelises firmas ning näiteks Ameerika Ühendriikide otsingumootorites on tulemused veel alles. Selle peale pöördus jurist Prantsuse kohtu poole. Prantsuse kohtus saavutas ta võidu ning Google kaotas kohtuvaidluse. Google oli kohustatud eemaldama kogu internetist viited Dan Shefeti andmetele. Samuti selleks, et tagada see, et Google emaettevõte Google Inc. Ameerika Ühendriikides peaks kinni kokkulepitust, määrati Google'i Pariisis asuvale filiaalile 1100 dollarit päevas trahvi, kuni emaettevõte eemaldab vastavad andmed kogu internetist. Kuid antud juhul peab silmas pidama, et tegemist oli erijuhtumiga. [110]

Kuna internet muutub kiiresti, siis muutuvad ka nendes olevad andmed. Samuti on aja jooksul allikate maht suurenenud ning selle tagajärjel toimub ka informatsiooni kiirem vahetumine. Mida rohkem informatsiooni otsitakse või kasutatakse, seda rohkem uudset informatsiooni luuakse. Inimesed aitavad kaasa informatsiooni loomisele tänu selle kasutamisele. Inimeste sekkumine informatsiooni suurendab selle väärtust oluliselt.[111] "Õigus olla unustatud" aspekt aitas kaasa sellele, et Google lõi otsingumootorisse teabevormi, mille kaudu isikud saavad oma andmeid kustutada. Antud teabevormi näol on tegemist kasutajasõbraliku ja tõhusa viisiga, kuidas oma andmeid veebist kustutada.

Muudatused, mis kaasnesid *Google vs. Spain* kohtulahendiga tõid kaasa mitmeid valikuvõimalusi kaitsmaks enda isikuandmeid. Samuti aitab "õigus olla unustatud" otsustada enda isikuandmete saatuse üle ning kui andmesubjekt peab vajalikuks, siis on võimalik ka lasta need eemaldada. Informatsiooni eemaldamiseks saab põhineda mitmetel õiguslikel regulatsioonidel. Nendeks on kohtulahendid, mis põhinevad antud teemal, uus andmekaitsedirektiiv ning praktikast tulenevad erinevad õiguslikud tõlgendused, mis aitavad isikul põhjendada miks on vajalik tema isikuandmed veebist eemalda. "Õigus olla unustatud" on aspekt mille määratlus on väga mitmekesine ning lai ning seda on lihtne kasutada. Kuid siinkohal tuleb meeles pidada seda, et "õigus olla unustatud" näol ei ole tegemist absoluutse õigusega.

[110] Arvutivõrgus: https://uk.reuters.com/article/us-eu-google-privacy-lawyer/lawyer-who-won-against-google-takes-privacy-case-to-brussels-idUKM1KBN0OR2D520150611
(15.03.2018)

[111] Ambrose, M. L. (2013) It's About Time: Privacy, Information Life Cycles, and the Right to Be Forgotten. Stanford Technology Law Review, 16 (2), lk 369-422, lk 394.

"Õigusel olla unustatud" on olemas ka negatiivsed mõjud ning antud kontseptsioon on leidnud internetis kriitikat. Näiteks kuna seda õigust on võimalik mitmeti mõista, siis võib see kujutada ohtu informatsioonilisele juurdepääsule ja online sõnavabaduse suhtes.[112] Samuti kuna andmete eemaldamine Google'st on muudetud võimalikult lihtsaks siis seda võimalust võivad ära kasutada terroristid või teised halva tähelepanuga organisatsioonid. Näiteks kurjategijad, kes varjavad ennast politsei eest saavad ennast kaitsta sellega, et eemaldavad andmed internetist ning saavad kergesti uut elu alustada. Samuti kehtib ka see sõjakurjategijatele, kes ei soovi enda isikut paljastada. Nad saavad väita, et teatud ühendused või informatsioon internetilehekülgedel on avalikkusele tähtsusetu ning langeb nende privaatsuse- ja isikuandmete õiguse kaitse alla.[113]

Samuti ei ole enamus teadlik sellest, kuidas Facebook kasutab nende andmeid selleks, et firmad saaksid oma reklaamide abil oma kaupu või teenuseid müüa. Paljud inimesed on kindlasti täheldanud seda, et kui üks päev on nad Google otsingumootorit kasutanud selleks, et otsida mõne ravimi kohta informatsiooni ning järgmisel hetkel minnes Facebooki on seal selle otsitava ravimi reklaamid. Sellist teenust teostatakse läbi erinevate küpsiste. Küpsised annavad reklaamipakkujatele teada, kes sa oled ning annavad ka teada, et teile on võimalik nende teenust või toodet pakkuda, kuna informatsiooni põhjal saab järeldada, et te olete huvitatud nende tootest või teenusest.[114] Antud informatsioon tuleb isikute profiili info põhjal, jagatud postituste järgi, saadetud sõnumite järgi, üleslaetud failide järgi, üleslaetud failide asukoha järgi või siis teiste isikute kaudu kellega ollakse Facebookis kuidagi seotud, kas siis sellega, et antud isikut on märgitud kellegi teise pildi peal või see isik on nende sõbralistis. Facebook töötleb väga suures mahus kasutajate andmeid ning Facebookis toimub ka väga palju turundamist, mille jaoks need andmed vajalikud on.

Teine oluline lahend, mis on seotud andmete säilitamise ning hävitamisega on *Digital Rights Ireland v Minister for Communications, Marine and Natural Resources, Seitlinger and Other.*[115] Antud kohtulahendis leiti, et *elektroonilise andmeside direktiiv 2006/24/EÜ* on kehtetu. Kehtuks loeti see tänu sellele, et andmete säilitamise direktiivis toodud meetmed sideandmete massiliseks säilitamiseks ei ole proportsionaalsed ning antud direktiiv on vastuolus Euroopa Inimõiguste ja

[112] Fazlioglu, M. (2013) Forget me not: the clash of the right to be forgotten and freedom of expression on the Internet, *International Data Privacy Law,* vol. 3, no. 3, lk 157.
[113] Peltz-Steele, R. J. (2013) The New American Privacy. *Georgetown Journal of International Law*, 44 (2), lk 365-410, lk 379.
[114] https://news.sky.com/story/what-does-facebook-do-with-my-data-and-how-do-i-stop-it-11299792 (11.05.2018)
[115] EIKo 08.04.2014, C-293/12 ja C-594/12, *Digital Rights Ireland v Minister for Communications, Marine and Natural Resources, Seitlinger and Others*

põhiõiguste konventsiooniga. Riive hõimab põhiõiguste harta artiklis 7 sätestatud õigust eraelu puutumatusele ning isikuandmete töötlemine riivab artiklis 8 sätestatud õigust isikuandmete kaitsele. Kohtu arvamuses pidas kohus õigust eraelu puutumatusele niivõrd oluliseks, et otsustas piirata sideandmete kogumist ja kasutust.[116] Kohus jõudis järeldusele antus kohtulahendis, et sideandmete kogumine kui ka siseriiklike ametiasutuste ligipääs nendele andmetele kujutavad endast privaatsusõiguse rikkumist. Seda tänu sellele, et kogutud sideandmed võimaldavad teha järeldusi isiku eraelu kohta ning tänu sellele on võimalik isikut tuvastada. Nende andmete põhjal on võimalik teada saada isiku igapäevaste harjumuste kohta, informatsiooni alalise elukohta kohta, sotsiaalsete gruppide kohta ning nende kellega ta lävib. Tänu sellele, et kui kasutatakse neid andmeid hiljemalt võib isikule jääda mulje, et tema eraelu jälgitakse.

Kohtu arvates on sideandmed sama privaatsed kui sideseansi sisu ning nende kasutamine on raske riive privaatsusõigusele. Samuti oli kohus arvamusel, et Euroopa Liidu õigust tuleb tõlgendada kitsendavalt ning andmetele ligipääsu saab lubada ainult siis, kui soovitakse ennetada raskeid kuritegusi.[117] Kuid Euroopa Kohtu arvates ei olnud õigustatud olukord, kus andmeid koguti isikute kohta, kelle suhtes ei ole mingeid tõendeid, et nendel isikutel oleks kaudne seos raskete kuritegudega.[118] Andmeid võib koguda ainult siis, kui on kindlad tõendeid, et see isik on seotud raske kuriteoga või tahab sooritada rasket kuritegu või on mõni teine oht julgeolekule. Kohus rõhutas ka seda, et andmete ligipääs peab jääma proportsionaalsuse põhimõtte piiridesse. Kuid on olemas ka erandid, et mis juhul võib andmetele ligipääseda. Nendeks on siis seaduses sätestatud tagatised, mis kirjeldavad täpseid eeskirju, et millistel asjaoludel ja millistes tingimuste kohaselt peavad sideettevõtjad andma riigi pädevatele asutustele juurdepääsu andmetele. Selle näol on tegemist põhiõigust piirava erandiga ning seda on kohustatud tõlgendama kitsendavalt. Kuid see tagatis peab läbima eelneva kontrolli kohtu näol ning alles siis võivad pädevad asutused tegutseda. Samuti mainis kohus, et kuidas tuleb andmetega käituda, kui säilitamistähtaeg on läbi. Kohus nõudis, et liikmesriigi õigusnormid peavad tagama selle, et eriti kõrgel tasemel kaitse ja turvalisuse ning, et andmeid säilitatakse liidu territooriumil ning peale säilitamistähtaja lõppu hävitatakse saadud andmed.[119]

[116] Ginter, G. Schasmin, P. (2017) Lahendite *Tele2 Sverige* ja *Digital Rights Ireland* mõju sideandmete mugavkasutusele Eestis. Juridica, 1, lk 43.
[117] *Ibid.*
[118] *Supra nota* 116, lk 47.
[119] *Supra nota* 116, lk 48.

2.5. "Õigus olla unustatud" kollisioon USA õigusega

Antud magistritöö keskendub Euroopa Liidus vastuvõetavale uuele andmekaitsemäärusele, mis ei kehti Ameerika Ühendriikides, kuid sellest olenemata peab autor oluliseks rääkida täpsemalt kuidas on see siiski seotud USA õigusega. Interneti puhul on tegemist väga mahuka informatsiooniallikaga. Samuti veedavad inimesed tänapäeval palju rohkem aega oma nutiseadmetes ning reisimiseks on rohkem võimalusi ja vabadust, tänu sellele levib informatsioon ka teiste kontinentide vahel. Seadusi tehakse riigi või liidu tasandil, kuid internet on globaalse levikuga, ületades riigi territoriaalseid piire, milles seadused on loodud.[120] Samuti tagab interneti kättesaadavus andmete vaba liikumise ning seda nii liidu piirides, kui ka piire ületades. Ühtse digitaalse turu eesmärkideks ongi andmete vaba liikumine, kuid järgida tuleb põhimõtet, et andmeid edastatakse riikidesse, kus on töötlemisel tagatud volitatud töötaja poolt ka isikuandmete tõhus kaitse.

Mitmed suured internetiettevõtted nagu Google või Facebook on USA'st pärit ning nende vahendusel toimib Euroopa Liidus massiline infovahetus. Kuid võrreldes Euroopa Liiduga on USA-s andmekaitse, privaatsuse ja sõnavabadusega kehtivad regulatsioonid teistsuguse sisu ja põhimõtetega. Ameerika Ühendriikide privaatsusõigus koosneb killustunud süsteemis föderaalsetest ning osariikide seadustest. Privaatse informatsiooni kasutamine on teatud valdkondades reguleeritud, näiteks on olemas patsientide registrid, mootorsõidukite registrid, kuid puudub ühtne regulatsioon isikuandmete kaitsele tervikuna.[121] Samuti on USA-s kui tavaõiguslikus õigussüsteemis lisaks seadustele ka kohtute loodud pretsedendid, mis *common law* riikides võrreldes kontinentaalse õigussüsteemi riikidega omavad väga suurt rolli.[122] USA isikuandmete kaitse puudulikkus seisneb selles, et paljud andmesubjektidega seotud andmed, mis Euroopa Liidus on isikuandmetega kaitstud ei ole seda Ühendriikides.[123] Samuti ei ole USA's seadusandlikul tasandil leidnud tunnustust mitmed olulised põhimõtted, mis Euroopa Liidu andmekaitse korral on olulised ning mida rakendatakse andmete töötlemisel. Kokkuvõtvalt saabki järeldada, et Ameerika Ühendriikide lähenemine andmekaitse õigusele on võrreldes

[120] Hare, S. (2016) For your eyes only: U.S. technology companies, sovereign states, and the battle over data protection. *Business Horizons*, 59 (5), lk 549-561, lk 550.
[121] Diorio, S. Data Protection Laws: Quilts versus Blankets, *Syracuse Journal of International Law and Commerce*,Vol 42, Nr 2, lk 491.
[122] Burke, J.(1993) Kohtuniku roll Ameerika õigussüsteemis, Juridica,nr 3, lk 59-60, lk 59.
[123] Shaffer, G. (2000) Globalization and social protection: the impact of EU and International rules in the ratcheting up of U.S. data privacy standards, vol 25, *Yale Journal of International law*, lk 27.

Euroopas rakendatava andmekaitse õigusega vägagi erinev. Seda ennekõike tänu sellele, et USA-s puudub ühtne ja terviklik andmekaitse raamistik, mis aga Euroopas on olemas ning USA-s tegeletakse andmekaitse küsimustega valdkonniti.

USA's puuduvad võimalused näiteks oma andmeid kustutada, mis Euroopas tuleneb õigusest olla unustatust. Erinevused on tingitud juba ka sellest, et USA õigus kuulub teise õigussüsteemi, kui Euroopa õigus. Nimelt kuulub USA õigus Anglo-Ameerika õigussüsteemi ning Euroopa õigus kuulub Romaani-Germaani õigussüsteemi. Samuti on Euroopas isikuandmete kaitse ja privaatsusõigus väga olulised, USA õiguses väärtustatakse teisi väärtusi. Kui USA-s tekib küsimus, et kumb õigus jääb peale, siis peale jääb õigus sõnavabadusele. USA-s peetakse õigust sõnavabadusele väga oluliseks ja tähtsaks õiguseks, kuid leidub ka erandeid, kus privaatsusõigus on tõusnud kõrgemale kui sõnavabadus.

Mitmeid kokkuleppeid on sõlmitud, et muuta Euroopa Liidu ja USA vahelist andmevahetust õiguspäraseks. Läbirääkimised USA-ga algasid 90ndate teisel poolel ning selle tulemuseks ja ka nendest kõige tuntum on varasemalt kehtinud andmekaitsedirektiivi raames loodus 2000.a *Safe Harbour* kokkulepe. Selle eesmärgiks oli see, et USA tagaks andmete liikumise kahe kontinendi vahel. Seda siis Euroopa ja USA vahel.[124] See oli vajalik tänu sellele, et USA ettevõtted jagasid andmeid USA-le kuna seal säilitati neid. Tänu sellele oli see kokkulepe vajalik Euroopa Liidu kodanike isikuandmete kaitseks.

Safe Harbouri allakäik algas peale suurt skandaali. Üks suurimaid skandaale, mis USA välisluures on tekkinud on skandaal, mis on seotud Edward Snowdeniga. Edward Snowden on endine CIA töötaja, kes lekitas 2013.a suvel NSA ja CIA ülisalajase jälgimisprogrammi *PRISMI* ja *UpStream* kohta infot. *PRISM* oli jälgimisprogramm, mille kaudu USA valitsus teostas ameeriklaste ning ka teiste kodanike üle massjärelevalvet jälgides inimeste internetiliiklust ning ka isikuandmeid, saades andmete ligipääsu eraettevõtetelt. *UpStream* oli programm, mille raames luureteenistuse ametid kogusid internetiliikluse kohta infot otse allikast ehk ookeaneid läbivatest kaablitest.[125]

Mõlema programmi näol oli tegemist kahtlase tegevusega inimõiguste aspektist vaadatuna.

[124] Svantesson, D. J. B. (2016) Cross-Border Data Transfers after the CJEU's Safe Harbour Decision: A Tale of Gordian Knots. Alternative Law Journal, 41 (1), lk 39-42, lk 39.
[125] Free Snowden; Surveillance programs. Arvutivõrgus: https://edwardsnowden.com/surveillance-programs/ (15.03.2018)

Kogutuid isikuandmeid hoiti USA serverites *Safe Harbour* kokkuleppe alusel, aga isikuandmeid töötlevad ja säilitavad ettevõtted lähtusid USA õigusest. Tänu sellele, et loodud *Safe Harbour* kokkulepe oli loodud eraettevõtetele ning ei olnud USA luureteenistusele ega ka riiklikule julgeolekuagentuurile siduv, tekitas see mitmeid probleeme isikuandmete kaitse tagamises. 2015.a leidis Euroopa Liidu kohus, et *Safe Harbour* kokkulepe ei taga piisavat kaitset isikuandmete kaitsele ning tühistas selle kokkuleppe. 2017. a veebruariks loodi uus kokkulepe nimega *Privacy Shield. Safe Harbouri* kehtestuks tunnistamine tähendas seda, et selle programmi alusel esitatud isikuandmete töötlemine ja edastamine muutus koheselt ebaseaduslikuks.

Magistritöö autori arvates on Euroopa Liidu piires nende kodanike õigused korrektselt määratletud, mis puudutavad privaatsusõiguse või andmekaitse õiguse küsimusi. Õigust andmete kustutamisele ja õigust sõnavabadusele saab iga kodanik lihtsalt rakendada ning ta isikuandmed on ka kaitstud. Samuti on tagatud ka läbipaistvus andmete töötlemisel. Kuna internetis suheldes või osteldes puutuvad Euroopa Liidu kodanikud kokku mitmete USA suurettevõtetega nagu näiteks Google otsingumootor või teised otsingumootorid, siis tekib küsimus, kas kodanike isikuandmed on ikka kaitstud, kuna Ameerika Ühendriikide õigussüsteemis ei esine samasuguseid regulatsioone nagu seda on Euroopa Liidus. Samuti saaks antud küsimuse üle pikemalt arutada, kui räägiks lähemalt sõnavabadusest ja ettevõtlusvabadusest, kuid seda teemat ei käsitleta antud magistritöös.

2.6. Isikuandmete ülekantavas

Isikuandmete ülekantavuse vajadus on tekkinud praktikast, kuna hetkel ei ole isikutel võimalik enda isikuandmeid (fotosid, sõprade andmeid jms) eemaldada ühest keskkonnast ning tõsta neid ja taaskasutada neid teises sarnases keskkonnas. Antud probleem tekib just siis kui oleks vaja vahetada teenusepakkujaid. Teenusepakkuja vahetamine võib muutuda ebameeldivaks, kuna vahetuse käigus võivad isiklikud ja sotsiaalsed informatsioon kaotsi minna. Andmete liigutatavus puudutab ka enda identiteedi ja reputatsiooni kandmist ühest interneti keskkonnast teise. Reputatsioon on oluline internetis kaubeldes, kus eduka kauplemise võtmeks on teiste sama interneti lehekülje kasutajate poolt antud positiivsed hinnangud, mis muudavad müüja teiste ostjate silmis usaldusväärseks. Kui isik otsustab vahetada internetikeskkonda kus kaubelda, kaotab ka algses keskkonnas loodud tema identiteediga kaasnenud reputatsiooni ning peab uues keskkonnas alustama algusest.

Selleks, et omada suuremat kontrolli isikuandmete üle, loodi peale andmete kustutamise õiguse ka isikuandmete ülekantavuse põhimõte, mis võimaldab andmeid liigutada ühe vastutava töötleja juurest teise vastutava töötleja juurde. Antud põhimõte tuleneb üldmääruse artikli 15 (3)mis sätestab, et:

„[...] Vastutav töötleja esitab töödeldavate isikuandmete koopia. Kui andmesubjekt taotleb lisakoopiaid, võib vastutav töötleja küsida mõistlikku tasu halduskulude katmiseks. Kui andmesubjekt esitab taotluse elektrooniliselt, esitatakse ka teave üldkasutatavate elektrooniliste vahendite kaudu, kui andmesubjekt ei taotle teisiti. [...][126]

Samuti on siin oluline meeles pidada seda, et vastutav töötleja peab järgima seda, et mis liikmesriigi õigust tuleb töödeldavatele andmete kohaldada. Kui vastutab töötleja töötleb isikuandmeid ning suunab neid kindlasse liikmesriiki, tuleb direktiivi kohaselt kohaldada viidatud liikmesriigi õigust.[127] Kui vastutav töötleja tegeleb mitme liikmesriigi andmetega, siis ta peabki jälgima, et iga liikmesriigi puhul, mille andmeid tema kasutab, järgitakse selle liikmesriigi andmekaitseõigust.[128]

Magistritöö autor on seisukohal, et andmete liigutatavuse põhimõtte tutvustamine aitab andmesubjektidel omada paremat kontrolli enda isikuandmete üle. Samuti võrreldes isikuandmete kustutamise õigusega on andmete liigutatuvus praktikas lihtsam ning kiiremini rakendatav kui kustutamine. Kuna antud põhimõte tekitab lisakulutusi teenusepakkujatele on arusaadav, miks teenusepakkujad ei ole selle poolt, kuid üksikisikutele tagab see parema kontrolli iseenda andmete üle. Antud õigus vajab veel täpsustamist, et paremini aru saada reguleerimisalast, kuid see võimaldab andmesubjektil paremini liikuda ühe teenusepakkuja juurest teise juurde, kes pakub talle paremaid tingimusi. Tänu sellele ei pea üksikisikud isikud enam olema ainult ühe teenusepakkuja juures, kuna nende kõik andmed on nende juures, vaid saavad minna ka teiste teenusepakkujate juurde, kelle teenus võib olla näiteks turvalisem, kvaliteetsem ning hind soodsam.

[126] Üldmääruse artikkel 15 (3).
[127] Pormeister, K. (2018) Liidusisese kohalduva õiguse dilemma isikuandmete kaitse üldmääruses. Juridica, 2, lk 135.
[128] *Ibid.*

2.7. Euroopa Liidu siseturu tugevdamine

Isikuandmete kaitse reformi üheks eesmärgiks oli parandada ja tugevdada Euroopa Liidu siseturgu, et siseturg oleks efektiivsem. Samuti nähti vajadust eemaldada barjäär ettevõtetele ja avaliku sektori asutustele, mis oli tekkinud õiguskindluse puudumisest ning ka sellest, et isikuandmete kaitse seadused olid liikmesriigiti erinevad.[129] Antud reform on kõige vajalikum rahvusvahelistele ettevõtetele, kes asuvad mitmes Euroopa Liidu liikmesriigis ning kes vanasti pidid arvestama iga liikmesriigi enda seadusandlusega.[130] Varasemalt tekkisid direktiivist tuleneva õiguse tõlgendamisel, mis oma korda takistasid andmete vaba liikumist Euroopa Liidu siseturul. Samuti kuna puudus õiguskindlus, siis erinesid ka kulud, mis olid seotud andmete töötlemise ja edastamisega liikmesriikide vahel ning ei taganud ka piisavat kaitset isikuandmetele.

Kõige suurem ebavõrdsus tekkis suurte, keskmiste ja väikeste ettevõtete vahel, sest suurtel ettevõtetel on rohkem ressurssi, seda nii tööjõu kui finantsvahendite koha pealt ning tänu sellele said nad ka kergemini tagada, et nende tegevus vastaks õigusaktidele. Kuid väiksematel või keskmise suurusega ettevõtetel ei pruugi sellist võimalust olla, mis tekitas olukorra, kus väikesed või keskmise suurusega ettevõtted loobusid oma teenuste pakkumisest internetis või teenindasid kliente ainult enda liikmesriigi siseselt, kuna siis ei pidanud järgmine teiste liikmesriikide seadusandlust.

Töö autor on arvamusel, et selline olukord tekitas väga ebavõrdse seisu. Suuremad ettevõtted ainult suurenesid ja said aina edukamaks, kui väikesed ettevõtted pidid oma tegevust koondama. Samuti ei lähe see Euroopa Liidu siseturu põhimõtetega kokku, et kuidas kõigile ei ole tagatud võrdsed tingimused ettevõtlusega tegemiseks. Kõik need probleemid tekkisidki vanast direktiivist ning aina rohkem nähti, et on vaja reformida andmekaitse direktiivi. Probleemid tekkisid just praktikas ning oli selge, et riigiti saadi erinevalt direktiivist aru ning see tekitaski õiguskindluse puudumise ja õiguse killustamise. Samuti tekkis probleeme direktiivist tulenevate mõistetest aru saamisega.

[129] Commission staff working paper. Impact assessment lk 11.
[130] Euroopa Komisjoni teatis.Terviklik lähenemine isikuandmete kaitsele Euroopa Liidus, lk 3.

2.8. Ettevõtete kulude vähendamine

Selleks, et oleks võimalik saavutada suurem õiguskindlus, tuleks Euroopa Komisjoni hinnangul vähendada ettevõtete halduskoormusi. Kõige suuremad kulutused ettevõtetele on tingitud direktiivi artiklist 18, kus on sätestatud, et vastutav töötleja peab teavitama järelevalveasutust andmete töötlemisest. Komisjoni hinnangul on need kulutused rahvusvahelistel ettevõtetel 2,3 miljardit eurot aastas.[131] Ulatuslikud kulutused puudutavad eelkõige väikseid ja keskmise suurusega ettevõtteid, kellel võib see takistada ettevõtlusega tegelemist rahvusvahelisel turul.

Nagu varasemalt mainitud, siis suurimad kulutused kaasnevad Euroopa Komisjoni arvamusel direktiivis ette nähtud teavitamisekohustusega. Euroopa Komisjoni arvates peab iga vastutav töötleja teavituse eest kandma keskmiselt kulutusi 200 euro ringis.[132] Samuti on andmete säilitamine kulukas. Üldmääruses on sätestatud ka konsulteerimise andmekaitseasutusega kohustus (artikkel 36), andmekaitseametniku määramise kohustus (artikkel 37) ning seda kõike era- ja avaliku sektori asutustes, kus on tööl rohkem kui 250 töötajat, ehk tegemist on keskmise suuruse asutusega. Nende kohustusega kaasnevad kulutused, kuna need eeldavad täiendava tööjõu palkamist. Samuti kaasnevad kulutused artikliga 33, mis sätestab, et järelevalveasutust tuleb teavitada andmekaitse rikkumisest 24 tunni jooksul. Üldmääruses sätestatud meetmetega ei vähendata kulusid, vaid need pigem suurenevad. Autor on arvamusel, et üldmäärusega seotud kohustused on vajalikud, et püsiks õiguskindlus, ning et andmeid töödeldakse õiglaselt ning vajalikult, kuid selleks, et oleks ausam olukord võrreldes väiksemate ettevõtetega, tuleks proovida antud kulutusi vähendada, et ei tekiks olukorda, mis on suurtele ettevõtetele soodne aga väiksemad ettevõtted on olukorras, kus peaksid oma teenustest loobuma.

2.9. Mikro-, väikese ja keskmise suurusega ettevõtetele erandite kohaldamine

Mikro-, väikese ja keskmise suurusega ettevõtted on oma suuruselt erinevad. Mikrosuurusega ettevõtteks on ettevõte, kus on alla 10 töötaja. Väikese suurusega ettevõte on suurem mikroettevõtteks ning see on ettevõte, kus on alla 50 töötaja ning keskmise suurusega ettevõte on kõige suurem ettevõte, kus on alla 250 töötaja. Euroopa Komisjon soovitab mikro-, väikese ja

[131] V. Reading, lk 3.
[132] Commission staff working paper. Impact assessment, lk 13.

keskmise suurusega ettevõte puhul oma kulusid ning ka konkurentsivõimet suurendada läbi erandite ning tänu sellele oleks sellistele ettevõttele teist laadi reeglid, kui suurema töötaja arvudega ettevõtetele.[133]

Antud eranditeks oleks seoses väljaspool liitu asuvate riikide vastutavate töötlejate kohustus määrata endale esindaja liidus (artikkel 27), andmekaitse ametniku määramise kohustus (artikkel 37) ning seoses halduskaristustega. Erandid kehtivad mikro-, väikese ja keskmise suurusega ettevõtetele ehk ettevõttele, kus on alla 250 töötaja.

Üldmäärusega kaasnevad halduskoormuse suurenemine tähendab väikese ning keskmise suurusega ettevõtetele vaatama neile rakenduva erandite süsteemile 300-7200 eurot lisakulutusi aastas, mis moodustavad 16-40% nende infotehnoloogia eelarvest.[134] Sellised erandid on kehtestatud selleks, et tagada andmesubjektide õiguste parem kaitse. Kuid üldmäärus näeb ette erandi, et ettevõttes, kus on alla 250 töötaja, ei ole kohustatud määrama andmekaitse ametniku tööle, kes kontrolliks volitatud töötajate andmete töötlemise õiguspärasust ning seaduslikkust. Kuid selle erandi rakendamise tõttu on isikute õigused vähem kaitstud ning seda tänu eranditele, mida on võimalik rakendada mikro-, väikse ja keskmise suurusega ettevõtetele ning selle erandiga ei tugevdata isikute õigusi andmete töötlemisel.

Magistritöö autor on arvamusel, et parem tasakaal tekiks siis, kus erandeid rakendatakse mitte ettevõtte suuruse järgi, vaid töödeldavate andmete mahu järgi. Tänu sellele ei tekiks üksikisikute õiguste vähendamist ning ka mitte ebavõrdseid olukordi, mis on tingitud ettevõtte erinevatest suurusest. Samuti tähendab see ka seda, et mingi hetk kaotavad väiksemad ettevõtted oma töö, kuna suurtel ettevõtetel on rohkem ressurssi, et töödelda isikute andmeid suuremas mahus ning suudavad tasuda mitmeid kohaldavaid lisakulutusi. Samuti on autor arvamusel, et halduskoormuse vähendamine ei ole hetkel üldmäärusega saavutatav, kuna direktiivis ei ole leitud head tasakaalu andmesubjekti õiguste kaitse vahel kui ettevõtjate õiguste kaitse vahel. Mitmes olukorras võib

[133] *Ibid*, lk 80.
[134] Christensen, L. The Impact of the Data Protection Regulation in the E.U. 2013, p 2. Arvutivõrgus: http://www.intertic.org/Policy%20Papers/CCER.pdf, 15.03.2018.

KOKKUVÕTE

Isikuandmete kaitse üldmääruse preambulas on sätestaud, et miks oli vaja luua uus määrus.

"Kiire tehnoloogiline areng ja üleilmastumine on tekitanud isikuandmete kaitsel uusi väljakutseid. Isikuandmete kogumise ja jagamise ulatus on märkimisväärselt suurenenud. Tehnoloogia võimaldab nii era- kui ka avaliku sektori asutustel kasutada isikuandmeid oma tegevuses enneolematus ulatuses. Füüsilise isikud avaldavad isikuandmeid üha avalikumalt ja ülemaailmsemalt. Tehnoloogia on põhjalikult muutnud nii majandust kui ka ühiskondlikku elu ja peaks täiendavalt hõlbustama liidusisest andmete vaba liikumist ning nende kolmandatesse riikidesse ja rahvusvahelistele organisatsioonidele edastamist, tagades samal ajal isikuandmete kõrgetasemelise kaitse.[135]" Kõik need punktid ongi mingil määral mõjutanud seda, et miks andmekaitse reform oli hädavajalik.

Isikuandmete kaitsele hakati rõhku panema peale Teist Maailmasõda, kui tehnoloogia *boomi* jooksul hakkasid valitsused ja ettevõtted hulgaliselt isikute andmeid koguma ning töötlema. Samuti veelgi tõhusamatele ja spetsiifilistele isikuandmete kaitse meetmetele tekkis infoühiskonna kiirest arengust ning interneti kättesaadavuse kiirest levikust. Infoühiskonnas tekkis vajadus tagada isikutele eraelu puutumatus ja privaatsusõiguse kaitse. Tänapäeva ühiskonnas on igal inimesel kiire ja kerge ligipääs elektroonilistele infoallikatele. Tänu sellele on isikuandmete kaitse rikkumisi rohkem. Interneti kiirest levikust tingituna on infoühiskonnas toimunud pöördelised muudatused. Sellest tulenevalt kasutavad isikud just erinevaid elektroonilisi seadmeid selleks, et saada informatsioonile ligipääs. Interneti kiirele levikule aitasid kaasa ka erinevad otsingumootorid, mis muutsid teabe kättesaamise veelgi hõlpsamaks. Tänu sellele tekkis olukord, kus oli vaja reguleerida informatsiooni käsitlemine, et oleks tagatud iga inimese isikuandmete kaitse ja õigus eraelu puutumatusele, mis on üheks põhiõiguseks. 90ndatel loodud andmekaitse regulatsioon ei taganud enam piisavat kaitset isiku privaatsus- ja andmekaitse õigusele ning loodi uus andmekaitse määrus, millega luuakse uued sätted ja

[135] Isikuandme kaitse üldmääruse preambula.

meetmed, mis on tänapäeval rohkem ajakohased ning aitavad käsitleda paremini isikute andmete töötlemisega seotuid probleeme.

Andmekaitsereformi raames võeti kasutusele uus isikuandmete kaitse üldmäärus, mis muutus kohalduvaks kõigile euroopa liidu liikmesriikidele 2018 aasta maist. Sellega kaasned mitmed muudatused ning lisad, mis eelnevas regulatsioonis puudusid või olid väga puudulikud. Kõige olulisemaks muudatuseks võib pidada andmekaitse üldmääruse artikkel 17, mis sätestab õiguse andmete kustutamisele internetis ehk termini "õigus olla unustatud". Antud artikkel sätestab, et

"Andmesubjektil on õigus nõuda, et vastutav töötleja kustutaks põhjendamatu viivituseta teda puudutavad isikuandmed ja vastutav töötleja on kohustatud kustutama isikuandmed põhjendamatu viivituseta, kui kehtib üks järgmistest asjaoludest."[136]

Antud artikkel tähendab seda, et andmesubjektil on õigus nõuda andmetöötlejalt või teenusepakkujalt teda puudutavate andmete kustutamist, kuid selleks, et see oleks võimalik, peavad need vastama artikkel 17 punktides a-f olevatele nõuetele. Käesolev säte koostati tänu *Google'i vs Spain* kohtulahendi C-131/12 otsusest[137]. *Google vs Spaini* kohtulahend oli seotud sellega, et Hispaania kodanik soovis, et Google kustutaks ära viite tema andmete, mis tulevad esile siis, kui keegi kasutab Google otsingumootorit, et tema kohta infot otsida. Andmed olid vananenud kuid kuna andmeteks olid võlgnevused, mis avaldati ühes Hispaania ajalehes, siis andmed olid ikka halvustavad. Tänu sellele soovis antud isik, et Google kustutaks andmed. Kohus nõustus kodanikuga, et andmed tuleks kustutada. Oluline on märkida ka seda, et isikuandmete kaitse on tihedalt seotud inimõigustega. Esmakordselt mainiti isikuandmete kaitset avaliku võimu eest ning, et informatsiooni ei tohi koguda, avaldada ja isikul on õigus nõuda ligipääsu tema kohta kogutavale andmetele aastal 1984. kui kohtunik Pettiti jäi eriarvamusele otsuses *Malone vs The United Kingdom.*[138]

Kõige suurem mõju oli Google'i kohtulahendil, kus selgitati välja isikuandmete kaitse olulised põhimõtted. Kohus leidis antud kaasuses, et Google on kohustatud kustutama oma viited ajalehe veebiformaadis olevatele andmete, mis ei olnud enam selleks ajaks asjakohased ning olid lahendatud juba. Kuid kui inimesed kasutasid Google otsingumootorit ning otsisid antud isiku nime, siis läbi Google said nad minna ajalehe kodulehele, kust said nad ligipääsu vanadele

[136] Andmekaitse üldmääruse artikkel 17.
[137] EIKo 13.05.2014, c-131/12, *Google vs Spain*.
[138] EIKo 02.08.1984, 8691/79, *Malone v The United Kingdom, kohtunik Pettiti eriarvamus*

andmetele. Samuti jõudis kohus järeldusele, et otsingumootorit saab pidada vastutavaks töötlejaks, kuna teenusepakkuja saab määrata isikuandmete töötlemiseks vajalikud vahendid. Antud kaasusest tuli ka kohustus kaitsta andmesubjekti isikuandmeid. Samuti on tänapäeval isikuandmete kaitse väga relevantne tänu Facebookile. Paljud isikud ei ole teadlikud sellest, et kuidas internetis või teistes sotsiaalmeedia keskkondades nende isikuandmeid töödeldakse.

Käesolevas magistritöö esimeses peatükis käsitles autor isikuandmete kaitse õiguse tekkimist, tutvustades olulisi õigusallikaid ning seletades miks oli andmekaitsereform vajalik. Samuti tutvustas autor olulisi mõisteid ja põhimõtteid andmekaitse valdkonnas. Esimese peatüki põhjal saab väita, et andmekaitsereform oli vajalik, kuna eelneva direktiiviga kaasnesid probleemid ning õigus oli killustunud liikmesriikide vahel, kuna liikmesriikidel anti võimalus andmekaitse õigus sulanduda nende siseriikliku õigusega. Samuti, et isikuandmete kaitse on tihedalt seotud eraelu puutumatusega, privaatsusõigusega, inimõigustega ja informatsioonilise enesemääramise õigusega.

Teises peatükis käsitles magistritöö autor andmekaitse üldmääruse põhilisi punkte ja olulisi muudatusi. Samuti ka asjakohast kohtupraktikat. Autor analüüsis teises peatükis muudatusi ning miks need tagavad tõhusama õiguskaitse andmekaitse valdkonnas. Olulistemaks uuendusteks peab autor "õigus olla unustatud", läbipaistvusprintsiip, teavituskohustus ja keeleline selge struktuur.

Antud magistritöö esimeseks uurimisküsimuseks oli, et kas Euroopa Liidu tasandil oli vaja kehtestada uus õigusakt, mis tagaks isikuandmete kaitset paremini. Kuna aja jooksul on internet muutunud ning teabe kättesaadavus on muutunud kergemaks, tekkis juurde viise kuidas isikute andmed ei olnud enam seadusandluse tasemel kaitstud. Samuti nähti, et praktikas on tekkinud erinevaid probleeme ning eelnev direktiiv ei taganud piisavalt tõhusa kaitse ning õigus on liikmesriigiti siseselt killustunud. Tänu sellele oli vaja luua Euroopa Liidu tasandil uus õigusakt ning andmekaitsereform, mis tagaks vajaliku kaitse isikuandmete kaitsele.

Teiseks uurimisküsimuse teemaks oli, et kuidas tagavad andmekaitsemääruses kasutatavad uuendused tõhusama õiguskaitse, mis on kooskõlas inimeste põhiõiguste ja vabadustega. Kõige olulisemaks uuenduseks saab pidada õigust olla unustatud õiguse kaasamist üldmäärusesse. Tänu sellele on isikutel rohkem kontrolli iseenda andmete üle. Sellega kaasneb valikuvõimalus, et kas isikud soovivad kustutada otsingumootorite tulemuste seast enda isikuandmeid või mitte. Samuti kaasneb sellega ka suurem informatsioonilise enesemääramise õigus. Samuti oli üheks oluliseks

uuenduseks ka teavitamiskohustus. See tähendab seda, et andmetöötleja on kohustatud teavitama andmesubjekti tema andmete töötlemisest. Tänu sellele on isikud teadlikud, kui keegi töötleb nende andmeid, nad on teadlikud, et mis firmad töötlevad nende andmeid ja mis eesmärgil ning nad on ka teadlikud sellest, et neil on õigus isikuandmete kaitsele. Teiseks oluliseks uuenduseks on see, et sooviti suurendada läbipaistvusprintsiibi kasutamist. Läbipaistvusprintsiip tähendab seda, et isikud on teadlikud sellest, et kui nende andmeid töödeldakse ning nad teavad, et mis andmetöötleja nende andmete töötlemist läbi viib. Selle muudatusega sooviti vähendada seda, et avalik sektor ei töötleks isikute andmeid liialt. Isikuandmete kaitse üldmääruses sätestati ka see, isikutel on võimalik vajadusel oma andmeid ülekanda. Andmete ülekandmine aitab suurendada isikul kontrolli enda andmete üle ning aitab kergemini vahetada teenusepakkujaid ja valida teenusepakkujaid tulenevalt teenuse kvaliteedist, mitte sellest, et milline teenusepakkuja omab rohkem isiku andmeid. Uue muudatusena saab välja tuua ka selle, et on nii põhjalikult seadusandluses sätestatud, et mis on andmetöötleja kohustused ja tööülesanded. Tänu sellele on tavainimesel ülevaade, et mida tehakse tema andmetega ning mis on üldse andmete töötlemine. Kindlasti on oluline muudatus ka see, et isikutele saadetav teave tema andmete töötlemisest peab olema selges keeles kirjutatud ning, et see oleks ka arusaadav lastele. Oluline on see tänu sellele, et nii suur osa internikasutajatest on just lapsed. Eestis võivad alates 14 aasta vanused anda enda nõusoleku isikuandmete töötlemiseks ning nooremad kui 14 aastaste eest peavad nõusoleku andma nende seaduslikud esindajad. See tagab piirangud ka erinevatele suurfirmadest teenuseosutajatele nagu Facebook, YouTube, Gmail, Spotify, kuna nad peavad tarvitusele võtma meetmeid, millega nad kontrollivad, et Eestis oleks noorema kui 14 aastase lapse puhul isikuandmete töötlemiseks antud mitte lapse poolt vaid tema seadusliku esindaja poolt. Autori arvates tagavad uuendused tõhusama õiguskaitse ning andmekaitsereform oli igati vajalik.

Kolmandaks uurimisküsimuseks oli, et mis on andmekaitse üldmääruse eeldatav mõju. Magistritöö autor on arvamusel, et "õigus olla unustatud" mõjub andmesubjektidele positiivselt ning tagab neile tõhusama isikuandmete kaitse ning privaatsuse. Tänu antud õigusele on isikutel võimalik kontrollida enda isikuandmeid ning enda kohta leiduvat informatsiooni otsingumootorite tulemuste seas. "Õigus olla unustatud" aitab kaasa ka Google poolt loodud vorm, mille kaudu saab isik nõuda teenusepakkujal enda isikuandmete kustutamist otsingumootorite tulemuste seast. Kuid tuleb tõdeda, et eestlased on kasutanud seda võimalust vähe. Kokkuvõtvalt saab öelda, et antud üldmäärus tagab tõhusama kaitse isikute andmetele, tutvustab isikutele nende õigusi, tagab andmetöötlejate tööülesanded ning aitab praktikas tulenevaid probleeme ennetada.

Andmekaitse üldmäärus on veel nii uus, siis tänu sellele on raske anda hinnangut, et kas uue üldmäärusega kaasnevad praktikas probleemid. Kuid privaatsusõigus on tänapäeval väga oluline ning antud teema on ka väga laialdane, kuid antud töö maht on piiratud, ei olnud võimalik selle töö raames antud teema kõiki probleeme süviti analüüsida ning uurida. Käesoleva töö eesmärgiks ei ole anda hinnangut andmekaitse üldmäärusele vaid analüüsida sellega kaasnevaid uuendusi ning jõuda järeldusele, et kas sellega on tagatud õiguskindlus või mitte. Samuti on töö autor arvamusel, et magistritöö käigus leidis töö hüpotees kinnitust ning "õigus olla unustatud" on tagatud tõhusam kaitse isikute andmetele.

Antud töö käigus uuritud andmekaitse aspektid on väga huvitavad, päevakohased ning väga suure informatsiooni mahuga. Neid valdkondi on võimalik süvitsi edasi uurida. Näiteks analüüsida, et kui suures mahus on eestlased teadlikud enda isikuandmete kaitsest ja privaatsusõigusest või kuidas peavad erinevad erasektori firmad kinni andmete töötlemisest ning kas igas piisavalt suures firmas on palgaline andmetöötleja. Samuti saab uurida ka seda, et kuidas kohaldatakse järelevalvet andmete töötlemisele ning kas rikkumiste korral kohaldatakse trahve. Kindlasti saaks uurida ka seda, et kuidas teised teenusepakkujad töötlevad isikute andmeid. Antud teema kohta saab koostada ka uurimust sellel teemal, et kuidas Ameerika Ühendriikide andmekaitse praktika erineb Euroopa Liidu liikmesriikide omast. Andmekaitse teemal on võimalik koostada ka väga tehnilist uurimistööd, kus seletatakse täpsemalt andmetöötlusest pilves või big data ehk suurandmete kogumisest. Samuti on autor arvamusel, et andmekaitseinspektsioon peaks eestlasi rohkem teavitama sellest, et kuidas internetis nende andmeid kogutakse ning mida kujutab endast andmete töötlemine.

SUMMARY

HARMONIZATION OF THE PERSONAL DATA PROTECTION GENERAL REGULATION WITH PERSONAL FUNDAMENTAL RIGHTS

Elizabeth Laan

The need for an effective protection for the personal data came important as a rapid development of the information society. In the information society, there was a need to ensure the protection of individual's privacy. In today's society, everyone has quick and easy access to electronic sources of information. As a result, there are more violation and criminal activity around personal data. Due to the fast development of the Internet, fundamental changes have taken place in the information society. Because of that, individuals use a variety of electronic devices in order to gain access to information. Various search engines, such as Google, have made it easier to gain access to personal data. This created a situation where it was necessary to regulate the handling of information in order to ensure the protection of personal data for every person. The data protection regulation created in the 90s no longer provided adequate protection for the privacy and data protection rights of a person. Therefore a new data protection regulation was created, which creates new provisions and measures that are more up to date and help to better address personal data issues.

A new regulation on personal data protection was introduced in the framework of data protection reform, which became applicable to all Member States of the European Union from May 2018. There are a number of additions and changes that were not included in the previous regulation. The most important change is the Article 17 of the General Data Protection Act (GDPR), which provides the right to delete data on the Internet - "right to be forgotten". This article means that the data subject has the right to require the data processor or service provider to delete the data relating to the person. In order to do so, they must meet the requirements of Article 17 (a) to (f). This provision was made thanks to the court judgment (C-131/12) against Google. It is also important to note that the protection of personal data is closely linked to human rights. The first

time when protection of personal data from public authority was mentioned was in 1984 when Judge Pettiti disagreed in *Malone vs The United Kingdom.*[139]

The biggest impact was the Google court judgment, which clarified the essential principles of personal data protection. The court found that Google was obliged to delete its references to the data contained in the newspaper's webform, which were no longer relevant at that time and were already resolved. But when people used the Google search engine and searched for the name of a given person, they could go to the newspaper homepage, where they got access to old data. The court also concluded that the search engine could be considered a data controller because the service provider can determine the resources necessary for processing personal data. The case also involved the obligation to protect the data subject's personal data. And today, personal data protection is also very important thanks to Facebook. Many individuals are not aware of how their personal information is being processed on the Internet or in other social media platforms.

In the first chapter of this Master's thesis, the author discussed the creation of data protection law by introducing important legal sources and explaining why data protection reform was necessary. The author also introduced important concepts and principles in the field of data protection. Based on the first chapter, it can be argued that data protection reform was necessary because the previous directive included flaws and the law was fragmented between EU Member States, since they were given the opportunity to integrate data protection rights into their national law. Also, the protection of personal data is closely linked to privacy in general as well as human rights and the right to information self-determination.

In the second chapter, the author of this thesis discussed the main points and changes of the general data protection regulation as well as the relevant case law. The author analysed the changes in the second chapter and how and why they ensure more effective law enforcement in the area of data protection. According to author, the most important innovation is the"right to be forgotten", the principle of transparency, an obligation to provide information in clear linguistic structure.

The first research question in this Master's thesis was that whether or not it was necessary to introduce the new legislation at European Union level so that it would ensure better personal data protection. As the Internet has changed over time and the availability of information has become easier, there has been more evidence on how the personal data was no longer protected

[139] EIKo 02.08.1984, 8691/79, *Malone v The United Kingdom, kohtunik Pettiti eriarvamus.*

at the legislative level. It was also seen that there were various problems in practice, and the previous directive did not provide sufficiently effective protection. The law was also fragmented within the EU Member States. This required the creation of new legislation at EU level and data protection.

The second issue of the research topic was how the reformations used in the data protection provide more effective law enforcement in line with human right. The most important reformation is the „right to be forgotten“ to be included in the general regulation. As a result, individuals have more control over their own data. This will involve choosing whether or not individuals want to delete their own personal data from search engine results. It also gives greater right to self-determination. One of the important reformations was also the notification obligation. This means that the data processor is required to inform the data subject to processing. As a result, individuals can be more aware when someone processes their data. They can get information of which companies process their data and for what purpose. They are also informed that they have the right to protection of their personal data. Another important reformation is the desire to increase the use of the transparency principle. The principle of transparency means that individuals are informed when their data is being processed. This amendment was intended to reduce the fact that the public sector would not process the data of individuals too much. The general regulation on the protection of personal data also provides the possibility for individuals to transfer their data if necessary. Data transfer will help increase the person's control over his or her data, and will help more easily switch service providers and choose them based on service quality, rather than which provider would collect personal information. A new amendment is very detailed on what are the data processor duties and tasks. As a result, the average person has an overview of what is done with his or hers data and what is the data processing all about. Another important change is that the information sent to persons about processing their data must be written in clear language so that it can also be understood by the children. This is due to the fact that so many Internet users are children. In the author's view, the innovations provide more effective law enforcement and data protection reform is needed.

The third research question was that either the "right to be forgotten" guarantees more effective law enforcement in the area of personal data protection. The author of the thesis thinks that "the right to be forgotten" affects the data subjects positively and provides them with more effective protection of personal data and privacy. Thanks to this right, individuals are able to verify their personal information and the information they find about themselves in search engine results.

The "right to be forgotten" is also facilitated by a form created by Google that allows a person to require the service provider to delete his or her personal information from the results of search engines. However, it must be admitted that Estonians have used this opportunity only a few times.

The GDPR is still so new, therefore it is difficult to judge that whether or not the new regulation has problems in practice. However, privacy law is very important today, but the topic is also very broad. The scope of this work was limited as it requires more deeper analyses and investigation on all the issues covered in this thesis. The purpose of this thesis is not to evaluate the general data protection regulation but to analyse the new reformations and to conclude whether it's needed or not. The author of the paper is also on the opinion that during the work, hypothesis was confirmed and the "right to be forgotten" guarantees more effective protection of personal data.

The data protection aspects studied in this thesis are very interesting and have a very large amount of information. These areas can be further explored. For example, to analyse how much the Estonians are aware of their personal data protection and privacy rights, or how different private sector companies deal with the processing of data, and whether the data processor is active in large companies. You can also look at how monitoring data processing is applied and whether fines are imposed in case of infringements. Certainly, one can also look at how other service providers process personal data. A study on this topic can also be drawn up on the topic of how the US data protection practice differs from the European Union Members. On the subject of data protection, it is also possible to draw up very technical research, which explains more precisely the processing of data in the cloud or the *big data* collection. The author's opinion is that Estonians should be more informed about how their data are being collected on the Internet and what is the processing of data in detail.

KASUTATUD KIRJANDUS

Raamatud

1. Bosco, F, Creemers, N. (2015) Profiling Technologies and Fundamental Rights and Values: Regulatory Challenges and Perspectives from European Data Protection Authorities. – Reforming European Data Protection Law. Dordrecht: Springer, lk 4.
2. Carey, P. (2004) Data protection: a practical guide to UK and EU law. Oxford: Oxford University Press, lk 3.
3. Lõhmus, U. (2012). PõhiS § 26/9.4. – E. J Truuväli jt (toim) Eesti Vabariigi põhiseadus. Komm vlj. 2. vlj. Tallinn: Juura.
4. Männiko, M. (2011). Õigus privaatsusele ja andmekaitse. Tallinn, Juura, lk 41.
5. Maruste, R. (2004) Konstitutsionalism ning põhiõiguste ja -vabaduste kaitse. Tallinn: Juura, lk 429
6. Tikk, E, Nõmper, A. (2007). Informatisoon ja õigus. Tallinn: Juura, lk 14.

Artiklid

1. Albers, M. (2005) Isikuandmete kaitse põhiõiguslik alus: kas õigus informatsioonilisele enesemääramisele ja/või eraelu austamisele? Juridica 8, lk 537–543, lk 537.

2. Alexy, R. (2001) Põhiõigused Eesti Põhiseaduses. - Juridica , eriväljaanne, p 6.1.2.2.
3. Ambrose, M. L. (2013) It's About Time: Privacy, Information Life Cycles, and the Right to Be Forgotten. *Stanford Technology Law Review*, 16 (2), lk 369-422, lk 394.
4. Brandeis, L. Warren, S. *The Right to Privacy, Harvard University Press,* lk 4.
5. Burke, J.(1993) Kohtuniku roll Ameerika õigussüsteemis; *Juridica*, nr 3, lk 59 -60, lk 59.

6. Byrum, K. (2017). The European right to be forgotten: A challenge to the United States Constitution's First Amendment and to professional public relations ethics. *Public Relations Review, 43*(1), 102-111.
7. Carbone, C. E. (2015) To Be or Not to Be Forgotten: Balancing the Right to Know with the Right to Privacy in the Digital Age. Virginia Journal of Social Policy & the Law, 22 (3), lk 525-560, lk 553.
8. Cate, F. H. (1998) The European Data Protection Directive and European-U.S. Trade. Currents: *International Trade Law Journal*, 7 (1), lk 61-80, lk 66.
9. Christensen, L. (2013) The Impact of the Data Protection Regulation in the E.U lk 2.
10. Cooley, R., Mobasher, B. & Srivastava, J. (1999) Data Preparation for Mining World Wide Web Browsing Patterns. – *Knowledge and Information Systems,* Vol. 1, 5-32.
11. Cukier, K. (2013) The Rise of Big Data. How It's Changing the Way We Think About the World. – Foreign Affairs 2013, nr 92, lk 28-29.
12. DeSimone, C. (2011). Pitting Karlsruhe Against Luxembourg? German Data Protection and the Contested Implementation of the EU Data Retention Directive. - *German Law Journal* 2010/11, No. 3, lk 293.
13. Diorio, S. Data Protection Laws: Quilts versus Blankets, *Syracuse Journal of International Law and Commerce*,Vol 42, Nr 2, lk 491.
14. Fazlioglu, M. (2013) Forget me not: the clash of the right to be forgotten and freedom of expression on the Internet, *International Data Privacy Law,* vol. 3, no. 3, lk 157.
15. Ginter, G. Schasmin, P. (2017) Lahendite *Tele2 Sverige* ja *Digital Rights Ireland* mõju sideandmete mugavkasutusele Eestis. *Juridica*, 1, lk 43.
16. Glon, C. (2014) Data Protection in the Europeal Union: A closer look at the current patckwork of data protection laws and the proposed reform that could replace them all. *International Journal of Legal Information*, 42 (3), lk 471- 492.
17. Gunasekara, G. (2014). Paddling in unison or just paddling? International trends in reforming information privacy law. *International Journal of Law and Information Technology, 22*(2), 141-177, lk 143.
18. Gutwirth, S, Leenes, R, & Poullet, Y (eds) (2011), Computers, Privacy and Data Protection:An Element of Choice, Springer, Dordrecht, lk 1-457, lk 39.
19. Hansen, T. (2014) Euroopa Inimõiguste Kohtu praktika kohtuotsustes isikuandmete avaldamisel, J*uridica*, 4, lk 313-324, lk 313.

20. Hare, S. (2016) For your eyes only: U.S. technology companies, sovereign states, and the battle over data protection. *Business Horizons*, 59 (5), lk 549-561, lk 550.
21. Heisenberg, D. (2005). Negotiating privacy : The European Union, the United States, and personal data protection, Ipolitics: Global Challenges in the Information Age lk 1-179, lk 139.
22. Ilus, T. (2002) Isikuandmete kaitse olemus ja arengusuunad. *Juridica*, 7, lk 435-446.
23. Ilus, T. (2005). Andmesubjekti osaluse põhimõte Euroopa Nõukogu konventsioonide ning Euroopa Inimõiguste Kohtu lahendite valguses. – *Juridica,* 8, lk 519.
24. Klosek, J. (2000) Data Privacy in the Information Age. Greenwood Publishing Group, United States of America, lk 8.
25. L. A. Bygrave. (1998). Data Protection Pursuant to the Right to Privacy in Human Right Treaties.- *International Journal of Law and Information Technology*, nr 6 (3), lk 255-259.
26. Liiv, E. (2014) Kas eraisikul on õigus unustusele Internetis? *Juridica*, 9, lk 643-651, lk 647.
27. M. J. Kelly, Satolam, D. (2017). The right to be forgotten. *University of Illinois Law Review* 2017(1), 1-64.
28. McGoldrick, D. (2013). Developments in the Right to be Forgotten. *Human Rights Law Review, 13*(4), 761-776.
29. Michael, K. (2013) Big Data: New Opportunities and New Challenges. – IEEE Security & Privacy. *IEEE Computer Society*, lk 22-24.
30. Peltz-Steele, R. J. (2013) The New American Privacy. *Georgetown Journal of International Law*, 44 (2), lk 365- 410, lk 379.
31. Portmeister, K. (2018) Liidusisese kohaldava õiguse dilemma isikuandmete kaitse üldmääruses. *Juridica, 2, lk 125-135.*
32. Reno, J. (2012) Big Data, Little Privacy. – CA Technology Exchange. *Insights from CA Technologies*, nr 3 (2), lk 28-32.
33. Shaffer, G. (2000) Globalization and social protection: the impact of EU and International rules in the ratcheting up of U.S. data privacy standards, vol 25, *Yale Journal of International law*, lk 27.
34. Shahin, S. (2016). Right to Be Forgotten. *Journalism & Mass Communication Quarterly, 93*(2), 360-382.
35. Solove, D (2009), Understanding Privacy, *Harvard University press*, Cambridge, lk 15-16.

36. Svantesson, D. J. B. (2016) Cross-Border Data Transfers after the CJEU's Safe Harbour Decision: A Tale of Gordian Knots. *Alternative Law Journal*, 41 (1), lk 39-42, lk 39.
37. Tirosh, N. (2017) Reconsidering the 'Right to be Forgotten' – memory rights and the right to memory in the new media era. *Media, Culture & Society*, Vol.39(5), lk 644-660.
38. Tzanou, M. (2013) Data Protection as a Fundamental Right Next to Privacy? "Reconstructing" a not so new right. *International Data Privacy Law*, vol. 3, lk 90.
39. Tzanou, M. (2013). Is Data Protection the Same as Privacy? An Analysis of Telecommunications' Metadata Retention Measures, *Journal of Internet Law,* Vol 17, nr 3, lk 23
40. Walker, R. (2012). The right to be forgotten. *Hastings Law Journal* 64(1), lk 257.
41. Waschke, M. (2012) Introduction to the Big Data. - CA Technology Exchange. *Insights from CA Technologies*. nr 3, lk 1.

Elektroonilised allikad

1. Free Snowden; Surveillance programs. Arvutivõrgus: https://edwardsnowden.com/surveillance-programs/ (15.03.2018)
2. Hustinix, P (2013). EU Data Protection Law - Current State and Future Perspectives, Kättesaadav arvutivõrgus: http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/Hustingx.pdf (15.02.2018)
3. Martin, A. What does Facebook do with my data and how do i stop it? Kättesaadav arvutivõrgus:https://news.sky.com/story/what-does-facebook-do-with-my-data-and-how-do-i-stop-it-11299792 (11.05.2018)
4. Parm, U. (2014) Pilveandmetöötlus: kättesaadav http://www.aki.ee/et/pilvandmetootlus (6.03.2018)
5. Rohtmets, E. (2013) Eesti andmekaitse Euroopa Kohtu praktika peeglis. - Riigikogu toimetised 28. Arvutivõrgus: http://www.riigikogu.ee/rito/index.php?id=14437, (28.02.2018).

Eesti õigusaktid

1. Avaliku teabe seadus.- RT I, 04.07.2017, 11.
2. Eesti Vabariigi põhiseadus. - RT I, 15.05.2015, 2.

3. Elektroonilise side seadus. – RT I, 01.07.2017, 2.
4. Isikuandmete kaitse seadus. - RT I, 30.12.2010, 11.
5. Isikuandmete kaitse seaduse seletuskiri. Arvutivõrgus: http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/IKS%20SELETUSKIRI%20(1).rtf., (28.02.2018).

Rahvusvahelised õigusaktid

1. Council of Europe. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. ETS No.108, Strasbourg 28/01/1981 (Convention 108).
2. Euroopa Liidu põhiõiguste harta. - ELT C 83, 30.03.2010.
3. Euroopa Parlamendi ja nõukogu direktiiv 95/46/EÜ, 24.10.1995, üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta. EÜT L 281, 23.11.1995.
4. Euroopa Parlamendi ja nõukogu määrus (EL) 2016/679, füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta. ELT L 119, 04.05.2016.
5. Isikuandmete automatiseeritud töötlemisel isiku kaitse konventsioon. – RT II 2001, 1, 3.
6. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 23. 09. 1980.

Eesti kohtulahendid

1. RKHKo 3-3-1-3-12 p 19, 12.06.2012.

Muud kohtulahendid

2. EIKo 02.08.1984, 8691/79, *Malone v The United Kingdom, kohtunik Pettiti eriarvamus.*
3. EIKo 26.03.1987, 9248/81, *Leander v Sweden.*
4. EIKo 07.07.1989, 10454/83, *Gaskin vs The United Kingdom*.
5. EIKo 22.02.1994, 16213/90, *Burghartz vs. Šveits*
6. EIKo 24.09.2004, 59320/00, *von Hannover vs. Saksamaa.*
7. EIKo 13.02.2003, 42326/98, *Odiere vs. Prantsusmaa.*
8. EIKo 13.05.2014, c-131/12, *Google vs Spain*.

9. EIKo 08.04.2014, C-293/12 ja C-594/12, *Digital Rights Ireland v Minister for Communications, Marine and Natural Resources, Seitlinger and Others.*

Muud allikad

1. Artikkel 29 alusel asutatud andmekaitse töörühm. Advice Paper on Special Categories of Data (sensitive data), 2000. https://ec.europa.eu/info/law/law-topic/data-protection_en (19.02.2018)
2. Commision Staff Working Paper Impact Assessment /SEC/2012/0072 final, 25.01.2012.
3. Euroopa Komisjoni eelnõu seletuskiri „Euroopa Parlamendi ja nõukogu määrus üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta.“ KOM(2012) 11. Brüssel: 25.01.2012, lk 3. Arvutivõrgus:http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_et.pdf, (26.02.2018)
4. Euroopa Komisjoni teatis Euroopa Parlamendile, nõukogule, majandus- ja sotsiaalkomiteele ning regioonide komiteele. Terviklik lähenemine isikuandmete kaitsele Euroopa Liidus. KOM(2010) 609 lõplik. Brüssel: 04.11.2010. Arvutivõrgus: http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_et.pdf, (26.02.2018)
5. 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, 21.02.2018.
6. 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, 21.02.2018.
7. Free Snowden; Surveillance programs. Arvutivõrgus: https://edwardsnowden.com/surveillance-programs/ (15.03.2018)