CORE
Metadata, citation and similar papers at core.ac.uk
Provided by DSpace at Tartu University Library

TARTU ÜLIKOOL
SOTSIAALTEADUSTE VALDKOND
ÕIGUSTEADUSKOND
Karistusõiguse osakond

Olgert Rõõm

# SÜÜTUSE PRESUMPTSIOON SUURANDMETE AJASTUL

Magistritöö

Juhendajad:
*J.S.D* Helen Eenmaa-Dimitrieva
*LL.M* Kaspar Kala
*mag. iur.* Andres Parmas

Tartu
2017

# SISUKORD

# SISSEJUHATUS

Andmed on hulk numbreid või sõnu, mis on saadud andmesisestuse, mõõtmiste või mõne muu tegevuse tulemusena.[1] Suurandmeteks nimetatakse andmemassi, mis on saadud erinevatest allikatest nagu näiteks interneti otsingumootorite kaudu saadud informatsiooni andmelaod, suhtluskeskkondadest kogutud informatsioon jne, mida ei ole võimalik analüüsida tavapäraste meetoditega ühe serveri või arvuti baasil.[2]

Arvestuslikult on suurandmete turu kasvumäär kogu info- ja kommunikatsioonitehnoloogia (edaspidi „IKT“) turu kasvumäärast kuus korda kiirem, olles *International Data Corporationi* poolt aastateks 2013–2017 koostatud ülemaailmset suurandmete tehnoloogiat ja teenuseid käsitleva hinnangu kohaselt jõudnud kokku 50 miljardi euroni.[3] Tänapäevase digitaalse turu ehk ka infoühiskonna ulatust iseloomustavad alljärgnevad faktid: [4]

- käesoleval hetkel toodetakse kahe päeva jooksul sama palju andmeid kui aegade algusest kuni 2003. aastani kokku;
- 92% maailma andmetest on loodud viimase kahe aasta jooksul;
- igas kuus lisandub *Facebook*'i 30 miljardit infokannet;
- iga minut täieneb *Youtube* 72 tunni jagu videomaterjaliga;
- igas minutis luuakse 570 uut veebilehte;
- inimese DNA dekodeerimine võttis varasemalt 10 aastat, nüüd 7 päeva.

Tänapäeval on suurandmete kogumine ja töötlemine uue digitaalse turu lahutamatuks osaks. Nii eraettevõtted, kui ka valitsusasutused soovivad igapäevaselt leida uusi ja tõhusamaid viise, kuidas kogutud andmeid analüüsida ning väljundina saadavaid andmeid kasutada.[5] Eesmärgiks on saavutada võimekus, et kogutud andmemassist oleks võimalik andmete töötlemise ja

[1] Andmebaas. Kuidas vahet teha andmetel ja informatsioonil. Arvutivõrgus: http://andmebaas.ee/andmed-ja-informatsioon/ (25.04.2017).
[2] Privacy International, UK. Big Data: An introduction to Data Protection. The European Digital Rights papers 2013, No 6, lk 10. Arvutivõrgus: https://edri.org/files/paper06_datap.pdf (01.04.2016).
[3] Euroopa Parlamendi resolutsioon 2015/2612(RSP), 10. märts 2016. Eduka andmepõhise majanduse suunas liikumise kohta. Arvutivõrgus: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2016-0089+0+DOC+XML+V0//ET&language=ET (04.04.2016).
[4] E. Kert. Kuidas Big Data aitab teha paremaid krediidiotsuseid? Arvutivõrgus: https://web.creditinfo.ee/erki-kert-big-data.pdf (22.02.2016).
[5] M. Normet. Jälgimisühiskond ja mobiiltelefon. Akadeemia 2005/5, lk 949.

analüüsi käigus välja selekteerida kogu vajaminev info, mis võimaldaks teostada saadud tulemi pinnalt käitumismustritega seonduvaid ennustusi või võtta vastu otsuseid.

Suurandmed sisaldavad ka isikuandmeid, milleks on mis tahes andmed tuvastatud või tuvastatava füüsilise isiku kohta.[6] Isikuandmete puhul on tähtis välistada võimalus, et neid võidaks kasutada volitamata ning isikuandmete kaitset ja privaatsust rikkuval moel, sest selline kasutamine võib kaas tuua nii õiguskaitseasutuste järelevalvemeetmed kui mainekahju.[7] Nimelt võivad suurandmed hõlmata olulisi riske ja probleeme, eelkõige põhiõigusi puudutavates küsimustes (sh eraelu puutumatus ja andmekaitse). Kaitsmaks isikuid isikuandmete töötlemisel on loodud Euroopa Liidu (edaspidi „EL“) andmekaitse raamistik, mille eesmärgiks on tagada ka innovaatiliste ja konkurentsivõimeliste ärimudelite arendamine.[8] Andmekaitse põhimõtted võiksid olla ka stiimuliks, et töötada välja innovatiivseid viise avalikkuse teavitamiseks ja kaasamiseks.[9]

Võttes arvesse eeltoodut tuleks suurandmete kasutamisel leida optimaalne tasakaal turvalisuse tagamiseks vajaliku analüüsi teostamise ja andmete kaitsmise ulatuses. IKT ja tehnika areng on pannud inimesed olukorda, kus nad ei oska enam oma privaatsust kaitsta, kuna nad ei ole teadlikud meetmetest ja vahenditest, kuidas nende privaatsust võidakse rikkuda.[10]

Era- ja avalik sektor kasutavad üha enam suurandmeid ning seda enamjaolt ilma läbipaistva süsteemi ja aruandekohustuseta. Kogutud andmete põhjal teostatav universaalne ennustusmudel võib seada kahtluse alla fundamentaalsed õiguspraktikas kujunenud arusaamad, sealhulgas ka süütuse presumptsiooni.[11]

Süütuse presumptsioon on üks ausa kohtumenetluse tagajatest, mis aitab vältida kestvalt ja pidevalt kriminaalmenetlusõiguses tõusetuvate uute küsimuste lahendamisel menetleja poolt

---

[6] Isikuandmete kaitse seadus. – RT I 2007, 24, 127 … RT I, 06.01.2016, 10. § 4, lg 1. Arvutivõrgus: https://www.riigiteataja.ee/akt/106012016010 (29.03.2016).

[7] Suurandmed ja privaatsus. Juhendmaterjal organisatsioonidele, 19. jaanuar 2017, lk 10. Andmekaitse inspektsioon. Arvutivõrgus: http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/suurandmed_ja_privaatsus.pdf (15.03.2017).

[8] Euroopa Parlamendi resolutsioon 2015/2612(RSP), 10. märts 2016. Eduka andmepõhise majanduse suunas liikumise kohta.

[9] Suurandmed ja privaatsus, lk 3, 10.

[10] M. Männiko. Õigus privaatsusele ja andmekaitse. Tallinn: Juura 2011, lk 21.

[11] I. Kerr, J. Earle. How Big Data Threatens Big Picture Privacy. 66 Stan. L. Rev. Online 65, September 3, 2013, lk 67 Arvutivõrgus: https://www.stanfordlawreview.org/online/privacy-and-big-data/prediction-preemption presumption (22.02.2016).

hoiaku kujunemist "kõik on niigi selge".[12] Presumptsioonid on õigustehnilised võtted, mille ülesandeks on õiguse rakendamisprotsessile teatud suuna andmine. Millegi presumeerimine tähendab teatud väite tõepärasuse eeldamist seni, kuni pole tõendatud vastupidist.[13] Suurandmete kasutamisega kaasnevat süütuse presumptsiooni riivet saab kirjeldada läbi julgeoleku- ja politseiasutuste töös tõstatuva põhjendatud kahtluse olemasolu, millega üldjuhul põhjendatakse esmaste toimingute läbiviimise vajadust kuritegude ennetamiseks ning avastamiseks.

Isikuandmete kogumist ja töötlemist nii era-, kui ka avaliku sektori poolt võidakse kasutada eesmärgiga mõjutada neid, kelle kohta käiv teave on kokku kogutud, mida saab käsitleda kui jälgimist.[14] Jälgimisega kogutud andmete puhul on enamjaolt tegemist avalikkuse eest piiratud materjalidega, mis on mõeldud kasutamiseks ainult julgeoleku- ja politseiasutuste töös. Laiem avalikkus sai globaalses mahus teostatavatest andmete kogumisest ning sellega seonduvatest jälgimistest teada läbi *WikiLeaks*-i materjalide avalikustamise ja Edward Snowden-i kaasuse, mis käsitles Ameerika Ühendriikide (edaspidi „USA") Rahvuslik Julgeolekuagentuuri (edaspidi „NSA") poolt kogutud andmeid. Mõlemad illustreerivad USA poolt globaalses ulatuses läbiviidud andmete kogumist (sh massjälgimist) ja kasutamist ning suurandmete ja jälgimise omavahelist seost.[15]

Läbi massjälgimise on USA luureasutustel suuremal või väiksemal määral olnud juurdepääs EL-i üksikisikute isikuandmetele, mis on salvestatud või muul viisil töödeldud USA suuremate pilveteenuste osutajatega sõlmitud pilveteenuste lepingute raames. Tuvastatud on, et USA luureasutused on pääsenud juurde EL-i pinnal asuvatesse serveritesse salvestatud või muul viisil töödeldud isikuandmetele, murdes sisse *Yahoo* ja *Google* sisevõrkudesse. Välistada ei saa ka seda, et luureasutused on pääsenud ligi liikmesriikide riigiasutuste või ettevõtete ja institutsioonide poolt pilveteenustesse salvestatud teabele. Eeltooduga võib kaasneda era- ja perekonnaelu puutumatuse, teabevahetuse saladuse, süütuse presumptsiooni, sõna- ja teabevabaduse, kogunemis- ja ühinemisvabaduse ning ka ettevõtlusvabaduse riive.[16]

---

[12] E. Kergandberg, M. Sillaots. Kriminaalmenetlus. Tallinn: Juura 2006, lk 51.
[13] Kergandberg/Sillaots, lk 50.
[14] M. Normet, lk 949.
[15] D. Lyon. Surveillance, Snowden, and Big Data: Capacities, consequences, critique. Big Data & Society, July–December 2014, lk 1. Arvutivõrgus: http://bds.sagepub.com/content/spbds/1/2/2053951714541861.full.pdf (07.06.2016).
[16] Euroopa Parlamendi resolutsioon 2013/2188(INI), 12. märts 2014, USA Riikliku Julgeolekuagentuuri jälgimisprogrammi ja EL-i liikmesriikide jälgimisasutuste ning nende mõju kohta EL-i kodanike põhiõigustele ja Atlandi-ülesele koostööle justiits- ja siseküsimustes. Arvutivõrgus:

Käesoleva magistritöö eesmärkideks on välja tuua ning analüüsida suurandmete kasutamise erinevaid võimalusi ja meetodeid ning seda peamiselt korrakaitseorganite võimalikest huvidest ja eesmärkidest lähtuvalt ning samuti tuvastada, kas suurandmete kasutamine võib kaasa tuua võimaliku süütuse presumptsiooni riive seoses andemete alusel kujundatavate otsustega. Suurandmete kasutamist vaadeldakse töös enamjaolt USA praktiliste näidete alusel, kuna seoses toimunud *WikiLeaks*-i avalikustamistega ja Edward Snowden-i kaasusega on need kõige ülevaatlikumad jälgimise käigus kasutatavate meetodite ja taktika osas. Seoses eelnevalt mainitud avalikustamistega on käesolevat tööd võimalik avaliku sektori poolt kasutatavate meetodite ja taktikaga seonduvate andmetega ka sisustada. Töö sisaldab näiteid, kuidas on võimalik kogutud suurandmeid kasutada ning millised ohud kaasnevad automaatselt töödeldud andmete alusel järeldusotsuste tegemisega.

Magistritöö teema on päevakohane ja oluline, kuivõrd IKT kiire arenguga seonduvalt tekib maailmas igapäevaselt rohkelt andmeid. Andmeid analüüsitakse ja töödeldakse loodud arvutialgoritmide ning kaasaegsete andmetöötlusvahenditega, loomaks otsuste vastuvõtmist võimaldavaid korrelatsioone, suundumusi ja mudeleid. Andmete pinnalt järeldusotsuste teostamine võib kaasa tuua süütuse presumptsiooni riive seoses nende alusel otsuste kujundamisega. Nimelt arvestades isiku kohta olemasolevaid andmeid kujundatakse nende pinnalt tema osas toimingute läbiviimiseks seisukohad ning põhjendatakse neid selle alusel ka kohtu jaoks jälitustoiminguteks loa saamisel. Käsitletud teema aktuaalsusele on viidanud ka Kalev Hannes Leetaru, keda nimetatakse internetiajastu üheks juhtivaks novaatoriks ning peetakse suurandmete valdkonnas teerajaks.[17] Leetaru sõnul on suurandmed väga võimsad, sest need võimaldavad näidata laiemat pilti ja anda aimu, kas oleme jätnud midagi märkamata.

Eeltoodust tulenevalt püstitab magistritöö autor hüpoteesi, et suurandmete kogumine seoses võimalike kuritegude ennetamise ning sellega seonduvate protsesside suunamisega võib viia selleni, et andmetest saab süüstavate järelmite kogum. Suurandmete analüüsi käigus saadu võimaldab teha ennatlikke järeldusi isiku süü tõendatuse osas, mis võib kaasa tuua süütuse presumptsiooni riive.

---

http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0230+0+DOC+XML+V0//ET (04.04.2016).

[17] O. Eylandt. Eesti juurtega IT-geenius: ühes asjas Orwell eksis. Eesti Päevaleht, 7. jaanuar 2017. Arvutivõrgus: http://m.epl.delfi.ee/article.php?id=76787520 (07.01.2017).

Magistritöös püstitatud hüpoteesi tõesuse kontrollimiseks püstitab autor järgmised uurimisküsimused:

1. Mis on suurandmed? Mis on suurandmete kasutusvõimalused? Millised on andmete kasutamise võimalused ennetusotsuste teostamiseks ja analüüsiks? Mis on suurandmete töötlemisega kaasnevad mõjud isikute õigustele?
2. Mis on süütuse presumptsioon ja kuidas võib selle sisustamine muutuda suurandmete ajastul? Kas suurandmete pinnalt kujundatud otsused on piisavad põhjendatud kahtluse olemasolu kinnitamiseks?
3. Kas suurandmete kasutamine toob kaasa võimalikud süütuse presumptsiooni riived? Kuidas mõjutab suurandmete kasutamine isikute õigusi ja tõendite kujunemist?

Magistritöö koosneb neljast peatükist, mis vastavalt teemakäsitlustele jagunevad alapeatükkideks.

Esimene peatükk magistritöös käsitleb suurandmete mõistet ja kasutajaid ning nende kogumise ja kasutamise võimalusi. Samuti nende kasutamisega kaasnevaid kasutegureid ja privaatsusega seonduvaid ohte ning isikuandmete kaitse võimalusi. Lisaks käsitletakse peatükis suurandmete põhiseid analüüsi teostamise võimalusi ja nende kasutusvõimalusi.

Teises peatükis käsitletakse suurandmete kasutusala ja olemasolevaid isikuõiguste kaitse võimalusi. Peatükk annab ülevaate elektrooniliste ja sideandmete kogumisest ja kasutamisest EL-is ning Eesti õigusruumis.

Magistritöö kolmas peatükk annab ülevaate süütuse presumptsiooni ajaloolisest sisust ning selle tähendusest ja käsitlusest. Peatükis käsitletakse süütuse presumptsiooni võimalikke riiveid ja põhjendatud kahtluse kujunemist seoses suurandmete alusel teostatavate otsustustega.

Neljas peatükk käsitleb suurandmete hindamist, nende põhjal tehtud otsuseid ja kujunenud tõendite usaldusväärsust. Samuti käsitletakse peatükis ka suurandmete töötlemisega kaasnevaid mõjusid isiku õigustele. Peatükk võtab ühtlasi ka kokku suurandmete põhjal tehtud otsuste ja saadud teadmiste mõju süütuse presumptsiooni tagamisele.

Käesoleva magistritöö puhul on tegemist teoreetilise uurimusega, milles töö autor kasutab analüütilist meetodit. Autor püüab töös tõstatatud küsimustele leida vastuse erialase kirjanduse

kaudu. Magistritöös on allikmaterjalina kasutatud erialapõhist kirjandust, õigusteadlaste artikleid ning nii siseriiklikke kui ka teiste Euroopa riikide õigusakte ja kohtupraktikat.

Märksõnad: internet, suurandmed, süütuse presumptsioon, kriminaalmenetlus.

# 1. SUURANDMED JA NENDE KOGUMISE VÕIMALUSED

Viimase sajandi jooksul on maailmas toimunud kiire tehnoloogia areng, mis on ühiskonnale avaldanud laiapindset mõju. Arvutite areng on muutnud kommunikatsiooni ja informatsiooni edastamise kiireks, tõhusaks ning odavaks. Informatsiooni on võimalik lihtsalt hoiustada ja suurtes mahtudes edastada, selekteerida ning transformeerida vastavalt vajadusele ja kontekstile.[18]

## 1.1 Internet ja suurandmed

### 1.1.1 Internet ja salvestuvad andmed

Interneti juured ulatuvad 1960. aastatesse, mil USA-s rajati sõjalisel eesmärgil ja vaid piiratud kasutajate hulgale (ca 0,1% maailma elanikkonnast) tänapäevase Interneti eelkäija ARPANET. Internet on 1990ndatel populaarseks saanud termini küberruum[19] peamine ja olulisem osa. Selline muutus on võimaldanud liigutada majanduslikke, poliitilisi, geograafilisi ja sotsiaalseid piire[20]. Internet on mänginud kandvat rolli loomaks uut liiki tegevusi võimaldavat küberruumi ehk siis tulenevalt tehnika ning IKT kiirest arengust on Internet teinud oma levikus ja arengus märkimisväärse hüppe. Näiteks 2014. aastaks oli interneti kasutajate arv maailmas kasvanud ligikaudu 2,8 miljardi kasutajani, mis moodustas umbes 40% maailma rahvaarvust. 2015. aasta novembri seisuga kasutas internetti juba 46,4% maailma elanikkonnast. Kuigi Internet on oma olemuselt globaalne, on regiooniti selle kasutuserinevused küllalt suured: Põhja-Ameerikas 87%, Euroopas 73%, Aasias 40%, Aafrikas 28% elanikkonnast.[21] Siinjuures on oluline, et nii Interneti kui ka küberruumi kasutajate arv on maailmas plahvatuslikult kasvanud just viimase aastakümne jooksul ning kogu protsess on avaldanud tohutut mõju pea kõikidele ühiskonna valdkondadele.

[18] P. Birkinshaw. Freedom of Information: The Law, the Practice and the Ideal. 3. Ed. UK: Hobbs the Printers Ltd 2001, lk 10, 11.
[19] Küberruum on mõtteline keskkond, kus toimub suhtlemine arvutivõrkude kaudu. Arvutivõrgus: https://en.oxforddictionaries.com/definition/us/cyberspace (25.04.2017).
[20] Wall, D. S. Cyberspace Crime. England: Dartmouth Publishing Company Ashgate Publishing Limited 2003, lk 477.
[21] Internet Usage Statistics: The Internet Big Picture. Internet World Stats. Arvutivõrgus: www.internetworldstats.com/stats.htm (22.02.2016).

Internet ei ole disainitud mitte turvalisust silmas pidades, vaid eesmärgiga luua efektiivne informatsiooni edastamise kanal, mistõttu on informatsiooni kaitsmine Internetis suur väljakutse nii kasutajatele, teenuse pakkujatele, kui ka õiguskaitseasutustele.[22] Internetis sisalduv andmetest moodustuv kogum isiklikest ja mitteisiklikest seostest võimaldab vajadusel kogumitesse grupeerida sarnaste huvide, ideede ning tegevustega isikuid.[23] Antud informatsiooni pinnalt tuvastatavad seosed annavad informatsiooni töötlusele väärtuse.[24] See võimaldab luua informatsiooni põhjal seoseid ning teha järeldusi.

Riigid või asutused, kes jälgivad Internetis toimuvat liiklust saavad analüüsida kõiki krüpteerimata pakette ehk suuremat osa veebiliiklusest. Juhul kui paketi sisu on krüpteeritud, siis saab jälgija teada, kelle poolt pakett saadeti, kuna see saadeti ja mis on selle sihtpunkt. Internet on üles ehitatud nii, et ei ole võimalik ette määrata, kuidas mingi pakett sihtkohta jõuab. Pakett liigub kõige optimaalsemat teed kasutades sihtpunkti. Seetõttu ei saa Internetis vältida paketi liikumist läbi riikide, mis jälgivad ja salvestavad Internetis toimuvat liiklust. Näiteks ei saa Eesti Vabariigis (edaspidi „EV“) vältida andmeside edastamist läbi Rootsi Kuningriigi (edaspidi „Rootsi“), sest tänu kiiretele ühendustele liigub suur osa riigist väljuvast andmesidest just läbi Rootsi.[25]

Internetipõhised suhtluskeskkonnad võimaldavad nende kasutajatel suhelda paljude inimestega odavalt ja lihtsalt. Selline suhtlus tekitab suures koguses andmeid, mille mahud ja salvestamine on käesoleval hetkel, võrreldes varasemate aegadega, hüppeliselt kasvanud. 1965. aastal ennustas Gordon Moore, et mikrokiibil olevate transistoride arv kahekordistub iga kahe aasta järel. Seda nimetatakse Moore'i seaduseks. Tegelikkuses on kasv aga osutunud veelgi kiiremaks. Nimelt on protsessorite kiirus ehk taktsagedus ja operatiivmälu mahu võimekuse kasv toimunud iga 18 kuu jooksul. Suurenenud andmete maht on toonud kaasa nende väärtuse kasvu. Andmete mahu kasvuga on aga kaasnenud väljakutse, kuidas neid järjest efektiivsemalt analüüsida.[26]

---

[22] X. Li. Cybercrime and Deterrence: Networking Legal Systems in the Networked Information Society. Turku: Turun Yliopiston oikeustieellisen tiedekunnan julkaisuja 2008, lk 176.
[23] J. Zittrain. The Future of the Internet And How To Stop It. Yale University Press New Haven and London 2008, lk 234.
[24] P. Birkinshaw, lk 18.
[25] Turvaline veebiliiklus: HTTPS. Miks internetiliiklust saab pealt kuulata ja jälgida. Tartu Ülikool: Loodus- ja täppisteaduste valdkond, arvutiteaduse instituut. Arvutivõrgus: https://courses.cs.ut.ee/2015/infsec/Et/HTTPS (20.03.2017).
[26] NIST Big Data Interoperability Framework: Volume 1, Definitions. National Institute of Standards and Technology U.S Department of Commerce, lk 4. Arvutivõrgus: http://bigdatawg.nist.gov/_uploadfiles/NIST.SP.1500-1.pdf (22.02.2016).

Miljonitesse arvutitesse maailmas salvestuvad igapäevaselt erinevad andmed. Viimase kolme aastakümne jooksul on iga 14 kuu tagant andmete salvestusmahud kahekordistunud. Nõudlus on hakkama saada andmemahtudega, mis ulatuvad juba terabaitidest petabaitideni ja isegi ka zettabaitideni.[27] Eeldatakse, et arvutitesse salvestatud andmete maht kogu maailmas on tänapäeval juba umbes 300 exabaiti, mis on 300 miljardit gigabaiti ning andmete salvestamise maht suureneb iga aastaga umbes 28%. Samas on salvestatud andmete maht võrreldes infoga, mida edastatakse ilma seda salvestamata väga väike. Iga-aastane andmete edastus maailmas on eelduslikult kokku kuni 1,9 zettabaiti, mis on 1900 miljardit gigabaiti. Sellest kasvavast andmemahust kujunevadki järgmise põlvkonna andmeressursid.[28]

Tänapäeval, kus peaaegu pool maailma elanikkonnast kasutab suhtluseks *online*-kanaleid, toob see endaga kaasa enneolematult suures koguses väga mitmesugustest allikatest pärinevaid andmeid. Sellest tulenevalt on muutunud ajas ka arusaam, kuidas erinevat teavet nähakse ja käideldakse ning kuidas uusi mooduseid struktureerimata andmeallikate info kasutuseks leitakse. Isikutel on lihtsam juurde osta salvestusmahtu, kui hakata läbi vaatama ja kustutama andmeid, mis võivad kunagi hiljem vajalikuks osutuda. Ettevõtted omakorda on andmete kasvavast väärtusest hästi aru saanud ning töötavad aktiivselt välja uusi strateegiaid, kuidas paremini ja kasumlikumalt andmeid käidelda.[29] Kuigi andmetel on kasvav väärtus, siis andmete hoiustamise hind on väga suures ulatuses viimase kümnendi jooksul langenud ning see trend on jätkuv.[30]

Internet on muutnud isikute vahelist suhtlust kaotades ära barjäärid, mis on seotud näiteks nii distantsi, ajaliste ja finants võimalustega. Selline suhtlus tekitab suures koguses andmeid, mida saab analüüsida ja transformeerida otsusteks.

### 1.1.2 Suurandmete mõiste

Suurandmeid saab iseloomustada kui andmekogumeid, mille peamisteks omadusteks on maht, erinevate andmeformaatide paljusus, andmete kiirus ja varieeruvus, ning mis nõuavad

[27] B. Akhgar, jt. Application of Big Data for National Security: a practitioner´s guide to emerging technologies. 1 Ed. Amsterdam: Elsevier/Butterworth-Heinemann 2015, lk 3.
[28] J. J. Berman. Principles of Big Data: Preparing, Sharing and Analyzing Complex Information. Elsevier Inc., 2013, lk 15.
[29] B. Akhgar, jt., lk 3.
[30] T. Craig, M. E. Ludloff. Privacy and Big Data. O'Reilly 2011, lk 17.

mõõdetavat arhitektuuri, tõhusat salvestusvõimekust, andmete käsitlust ja analüüsi. Neid saab kirjeldada kui keerulist, kiirelt muutuvat ja massiivset andmete kogumit, mis ületab igapäevaselt laialdaselt kasutatava tarkvara analüütilise võimekuse seda korrastada. [31] Traditsioonilised andmed aga on see-eest väikse mahuga andmed ehk väikeandmed, mis on defineeritavad kui elektroonilised andmed, mis on salvestatud andmebaasides, andmeladudes ja olemasolevates süsteemides.[32]

Suurandmed on muutunud liiga mahukaks, et neid konventsionaalsete meetmete ja seadmetega oleks võimalik käidelda.[33] Ehk siis suurandmed kujutavad endast andmeid, mille maht ületab tavalise konventsionaalse andmebaasi töötlusvõimekuse – andmemaht on liiga suur, see muutub kiiresti ja ei sobitu andmebaasi arhitektuuri piiridesse.[34] Suurandmete omadused, mis sunnivad uut arhitektuuri ümber kujundama on: [35]

- suurandmete maht (andmekogumi suurus);
- andmeformaatide paljusus (andmed mitmetest hoiukohtadest, domeenidest);
- andmete tekkimise ja töötluse kiirus (kiiruse määr);
- andmete muutuvad omadused (muutumine erinevate tunnuste alusel).

Suurandmete laialdasele kasutusele on kaasa aidanud üha suuremate andmehulkade salvestamiste võimaluste levik ja andmete töötlemise võimekuse kasv ning seda järjest väiksema raha eest. Koos arengute ning edusammudega teaduses, meditsiinis ja majanduses kasvab igapäevaselt allikate hulk, mis andmeid toodavad. Seda eriti läbi elektroonilise kommunikatsiooni nagu e-post, raadiosageduslik identifitseerimine (RFID), mobiilne kommunikatsioon ja sotsiaalmeedia kasutamine. Samuti ettevõtlusega seotud andmed nagu jaekaubandus, transport, kommunaalteenused ja sensortitelt ning satelliitidelt saadavad andmed. Üldjuhul on antud andmete näol tegemist töötlemata toormaterjaliga ning neist korralike ja kvaliteetsete reaalselt kasutatavate andmete saamiseks on vajalik nende mitmekordne töötlus ning analüüs. Arvestuslikult on ligi 80% eelpool kirjeldatud andmetest üldse struktureerimata või pooleldi struktureeritud.[36]

[31] E. Dumbill. Big Data Now: 2012 Edition. 1 Ed. O'Reilly Media Inc., 2012, lk 3.
[32] C. Batini, M. Scannapieco. Data Quality: Concepts, Methodologies and Techniques (Data-Centric Systems and Applications). Springer-Verlag Berlin Heidelberg 2006.
[33] B. Akhgar, jt.,lk 3.
[34] E. Dumbill 2012, lk 3.
[35] NIST Big Data Interoperability Framework: Volume 1, lk 5.
[36] B. Akhgar, jt., lk 3.

Pikaajalisi kogemusi igapäevaselt suures mahus andmete struktureerimisega omavad mitmed suurettevõtted (nt *Facebook, Twitter, Google* või *Yahoo*). Need ettevõtted on juba pikka aega tegelenud suurte andmemahtude töötlemisega ning nende puhul on tegemist esmaste suurandmete töötlemise tehnoloogia arendajate ja kasutajatega. Viimase aja areng ja nn asjade internet[37] on andmete loomist veelgi suuremas mahus kasvatanud. Seadmete kasutamise moodused on muutunud ning ka lihtne fotoülesvõte sisaldab tänapäeval suures mahus metaandmeid[38]. Lisaks intelligentsele pildituvastus- ja näotuvastussüsteemile on võimalik fotodele lisada ka muid andmeid nagu näiteks foto nimetus, selle teinud isiku andmed, fotol olevad isikute nimed, foto tegemise geograafiline asukoht, foto tegemise kellaaeg ja kuupäev jms. Seda kõike on võimalik teha samaaegselt, fotot internetti üles laadides.[39]

Suurandmed sisaldavad endas ka isikuandmeid, sest *online*-tegevus jätab erinevatest toimingutest maha jälgi, mille alusel on võimalik tuvastada, kes isik on, mida ta ostab, kus käib jne.[40] Info töötlemine toimub näiteks vastavalt vanusele, soole, sissetulekule, riigi ja linna ehk asukoha alusel ning ka lehekülgede järgi, mida külastatakse ja mis meeldivad. Vastavalt käitumisharjumustele on isikud jagatud gruppidesse ning andmeid nende kohta võidakse müüa või anda inimeste teadmata kasutamiseks kolmandatele osapoolte, kes soovivad neid oma ärihuvidest lähtuvalt kasutada.[41] Näiteks on võimalik läbi viia rassipõhiseid analüüse. 2010. aastal teostati suhteportaal *OKcupid* poolt uuring[42] „Reaalsed asjad, mis meeldivad valgetele inimestele". Uuringust lähtuvalt oli märksõnade abil võimalik kindlaks teha isikute sugu, usulist kuuluvust ja seksuaalset orientatsiooni ning rassi.

Kogutud andmete töötlemine võimaldab erinevatel organisatsioonidel ja ka valitsusasutustel leida isikute kohta infot ning kasutades analüütilisi mudeleid ennustada nende võimalikku tulevikus asetleidvat käitumist. Ennustada on võimalik nii isikute huvidest lähtuvaid tuleviku

[37] Asjade internet ehk värkvõrk (inglise keeles IoT Internet of Things) on internetiühendusega seadmete võrk, kus need kasutaja ja üksteisega informatsiooni jagavad ja vahetavad ning koos teatud ülesandeid täidavad. Need seadmed võivad olla nii nutitelefonid, külmikud, pesumasinad, nutikellad, meditsiiniseadmed, hooned kui ka näiteks lennukimootorid. Lihtsaim asjade interneti näide see, kui garaažiuksed saavad aru, et omaniku auto on läheduses või kui omanik saadab käsu ukse avamiseks oma nutitelefonilt. Arvutivõrgus: http://forte.delfi.ee/news/tarkvara/ulevaade-asjade-internet-ja-mis-sellest-kasu-on?id=73717233 (02.01.2017).

[38] Metaandmed on andmed andmete kohta nagu IP-aadress, kõnede teostamise või sõnumite saatmise asukoht ja kestvus.

[39] B. Akhgar, jt., lk 4.

[40] Craig/Ludloff, lk 2.

[41] Craig/Ludloff, lk 13,14.

[42] C. Rudder. The Real Stuff White People Like. September 8, 2010. Arvutivõrgus: http://blog.okcupid.com/index.php/the-real-stuff-white-people-like/ (21.03.2016).

oste, poliitilist eelistust kui ka isegi võimalikku kriminaalset käitumist.[43] Näiteks kui isik ostab poest midagi, siis kaup, mida ostetakse seotakse kliendi identifitseerimisnumbriga võttes arvesse tema krediitkaardi andmeid, nime ja aadressi juhul kui klient ostu eest tasumisel kliendikaarti kasutab. Selliseid andmeid saab edaspidi kasutada ka selleks, et ennustada, millal poekülastaja vajab teatud kaupu. Antud meetodil kogutud informatsiooni kasutatakse täna peamiselt reklaami edastamise eesmärgil. USA-s Minneapolises leidis aset juhtum, kus teismelisele saadeti poest sooduskuponge rasedusega seonduvatele esemetele. Teismeline oli küll lapseootel, kuid ta ei olnud sellest veel oma vanematele rääkinud. Teismelise isa, kes neid reklaame nägi, esitas poe suhtes kaebuse, kuid sai seejärel teada, et tema tütar ootabki last. Peale toimunud vahejuhtumit muutis kauplus oma reklaamipoliitikat, kuna sai aru, et eelnevalt kehtinud otsepostitus isiku ostude alusel võib kaasa tuua ebameeldivaid situatsioone. Eeltoodu tõi kaasa selle, et kauplus muutis otsereklaami edastamist paigutades selle teiste pakkumiste hulka, et ei oleks võimalik tuvastada isikupõhiseid suunatud pakkumisi. Otsereklaami edastavad kauplused omavad kliendist head ülevaadet, mis hõlmab nende vanust, elukohta, etnilist tausta, milliseid toiduained nad ostavad ning mida neile meeldib lugeda.[44]

Otsereklaami rakendavad ka EV-s mitmed suuremad kaubandusketid ning seda teostatakse kliendikaartidega seotud ostude analüüsi põhjal. Elektroonilise side andmete kasutamine otseturunduseks on EV-s reguleeritud elektroonilise side seadusega[45] (edaspidi „ESS“), mille § 103[1] lg 1 kohaselt on füüsilisest isikust sideteenuse kasutaja või kliendi elektroonilise kontaktandmete kasutamine otseturunduseks lubatud üksnes tema eelneval nõusolekul. ESS § 103[1] lg 2 kohaselt on lubatud juriidilisest isikust sideteenuse kasutaja või kliendi elektroonilise kontaktandmete kasutamine otseturunduseks juhul kui:

- kontaktandmete kasutamisel antakse iga kord selge ja arusaadav võimalus tasuta ja lihtsal viisil keelata oma kontaktandmete selline kasutamine;
- isikul võimaldatakse oma õigust keeldumisele realiseerida elektroonilise side võrgu kaudu.

[43] Craig/Ludloff, lk 17.
[44] M. Mozer. Big Data and You. New York: The Rosen Publishing Group Inc., 2015, lk 33.
[45] Elektroonilise side seadus. – RT I 2004, 87, 593 … RT I, 23.03.2017, 5. Arvutivõrgus: https://www.riigiteataja.ee/akt/117052016002?leiaKehtiv (22.03.2017).

### 1.1.3 Suurandmete väärtus

IKT areng on võimaldanud transformeerida informatsiooni. Samuti võimaldanud selle konteksti paigutamist, eesmärgipärast hoiustamist, analüüsi ja käitlemist[46]. Andmed, mida suurandmetest selektsiooni ja analüüsi käigus soovitakse tuvastada ning mis annavad nendele väärtuse on järgnevad:[47]

- demograafilised ja geograafilised andmed
  - vanus;
  - sugu;
  - rahvus;
  - religioon;
  - haridus;
  - sissetulek;
  - kinnisvara omamine;
  - sotsiaalne ja majanduslik staatus;
  - asukoha põhised faktorid.
- psühholoogilised käitumispõhised andmed
  - reklaami mõjud;
  - tarbimisega seotud mõjud;
  - tarbimispõhisus (tavaklass, äriklass);
  - elustiilist või ühiskondlikust staatusest tulenev mõju;
  - ostupõhisus;
  - poliitiline kaasatus ja segmentatsioon;
  - andme- ja mobiilside kasutuvalikud.
- isiku käitumispõhised andmed
  - isiksusega seonduv (avatus, otsustuskindlus, ekstravertsus, vastutulelikkus, neurootilisus);
  - mõjutatavus (vastandumine, vajadused, autoritaarsus, hirm, sotsiaalse staatuse vajadus).

[46] D. S. Wall, lk 478.
[47] A. Nix. The Power of Big Data and Psychograohics. Concordia Summit 2016. Presentation. Arvutivõrgus: https://www.youtube.com/watch?v=n8Dd5aVXLCc (10.03.2017).

Suurandmete suurimaks väärtuseks on tulem, mida luuakse läbi suurandmete analüüsi ja töötlemise. Suurandmete kasutajad on aru saanud, et tõeline väärtus saavutatakse töötlemata andmetest läbi analüüsi kujunevatest seoste. Kasutajad saavad protsessi käigus kujunevat infot oma tegevuses efektiivsemalt kasutada tõhustades seeläbi nii oma tegevuse tootlust, protsesse kui ka klientide suunatud teenuseid.[48]

Selleks, et eelnevalt kirjeldatud väärtust luua tuleb läbida mitmeid andmete töötluse samme ja kombinatsioone. Kvaliteetsete andmete saamiseks on vajalik teostada järgnevad sammud: [49]

- tuvastamine – andmeallikaid tuleb tuvastada ning hinnata läbi saadava info väärtuse, kvaliteedi ja maksumuse;
- selekteerimine – tagab usaldusväärse käitlemise kogu andmete ulatuses;
- käitlemine – läbi selektsiooni toimub andmete automaatne töötlus, et transformeerida need formaati, mis võimaldaks korduvkasutust ning tulenevalt uuest infost kohest seoste tuvastamist;
- kujundamine – andmete formaat ning andmebaasi tehnoloogiline valik on sageli mõjutatud teistest väärtuspõhistest sammudest, eriti analüüsist;
- integreerimine – samm, mille käigus toimub info kombineerimise protsess;
- analüüsimine – on oluliseks kriitiliseks elemendiks igas eelkirjeldatud sammus, moodustades 80% kogu andmete töötlusest;
- väljundumine – analüüsi käigus saadud andmed muutuvad töötluse käigus kasutajatele kasulikuks ning neid saab väljundina kasutada.

Järgides eelpool nimetatud samme on väljundiks andmete transformatsioon informatsiooniks. Andmete analüüsi ja töötlusega saavutatakse andmete suurim väärtus, mis väljendub saadavas teabes.

### 1.1.4 Isikuandmed ja nende kasutamine

Arvutid koguvad ja toodavad pidevalt isikupõhiseid personaalseid andmeid. Näiteks seda, mida kindla arvuti kasutaja loeb, vaatab või kuulab. Samuti seda, kellega isik suhtleb või mida räägib.

[48] E. Dumbill. Understanding the Data Value Chain: Adopt a different wiew of data as a raw mateerial for the data lifecycle bussiness resource. IBM Big Data & Analytics Hub, November 10, 2014. Arvutivõrgus: http://www.ibmbigdatahub.com/blog/understanding-data-value-chain (18.03.2017)
[49] E. Dumbill 2014.

Näiteks talletab protsessor kõik, mida isik on kirjutanud, sh kaasaarvatud mustandid ja muudatused, mida isik selle kasutamisel teeb. Kui vajutada salvestamise nuppu, siis registreerib protsessor kohe uue versiooni, kuid arvuti ei kustuta vanemat versiooni ära seni, kuni arvuti kõvakettal ruumi jätkub. Internetti ühendudes toodetavad andmed kahekordistuvad. Näiteks andmed lehekülgedest, mida külastatakse, lisad, millele klikitakse, milliseid otsingusõnu kasutatakse jne. Internetibrauser edastab külastatavatele lehtedele infot, mis tarkvara kasutatakse, millal oli see installeeritud ja millised seadistused on lubatud.[50]

Otsinguandmete kogumi pinnalt on võimalik tuvastada näiteks poliitilisi ja usulisi vaateid, maailmavaatelisi veendumusi, tuvastada etnilist päritolu ja rassi. Otsingumootorites päringuid tehes on isikud enamjaolt avatumad, kui oma sõprade, töökaaslaste või perekonnaliikmetega ning samuti selles osas, mille kohta nad informatsiooni soovivad leida. Üldjuhul kirjutatakse alati välja, millest mõeldakse ehk mida otsitakse. Samas *Google* talletab, mis infot otsitakse, kelle kohta otsitakse, millised on inimeste probleemid jne. Kuna *Google* kasutamisel salvestub kõik ja määramata ajaks, siis on võimalik selle kaudu tuvastada, milline on kasutaja elustiil, harjumused ja vajadused. Näiteks kui lülitada sisse *Google* automaatne lünkade täitmise funktsioon, mis lõpetab otsingu ise vastavalt algosa kriteeriumitele, siis näiteks trükkides otsingusõna „kas ma peaksin oma n" pakkus *Google* välja: „Kas ma peaksin oma naisele ütlema, et mul on afäär". *Google* teab, kes on sellistele otsingusõnadele vajutanud ja otsinguid teostanud. *Google* tegevdirektor Eric Schmidt tunnistas 2010. aastal: „Teame, kus te olete, kus te olete varasemalt olnud ja me teame rohkem või vähem sellest, millest te mõtlete". Kui isikul on lisaks ka veel *Gmail*-i konto, siis on tal võimalik ise oma otsingute ajalugu vaadata iga korra osas, mil ta sisse logib. Ajalugu võimaldab minna tagasi, kuni konto loomiseni.[51]

Kuigi *Google* annab võimaluse muuta määratud seadistuste eelistusi, siis kustutada kõike seda, mis kasutajale ei meeldi, ei ole siiski võimalik. Salvestada on võimalik näiteks kasutaja otsitud termineid, IP-aadressi,[52] aega ning muud informatsiooni ehk otsinguteenuse osutajad töötlevad konkreetseid üksikisikute otsinguteenuste kasutamise logifaile eeldusel, et need ei ole muudetud anonüümseks. Otsinguteenuse osutaja võib ühelt IP-aadressilt pärinevaid eri

[50] B. Schneier. Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. W.W. Norton & Company, 2015, lk 13.
[51] B. Schneier, lk 22.
[52] IP tähendab internetiprotokolli, mis on osa internetis andmete ülekandel kasutatavast suhtlusprotokollist TCP/IP (Transmission Control Protocol/Internet Protocol). Arvutivõrkudes ja internetis ei tuvasta arvutid ja teised nutiseadmed teineteist mitte neile antud nimedega, vaid numbritega, mida nimetatakse IP-aadressiks.

taotluseid ning otsinguseansse siduda, mistõttu tekkib võimalus jälgida ja omavahel seostada kõiki ühelt IP-aadressilt tulenevaid veebiotsinguid. Teenuse kasutamist kirjeldavad andmed võib jagada erinevatesse kategooriatesse:

- päringulogid (otsingupäringute sisu, kuupäev ja kellaaeg, allikas, IP-aadress ja küpsis, kasutaja eelistused aga ka kasutaja arvutiga seotud andmed);
- andmed pakutud sisu kohta (iga päringu tulemuseks olnud viidad ja reklaamid);
- andmed kasutaja iga päeva liikumise kohta (klõpsud/klikid).[53]

Lisaks IP-aadressile võivad seadmed väljastada võrguliikluse käigus ka teisi identifitseerimisnumbreid nagu näiteks seadme võrgukaardi aadress ehk *Media Access Control* (MAC), mobiiliseadme (nutitelefon, tahvelarvuti, netipulk) unikaalse 15-kohaline numbri ehk International *Mobile Equipment Identity* (IMEI) või seadme kasutaja nime. IP-aadressi teades saab näiteks teha kindlaks, kellele võrk kuulub, kes seda haldab. Samuti leida teavet teenust pakkuva ettevõtte kohta. Võimalik on jälgida andmeedastuse teekonda, et leida loogiline tee arvutini ja teha kindlaks selle geograafiline asukoht. Erinevate otsinguteenuste abil on võimalik tuvastada failivahetuse ja/või isikute veebitegevusi (nt *Wikipeedia* toimetamine). Kõik sellised osad võivad üheskoos anda ülevaate alates isikute huvidest, hobidest, ja isikuomadustest, lõpetades poliitiliste eelistuste, terviseseisundi, seksuaalse orientatsiooni ning usuliste tõekspidamistega. Eeltoodud IP-aadressi põhised kasutajaandmed loetakse isikuandmeteks, mida sideettevõtjad ja teised organisatsioonid ning eraisikud ei tohi kolmandale osapoolele avaldada, välja arvatud kasutaja nõusolekul või seaduse alusel.[54] Minimeerimaks infokogumist ja kaitsmaks enda isikuandmeid ning internetikasutuse ajaloo põhjal teostatavaid analüüse tuleks muuta otsingumootorite seadistusi ja privaatsussätteid. Näiteks keelata ära domeenide poolt küpsiste seadmine või vastav domeen täielikult blokeerida.[55]

Tänapäeva tehnikaajastu on toonud kaasa laialdase mobiiltelefonide kasutamise, mis on tekitanud olukorra, kus arvuti funktsionaalsus ja võimalused on üle kandunud mobiiltelefonidesse. Mobiiltelefonid on muutunud elu keskmes olevateks tehnikavahenditeks, millega on võimalik suhelda kõikjal ning seda olenemata ajast ja kohast. Telefonide kasutusega

---

[53] M. Männiko, lk 114.

[54] Metaandmed ja privaatsus. Juhis organisatsioonidele ja kodukasutajatele seaduse rakendamisel, 28. oktoober 2015. Andmekaitse Inspektsioon. Arvutivõrgus: http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/Juhis%20-%20IP%20ja%20privaatsus.pdf (01.03.2016).

[55] Privaatsus ja anonüümsus veebid. Tartu Ülikool. Arvutiteaduse Instituut. Arvutivõrgus: https://courses.cs.ut.ee/2015/infsec/Et/Loeng-Anon%C3%BC%C3%BCmsusVeebis (01.03.2016).

kaasneb teenusepakkujal võimalus tuvastada, kus isik parasjagu viibib ja seda kogu telefoni kasutamise aja jooksul. See on midagi, mida ei fikseerita üheski lepingus, kuid süsteemile on selline töötamise viis omane. Mobiiltelefonide tööpõhimõte lähtub sellest, et sideettevõtja saab teada, kus seade parasjagu asub ning see annab võimaluse järelevalve teostamiseks. Tegemist on väga sensitiivse jälgimise vormiga, sest telefon fikseerib, kus selle kasutaja parajasti viibib, mis omakorda võimaldab tuvastata näiteks isiku elu- ja töökoha asukohad. Samuti on teostatava analüüsi pinnalt võimalik tuvastada, kus veedetakse vaba aega ning kui tihti ja mis marsruutidel liiklusvahendeid kasutatakse. Mobiiltelefonide kasutajakoha andmete ühendamisel teiste samas piirkonnas viibivate seadmete andmetega on võimalik tuvastada ka isikutevahelisi kohtumisi. Näiteks 2012. aastal teostatud uuringus suutsid selle läbiviijad ennustada, kus isik viibib 24 tunni pärast ja seda 20 meetrise täpsusega. Enne mobiiltelefonide laialdast kasutuselevõttu tuli sellise informatsiooni kogumiseks üldjuhul kasutada eradetektiivide teenuseid, kes isikut füüsiliselt jälgisid ja vajalikku informatsiooni talletasid.[56]

Internetis ja sotsiaalmeedias aktiivselt oma eraelulist infot jagavatel isikutel tuleb alati arvestada sellega, et olenemata erinevatest privaatsussätete rakendamise võimalustest tuleb neil endil vajalikud privaatsussätted endale vastavalt kohaldada. Selline privaatsussätete individuaalne kohaldamine on vajalik, kuna küberkeskkonnas toimuvad võimalikud inimeste privaatsuse riived sõltuvad konkreetsest situatsioonist, info iseloomust, infosubjektide omavahelistest suhetest, infosaajate rollist ja info levitamise tingimustest. Samuti tuleb sotsiaalmeedia kasutajatel leppida tõsiasjaga, et sotsiaalmeedia keskkondades jagatav informatsioon ei pruugi internetiavarustest kaduda. Sinna sisestatud info on kergesti leitav, kopeeritav, viidatav ning laialdaselt kasutatav.[57] Andmete kogumise järgselt väljub edasine andmetöötlus isiku kontrolli alt nii andmetöötluse sisu ja vormi, kui ka andmete töötlejate isikute ringi osas.[58]

Elektroonilised andmed sisaldavad erinevaid isikuga seoseid luua võimaldavad andmeid, sealhulgas ka isikuandmeid isikuandmete kaitse seaduse tähenduses. Antud andmed kogumis võimaldavad nii otsingute, kui ka tehnika vahendite nagu nt arvuti ja mobiiltelefonide kasutamisega seonduvalt luua isiku osas analüüsi teostamist võimaldavaid andmekogumeid.

---

[56] B. Schneier, lk 1, 2.
[57] A. Siibak, S. Suder. Ülemus kui „suur vend“, lk 4. Arvutivõrgus: https://www.etis.ee/File/DownloadPublic/6fadddc4-cec1-45d5-b3a3-dcc7ccd85c6c?name=Fail_Siibak%26Suder.pdf&type=application%2Fpdf. (01.03.2016).
[58] M. Männiko, lk 111.

Kogutud andmed võimaldavad analüüside abil teostada infol põhinevaid ennetavaid otsustusi, näiteks on võimalik ennustusi teostada läbi personaliseeritud otsingumootorite andmete. Otsingute teostamise käigus analüüsitakse teenuse pakkuja poolt külastatavaid lehti ja külastuste ajalugu. Tulenevalt kasutajate otsingutest suunatakse isikud otsingumootorisse sisestatud otsingusõnade põhjal lehekülgedele, mida nad on eelnevalt külastatud ja mis on populaarsemad ning mis võiksid neile huvi pakkuda. Seega tekivad otsingumootorite kasutajaliidestes sisalduvate algoritmide ennustuste põhjal populaarsemate lehtede kogumid ning isikute grupid suunatakse esmajoones nende infot kasutama. Suurandmete põhjal kujundatakse otsustused üldjuhul kasutajapõhiselt, kuid otsingumootori süsteemi ei adopteerita ainult kasutajapõhiselt, vaid kasutajat suunatakse erinevatele lehekülgedele konkreetse korporatsiooni huvidest lähtuvalt. Samas ei garanteeri ennetavad otsustused, et saadud info pinnalt saab kindlalt väita, kuidas teatud indiviid või isikute grupp võiks käituda.[59]

## 1.2 Suurandmete analüüs ja selle võimalikud kasutegurid

### 1.2.1 Suurandmete analüüs ja teostatavad otsingud

Maailm on jõudnud arvutipõhisesse algoritmide ajastusse, kus suurte andmemahtude analüüsi kaudu tuvastatakse erinevate seoste struktuure.[60] Suurandmete analüüse teostatakse läbi andmete analüüsi ja hindamise, mis on olulised ennustusotsuste teostamiseks. Näiteks luuakse seosed juba olemasolevate andmete ning konkreetse isikuga seotud info vahel. Seejärel identifitseeritakse ja sobitatakse loodud arvutipõhise profiiliga ka võimalikke teisi isikuid.[61] Suurandmete analüüsimiseks kasutatakse algoritme, mis on muutunud järjest täpsemateks. Samas kui käsitletavad andmemahud on liiga suured, siis kaob ära keskne eesmärk ning analüüsid muutuvad vähem efektiivsemateks.[62]

Suurandmete ajastuga seonduvalt on muutunud info kogumise põhimõtted ka kriminaalmenetluse kontekstis. Varasemalt nn väikese mahuga informatsiooni ajastul liigutati andmed olemasoleva küsimuseni ehk menetlust alustati küsimusest või hüpoteesist ja üritati

[59] Kerr/Earle, lk 67.
[60] D. J. Steinbock. Data matching, data mining, and due process. Georgia Law Review, University of Toledo – College of Law, Volume 40, Fall 2005, No 1, lk 4.
[61] D. J. Steinbock, lk 4.
[62] M. Toivonen. Big Data Quality Challenges in the Context of Business Analytics. University of Helsinki: Department of Computer Science 2015, lk 8. Arvutivõrgus: http://hdl.handle.net/10138/156666 (04.02.2017).

olemasolevate andmete alusel leida vastuseid läbi inimese poolse analüüsi.[63] Nn väikese mahuga info ajastul olid info kogumise meetodid suunatud vertikaalsele lähenemisele, kus välja otsiti kogu info konkreetse isiku või tegevuse kohta.[64] Suurandmete ajastul liigutatakse olemasolev küsimus aga info juurde ehk alustatakse suurandmete analüüsiga ning vaadatakse, millised hüpoteesid selle põhjal nähtuvad ja püstituvad. Seda võimaldavad läbi viia suurandmete töötlemise vahendid nagu info otsing, teatud tunnuste alusel läbi viidav analüüs, andmebaasidest info kontroll, statistiline modelleerimine ja algoritmid ehk ennetav analüüs, kus kasutatakse ka superarvutite ning tehisintellekti abi.[65] Suurandmete ajastul on info kogumise meetodid suunatud horisontaalsele info kogumisele, kus digitaalne informatsioon kogutakse täies ulatuses ning salvestatakse olenemata sellest, kas isiku või tegevuse osas puudub informatsiooni vajadus või mitte.[66]

Suurandmete ajastul on olemasoleva info kogumi pinnalt analüüsi läbiviimisel saadud andmed erinevate toimingute alustamise aluseks ehk programmid töötavad ning koguvad informatsiooni selliselt, et nende põhjal oleks võimalik küsimusi formuleerida ja püstitada.[67] Selle asemel, et formuleerida tees, kes võib konkreetse infoga seotud olla, saab suurandmeid kasutades analüüsida ja koostada tulevikku suunatud ennustusi.

Laiemalt vaadatuna ignoreeritakse inimeste monitoorimisega läbi arvutuslike järelduste süütuse presumptsiooni alustalasid, mis võivad viia selleni, et teatud inimeste gruppe hakatakse potentsiaalsete kahtlusalustena pidevalt hindama. Selline eelpreventiivne tegevus on väga problemaatiline, kuna eeldab massiliselt andmete kogumist kogu elanikkonna osas ja tegevust õigustatakse üldjuhul võimalike kuritegude toimepanemise ennetamisega.[68] Näiteks on suurandmed võimaldanud neid kasutavatel USA valitsusasutustel intensiivistada kuritegude ennetamiseks ja avastamiseks vajalikke jälgimismeetodite kasutamist, mida võib vaadelda kui omavahel seotud informatsiooni, tehnoloogia ja kommunikatsiooni konfiguratsiooni. Antud tulemuslikkus saavutatakse läbi uute tehnoloogiate rakendamise ja selle kaudu teostatava ennetava analüüsi, mis on kaasa toonud tajutava kvalitatiivse muutuse. Edasi on arendatud

[63] M. Hu. Small Data Surveillance v. Big Data Cybersurveillance. Pepperdine Law Review, Vol. 42, 2014, lk 802.
[64] M. Hu 2014, lk 832.
[65] M. Hu 2014, lk 802.
[66] M. Hu 2014, lk 832.
[67] M. Hu 2014, lk 803.
[68] M. Hildebrandt. Smart Tehnologies and the End(s) of Law: Novel Entanglements of Law and Technology. USA: Edward Elgar Publishing Inc., 2015, lk 99.

võimekust tõhustada suurandmete (sealhulgas metaandmete) töötlemist laiendades ja ühendades vajalikud andmekogud ning analüüsivahendeid.

Metaandmete ulatuslikust kasutusest annavad ülevaate järgnevad näited:

- Läbi NSA mobiiltelefonikõnede metaandmete kasutuse jälgimisprogrammi PRISM[69] on loodud otseühendus selliste suurfirmade nagu *Apple, Facebook, Google, Microsoft, Skype, Yahoo, YouTube* serverites olevate andmetega või teostatakse läbi nende internetiühenduse jälgimist. Samuti toimub läbi programmi nii küpsiste kui ka logide informatsiooni ja erinevate seadmete kasutamisega kaasneva info analüüs, mille aluseks võetakse kasutaja asukoht ning sotsiaalmeedias seostatud andmed. Sellise info töötlust võimaldab tarkvara, mis algoritmide ja kasutajate antud kodeeringu kaudu võimaldab seda süstemaatiliselt analüüsida ning muuta info operatiivselt kasutatavaks.[70]
- Kanada lennujaamades tuvastati läbi *WiFi* süsteemi ühenduste jälgimise *WiFi*-t kasutavate inimeste igapäevased seadmete geograafilised kasutuskohad. Tuvastamiseks kasutati identifitseeritavaid andmeid ning seostati need konkreetsete IP-aadressidega. Sellisel meetodil kogutud andmete alusel on võimalik alarmeerida õiguskaitseorganeid, kui konkreetne kahtlusalune siseneb mingisse asukohta (nt hotelli) või kontrollida tagantjärgi isiku viibimist mingis konkreetses kohas.[71]

Läbi teatud käitumismudelite korrelatsiooni võimaldavad suurandmed teha ennustusi konkreetsete isikute võimaliku kriminaalse käitumise osas.[72] Autori arvates võimaldab eeltoodud info menetluslikult ennetuslike meetmete rakendamist tuvastatud isikute suhtes. Sellega kaasneb aga oht, et otsuste vastuvõtmisel menetlustoimingute läbiviimiseks toetutakse vaid suurandmetest saadud korrelatsioonide analüüsile ning vähem tegelike võimalike põhjuste kontrollimisele, miks sellised seosed võivad esineda. See võib kaasa tuua ennatlikud otsused, mis põhinevad ekslikel seostel ja andmetest ajendatud võimalikel kujutelmadel.

[69] PRISM – Planning Tool for Resource Integration, Synchronization and Management ehk planeerimise, ressursi integreerimise, sünkroniseerimise ja juhtimise haldamise tööriist.
[70] D. Lyon, lk 1.
[71] D. Lyon, lk 3.
[72] B. Carrett. Big Data Is Changing Your World … More than You Know. United States, California: Atlantic Council, Columbia University Press, August 2013, lk 1. Arvutivõrgus: http://www.ciaonet.org.ezproxy.members.marshallcenter.org/record/31754?search=1 (23.08.2016).

### 1.2.2 Suurandmete analüüsi kasutegurid

Suurandmete analüüsist on võimalik saada ühiskondlikku kasu, mille kaasabil on võimalik luua paremaid tooteid ja teenuseid tarbijatele ning ärilisi eeliseid ettevõtetele.[73] See loob hulgaliselt võimalusi nii maailma majanduse mõistes, kui ka riikliku turvalisuse tõhustamise kontekstis. Suurandmeid saab kasutada väga erinevates valdkondades – krediidiriskide analüüsist ja meditsiinivaldkonna teadusuuringutest kuni linnaplaneerimiseni välja.[74] USA-s näiteks kasutatakse suurandmeid järgnevates eluvaldkondades: avalik ja erasektor, kaitsetööstus, meditsiin, teadustöö ja sotsiaalmeedia, ökosüsteemide uuringud, astronoomia ja füüsika, maa-, loodus- ja poolaarteadus ning energiasektor.[75]

Suurandmetest saadava võimaliku kasuga võib kaasneda aga mure eraelu puutumatuse ja andmekaitse osas.[76] Suurandmed võimaldavad inimese elu analüüsida nii mikro-, kui ka makrotasandil ehk nii indiviidi kui ka riigi tasandil. Sellega seonduvalt võimaldavad andmed luua uusi võimalusi valitsustele, eraettevõtetele, erinevatele organisatsioonidele ja ka teistele indiviididele. Lisaks saab suurandmeid kasutada muuhulgas kriitiliste globaalsete probleemide lahendamiseks ning uute teaduslike läbimurrete saavutamiseks nii inimeste ravis, kui ka keskkonnakaitses. Kogutud andmed võimaldavad reaalajas laiapindset informatsiooni analüüsi, millega saavutatakse suurem ressursside kasutamise efektiivsus.[77]

Suurandmete analüüsi kasutegur erasektoris väljendub suurandmete analüütilises väärtuses, mis võimaldab pakkuda uusi tooteid. Tulenevalt suurandmete haldamise kulude odavnemisest on suurandmete analüütikutel maailmas tekkinud võimalus analüüsida ja kontrollida andmeid, mis olid neile enne, tulenevalt nende kõrgest maksumusest, kättesaamatud. Andmed võimaldavad analüüsida eakaaslaste mõjusid klientide hulgas, mida teostatakse läbi ostjate käitumise analüüsi tuvastades seoseid tehingute ning sotsiaalsete ja geograafiliste andmete kaudu. Heaks suurandmete töötlemise ärilise edu näiteks on viimase kümnendi veebipõhiste *start up*-ide edu.[78]

---

[73] Suurandmed ja privaatsus, lk 11.
[74] J. Polonetsky, O. Tene. Privacy and Big Data: Making ends meet. 66 Stan. L. Rev. 25. September 3, 2013, lk 25.
[75] NIST Big Data Interoperability Framework: Volume 3, Use Cases and General Requirements. National Institute of Standards and Technology U.S Department of Commerce, lk 6-42. Arvutivõrgus: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1500-3.pdf (15.03.2017).
[76] Polonetsky/Tene, lk 25.
[77] B. Carrett, lk 1.
[78] E. Dumbill 2012, lk 3, 4.

Suurandmete analüüs on teadlastel võimaldanud luua uusi teaduslikke hüpoteese erinevatest allikatest pärit info kaudu. Teatud juhtudel on infokogum eelnevalt juba võrdlemiseks olemas. Näiteks on kogutud kliimaandmete põhjal võimalik teha järeldusi, et keskmine troopiliste tsüklonite tugevus on viimase paarikümne aastaga vähenenud. Samas ookeanitemperatuuri mõõteandmed näitavad aga ookeanivee temperatuuri tõusu. Eeltoodust tulenevalt sündis uus korrelatsiooni meetod, mis võimaldab määrata, arvestades ookeanivee temperatuuri, troopilise tormi tugevust. See 21. sajandi alguse klimatoloogia suund on uus ja ei pruugi küll kuhugi jõuda, kuid see kinnitab, et erinevatest allikatest saadud andmed, näiteks tormide ja ookeanivee temperatuuri kohta, võivad viia uute teaduslike paradigmadeni.[79]

Lisaks eeltoodule on suurandmete analüüsiga seotud areng muutnud üha lihtsamaks ka teabe kogumise konkreetsete isikute kohta. Kuna kogutu kasutamises nähakse suurepärast võimalust kaitsta paremini nii riigi sise- kui ka välisjulgeolekut saab seda sarnaselt eeltooduga käsitleda ka kui analüüsi võimalikku kasutegurit. Nimelt vajavad õiguskaitseasutused kuritegude ennetamiseks ja lahendamiseks teavet, mille kogumise tõhusus sõltub ühelt poolt tehnoloogia arengust ja teiselt poolt seadusandja antud volitustest kasutada nii eraõiguslikest allikatest, kui ka õiguskaitseasutuste poolt kogutavat infot.[80] Näiteks on Edward Snowden-i materjalide avalikustamisega tuntust kogunud infoportaal *The Intercept* avalikustanud nimekirja kümnetest USA erinevate teenistuste kasutatavatest seadmetest, mis võimaldavad koguda infot ja jälgida kodanike mobiilsidevahendeid. Need hõlmavad endas nii inimese endaga kaasaskantavaid, kui lennukitel kasutatavaid vahendeid.[81]

Samuti saab suurandmete põhjal analüüsi teostamist ilmestada Rootsi riigikaitse raadioasutus Försvarets Radioanstalt (edaspidi „FRA“) näitel, kus FRA jälgib suurt osa Vene Föderatsiooni (edaspidi „VF“) kaablipõhisest suhtlusest. FRA-le on antud laialdased volitused mööda kiudoptilisi kaableid kogu Rootsi saabuva ja sealt väljuva suhtluse pealtkuulamiseks (sh e-kirjad, tekstisõnumid ja telefonikõned). Suur osa VF-i suhtlusest toimub läbi Rootsi, sest VF-i ühendab organisatsiooni *TeleGeography* andmetel muu maailmaga vaid kuus merealust kiudoptilist kaablit ning peamised neist kulgevad Läänemere põhjas. *WikiLeaks*-is avaldatud

[79] J. J. Berman, lk 205.
[80] U. Lõhmus. Põhiõigused kriminaalmenetluses. 2. tr. Tallinn: Juura 2014, lk 338.
[81] The Secret Surveillance Catalogue. The Intercept. Arvutivõrgus: https://theintercept.com/surveillance-catalogue/ (22.02.2016).

USA Stockholmi saatkonna diplomaatilise telegrammi kohaselt liigub 80 protsenti VF-i kaablipõhisest välissuhtlusest läbi Rootsi. Antud andmeid jagab FRA NSA-ga.[82]

[82] L. Laugen. Rootsi on kübersõja kuningas, kes jälgib suurt osa Venemaa suhtlusest Läänemere kaabli kaudu. Delfi, 18. jaanuar 2017. Arvutivõrgus: http://www.delfi.ee/news/paevauudised/valismaa/usa-valjaanne-rootsi-on-kubersoja-kuningas-kes-jalgib-suurt-osa-venemaa-suhtlusest-laanemere-kaabli-kaudu?id=76942876 (20.01.2017).

# 2. SUURANDMETE KASUTUSALAD JA ISIKUÕIGUSTE KAITSE

Suurandmed moodustavad tänapäeva maailmas olulise osa pea igast eluvaldkonnast. Järjest enam kasutatakse neid otsuste vastuvõtmiste kujundamisel nii erasektoris, valitsuste tasandil kui ka indiviidide hulgas. Suurandmed võivad eksisteerida ainult digitaalselt, kuid need teenivad siiski ka materiaalse maailma huve.[83]Elektrooniline jälg, mille tekitavad elektroonilise kommunikatsiooni liiklus- ja asukohaandmed, võimaldab teha järeldusi isiku perekondlike, poliitiliste, kutsealaste, religioossete ja seksuaalsete seoste ning suhete kohta.[84]

Erinevat informatsiooni transformeeritakse praktiliselt alati digitaalsesse formaati ning seda olenemata sellest, millises formaadis see eelnevalt eksisteeris. Traditsiooniline informatsioon on olnud väga tugevalt subjektipõhine, kuid kaasaegne informatsioon moodustub läbi digitaalsete vahendite kaudu teostatava analüüsi. Tekkiv informatsiooni tõlgendus võib olla erinev originaalsest algformaadist ning seetõttu tuleb arvestada olemasoleva info konteksti ja hinnata kaasusepõhiselt selle kvaliteeti. Tulenevalt traditsioonilisest informatsiooni tähendusest sisaldab moderne informatsiooni definitsioon seega endas erinevaid eelpool nimetatud faktoreid, mida saab konkreetse kaasuse kontekstis klassifitseerida, arvestades nende väärtust ja õiguslikku tähendust. Õigus ise ei taga võrdselt kaitset kõikidele informatsiooni liikidele, vaid suunab informatsiooni käitlemist väärtuspõhise tulemi saavutamisele pärssides selle käitlemist ühiskonnale negatiivsel kujul.[85]

## 2.1 Suurandmete kasutusalad Ameerika Ühendriikides

Peale 11. septembril 2001. aastal toimunud terrorirünnakuid USA-s võttis USA Kongress vastu seaduse „Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001“ (edaspidi „USA PATRIOT ACT*“),* mis võimaldab riigi valitsusel koguda suuremas mahus erinevatest allikatest pärinevat

[83] B. Carrett, lk 1.
[84] U. Lõhmus. Veel kord õigusest sõnumite saladusele ehk kuidas 20. sajandi tehnoloogia mõjutab põhiseaduse tõlgendusi. Juridica 2016/III, lk 182.
[85] X. Li, lk 69.

informatsiooni. [86] USA PATRIOT ACT andis näiteks NSA-le ja USA Föderaalsele Juurdlusbüroole (edaspidi „FBI“) suuremad õigused jälitustoimingute ning menetluste läbiviimisel.[87] USA PATRIOT ACT vastuvõtmisega seonduvalt täiendati ka muid andmete kogumist võimaldavaid õigusakte nagu *The Foreign Intelligence Act* (edaspidi "FISA"), *The Electronic Communications Privacy Act* (ECPA) ja *The National Security Letter* (NSL). Tehtud täienduste eesmärgiks oli tagada efektiivsemad võimalused tuvastamaks indiviidide kommunikatsiooni mustreid, pealt kuulata ja -vaadata e-kirju, telefonivestlusi ning teostada läbiotsimisi.[88] USA konstitutsioonis on sarnaselt Euroopaga kehtestatud nõuded,[89] et tõendite kogumiseks on vaja tuvastada põhjendatud kahtluse olemasolu ning kohtult on vaja saada luba võimalikke isikuõigusi piiravate toimingute läbiviimiseks.[90]

2017. aasta märtsis esitas USA Kongress president D. Trumpile eelnõu muudatused, mille kohaselt tekib telekommunikatsiooni ettevõttevõtetel nagu näiteks Verizon, AT&T ja Comcast võimalus monitoorida Interneti kasutajate käitumisharjumusi ilma nende nõusolekuta. Samuti kasutada nende isiklikku ja majandustegevusega seonduvat informatsiooni müües neile kasutajapõhiseid reklaame. Sellega seonduvalt muutuvad ettevõtted konkurentideks 83 miljardi USA dollari suuruse *online* turu mõistes sellistele suurfirmadele nagu *Google* ja *Facebook*. Ettevõtted saavad müüa kasutajate informatsiooni edasi reklaami- ja finantsettevõtetele ning teistele, kes tegelevad personaalsete andmete kogumisega ning kes saavad ka antud informatsiooni kasutada ilma kasutajate nõusolekuta.[91]

2001. aastal toimunud terrorirünnakute järel on USA seadusandja võimaldanud valitusasutustel suures mahus andmete kogumist ning seda põhjendades vajadusega kaitsta riigi julgeolekut. Näiteks on FISA § 702 julgeolekumeetmete vajadust põhjendatud kui efektiivset turvalisuse

[86] E.C. Liu, C. Doyle. Goverment Collection of Privarte Information: Background and Issues Related to the USA PATRIOT Act Reauthorization in Brief. Congressional Research Service, May 19, 2015, lk 1. Arvutivõrgus: https://fas.org/sgp/crs/intel/R44042.pdf (22.03.2017).
[87] C. W. Michaels. No Greater Threat: America After September 11 and the Rise of a National Security State. New York: Algora Publishing 2002, lk 40.
[88] Liu/Doyle, lk 1.
[89] U.S. Const. Amend. IV: Arvutivõrgus: https://www.law.cornell.edu/wex/fourth_amendment (22.03.2017).
[90] Liu/Doyle, lk 1.
[91] B. Fung. The House just voted to wipe away the FCC´s landmark Internet privacy protections. The Washington Post, March 28, 2017. Arvutivõrgus: https://www.washingtonpost.com/news/the-switch/wp/2017/03/28/the-house-just-voted-to-wipe-out-the-fccs-landmark-internet-privacy-protections/?utm_term=.0ed450ff7031 (30.03.2017).

tagamise meedet, millega laiemalt vaadatuna on tagatud ka iga isiku õiguste kaitse.[92] NSA andmete kogumistega kaasnenud skandaal, mis USA-s 2013. aasta juulis tõstatus tõi üldsuseni arusaama, et riigis on iga kasutaja tegevus internetis jälgitav ja salvestuv. Samuti sai selgeks, et NSA poolt teostatud andmete kogumist FISA alusel, mis on suunatud välismaalastega seonduva informatsiooni kogumisele, on kasutanud ka USA enda kodanike osas informatsiooni kogumiseks. Nimelt on NSA FISA lõike 702 alusel 2011. aastast alates igal aastal kogunud umbes 250 miljonit internetikommunikatsiooni kannet[93] ning seda on teostatud ka USA kodanike osas.[94] FISA lõike 215 alusel on NSA-l olnud õigus koguda[95] sideandmete metaandmeid, mis sisaldavad nii helistaja kui ka vastuvõtja telefoni numbreid, kõne toimumise aega ja kuupäeva. Samas ei sisalda kogutud andmed teostatud kõnede sisu.[96]

NSA omab ja kasutab ka programme, mis salvestasid üheksa suurema USA internetiteenuse pakkuja kasutajate tegevusi, hõlmates pea kõike, mida tüüpiline Interneti kasutaja teeb. Koguti tekstsõnumeid, häälsõnumeid, videovestlusi, fotosid, failivahetust, sotsiaalmeedias toimuvat suhtlust, interneti sirvimise ajalugu ja internetis teostatud otsingud.[97] Programmid, mis kasutavad kogu olemasolevate andmete kogumise metoodikat on väljatoodud lisas 1.[98] Lisaks eelpool nimetatud andmete kogumise programmidele kasutab NSA erinevaid rünnakuprogramme, mis on välja toodud lisas 2.[99]

Loomaks ja tuvastamaks seoseid ning ennetamaks ja lahendamaks kuritegusid kasutavad erinevad USA politseiüksused suurandmeid aktiivselt juba täna. Näiteks kasutab FBI suurandmete ressursse läbi erinevate andmebaaside, sh elektrooniliste sõrmejälgede ja DNA[100] profiilide andmebaaside. Need on andmebaasid, kus on talletatud andmed isikuga seotud

[92] J. Magness. FISA Section 702: Is warrantless surveillance national security or a hitt o privacy? McClatchy DC BUREAU, March 1, 2017. Arvutivõrgus: http://www.mcclatchydc.com/news/politics-government/congress/article135841918.html (22.03.2017).
[93] L. K. Donohue. Section 702 and the Collection of International Telephone and Internet Content. Harvard Journal of Law & Public Policy, Vol 38, Winter 2015, Issue 1, lk 120.
[94] G. Greenwald. Rand Paul Is Right: NSA Routinely Monitors Americans' Communications Without Warrants. The Intercept, March 13, 2017. Arvutivõrgus: https://theintercept.com/2017/03/13/rand-paul-is-right-nsa-routinely-monitors-americans-communications-without-warrants/ (22.03.2017).
[95] Verizon forced to hand over telephone data – full court ruling. The Guardian, June 6, 2013. Arvutivõrgus: https://www.theguardian.com/world/interactive/2013/jun/06/verizon-telephone-data-court-order (23.03.2017).
[96] Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies. Liberty and Security in a Changing World. December 12, 2013, lk 17.
[97] J. A. T Fairfieldt, E. Luna. Digital Innocence. Cornell Law Review,Vol. 99, Issue 5, lk 982.
[98] M. Hu. Taxonomy of the Snowden Disclosures. Washington and Lee Law Review, Vol. 72, Issue 4, September 1, 2015, lk 1693-1697.
[99] M. Hu 2015, lk 1698-1699.
[100] DNA – deoxyribonucleic acid ehk desoksüribonukleiinhape on enamikus elusorganismides pärilikku informatsiooni säilitav aine.

lennureiside, vahistamiste, eelnevate karistuste, haridustee, isiku omandis oleva kinnisvara, sugulussuhte, krediitkaardi kasutamise, *Facebook* suhtluse, elektrooniliste kirjade ja muu infoga, mida on võimalik isikuga seostada kohta.[101] Teise näitena võib välja tuua juhtumi, kus 2014. aastal saadeti Chicago Politseiosakonna politseiametnikud teostama koduvisiite isikute juurde, kelle valik oli genereeritud potentsiaalsete vägivallakuritegude toimepanijate nimekirja alusel. Külastatavate isikute suhtes ei olnud eelnevalt ühtegi menetlust alustatud, tegemist oli võimaliku esineva kahtluse kontrollimisega.[102]

Suurandmete eelsel kasutusperioodil kaasnes peaaegu alati võimaliku kahtluse olemasoluga konkreetsete asukohtade jälgimine, tuvastamaks võimalikke kuritegude toimepanemisega seotud isikuid. Tuues eelnevas lõigus väljatoodud näite tänapäevasesse suurandmete kasutamise võimaluste konteksti, oleks läbi võimaliku infosüsteemi politseil juurdepääs kahtlustatavate andmetele. Samuti eelnevalt kogutud infole ning kolmandate osapoolte infole, mis annab võimaluse teostada analüüse, milles saab kombineeritult kasutada nii biomeetrilisi andmeid kui ka näotuvastus süsteemi. Selle kaudu on politseil võimalik patrullautosse paigaldatud kaamera ja vastava tarkvara abil skaneerida tänaval liikuvaid inimesi ning tuvastada juba varasemalt teadaolevaid varguste toimepanemisega seotud isikuid. Nii on võimalik siduda isikuga seonduvad eelnevad vahistamised, karistusandmed ning muu informatsioon ja ka võimalikud kaasosalised. Tuvastades isiku, analüüsitakse tema liikumist GPS andmete alusel ning tema kasutuses oleva sõiduki numbrimärgi jälgimisandmete kaudu. Arendades tarkvara ning lisades sinna veel isiku sotsiaalmeedia postitused või muu suhtluse, kus võib olla viiteid, et isik võib planeerida järjekordset varguse toimepanemist, on ennetavate meetmetega võimalik saavutada tulem, kus läbi andmete analüüsi on võimalik esile tuua ja välja pakkuda võimalikud kahtlusalused.[103]

Arvestades eeltoodut tähendavad suurandmed julgeoleku- ja politseiasutuste töös põhiliselt võimekust analüüsida suurt mahtu erinevatest allikatest pärinevat infot. Analüüsi tulemit kasutatakse otsuste kujundamiseks ja vastuvõtmiseks luues seoseid avastamaks kuritegevuse

[101] J. J. Berman, lk 202.
[102] Civil Rights, Big Data and Our Algorithmic Future: A September 2014 report on social justice and technology. 2014. Arvutivõrgus: https://bigdata.fairness.io/predictive-policing/ (22.02.2016).
[103] A. G. Ferguson. Big Data and predictive reasonable suspicion. University of Pennsylvania Law Review. Vol. 163, January 2015, No 2, lk 330, 331.

mustreid ning selle kaudu on võimalik ennetada võimalikke kuritegude toimepanemist. Selline areng muudab info analüütiku keskseks kriminaalmenetlust kujundavaks osaks.[104]

Suurandmeid on seega võimalik kasutada kriminaalpreventsioonis, kus erinevate analüütiliste vahenditega, mida õiguskaitseasutused kasutavad, on võimalik identifitseerida ja tuvastada võimalikke tulevikus asetleidvaid kuritegusid. Suurandmete põhine analüüs ja kuritegevuse uurimise analüütika on head kriminaalpreventsiooni ja ennetava uurimise läbiviimise vahendid. Näiteks on Los Angeles-i Politseijaoskond suurandmete põhist analüüsi kasutanud juba alates 2010. aastast. Kasutamise käigus on nad avastanud, et kuriteo sündmuste esinemisel on sarnane seos maavärina ja selle järeltõugetega. Andmete pinnalt on nimelt lihtsam ennustada, kus maavärinaga seonduv järeltõuge võib aset leida, sama on kasutatav ka kuritegude ennetamise kontekstis. Los Angeles-i Politseijaoskond, kasutades sama matemaatilist mudelit kriminaalkuritegude andmete puhul, on kasutusele võtnud algoritmi, mis suudab kuritegude mustrit arvestades ennetada kuritegude võimalikke toimumiskohti. Selliseks tarkvaralahenduseks on *PredPol*[105]. Selle abil suudetakse ennustada, kus järgmine kuritegu võib aset leida ning seda täpsusega kuni 150 $m^2$. Tarkvaralahenduse kasutuselevõtuga on suudetud piirkonnas vähendada 33% röövimisi ja 21% vägivallaga seotud kuritegusid. Sarnaste tarkvara lahendustena on USA-s veel laialdaselt kasutusel ka *IBM® i2 COPLINK*[106] tarkvara. Eeltooduga suurandmete põhised kriminaalanalüüsi meetodid aga ei piirdu. USA õiguskaitseasutustel on võimalik analüüsida kuriteomustreid ning läbi kogutava informatsiooni identifitseerida õigusrikkumistega seonduvaid isikuid. Näiteks sissemurdmiste toimumisel ja sündmuskoha fikseerimistel on nende andmete pinnalt, konkreetse kuriteo sooritaja meetodeid analüüsides nagu sisenemisviis, aeg, korduvus, kinnisvaratüüp jne ja seostades neid üleriikliku sissemurdmiste statistikaga, võimalik tuvastada seosed ning järeldada, kus sarnane kuritegu võib taas aset leida.[107]

Õiguskaitseasutused USA-s on võtnud andemete kogumisel aluseks põhimõtte, et kokku tuleb koguda kogu olemasolev info ehk andmete kogumise fookus on liikunud tagajärgedele

[104] D. Wyllie. How „Big Data“ is helping law enforcement. August 20, 2013. Arvutivõrgus: https://www.policeone.com/police-products/software/Data-Information-Sharing-Software/articles/6396543-How-Big-Data-is-helping-law-enforcement/ (22.02.2016).
[105] Tarkvaralahendus PredPol. Arvutivõrgus: http://www.predpol.com/.
[106] Tarkvaralahendus Coplink. Arvutivõrgus: http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?infotype=AN&subtype=CA&htmlfid=897/ENUS212-112.
[107] A. Kwapien. How Big Data Helps To Fight Crime? Datapine, May 10, 2016. Arvutivõrgus: http://www.datapine.com/blog/big-data-helps-to-fight-crime/ (19.03.2017).

keskendunud infokogumisest ennetavale info kogumisele, kus väga olulist rolli mängib andmete analüüs. Mingi konkreetse juhtunud sündmuse osas informatsiooni kogumine võib olla väga limiteeritud ja fokusseeritud vaid konkreetsele kahtlusalusele või sündmustele, mis üldjuhul toob kaasa jälgimise vajaduse. Ennetav infokogumine on aga suunatud sellele, et tuvastada ja identifitseerida isikuid juba siis, kui nad on muutunud kahtlustäratavaks. Eesmärgiks on tuvastada võimalikke tulevikus asetleidvaid sündmusi enne nende toimumist.[108] Erinevalt USA-st ei toimu EV-s kogu olemasoleva info ehk andmete automaatset kogumist. Üldjuhul viiakse EV-s info kogumist läbi konkreetse isikuga seonduvalt, võimaliku kuriteo kahtluse olemasolu kontrollimiseks. Täpsemalt on teemat kajastatud järgnevas punktis 2.2.

Suurandmete kogumise ajastul on nn mosaiikteooria transformeerunud infokildude ühendamise teooriaks, kus igaüks, kes kommunikeerib võib olla sihtmärgiks. Teooria kohaselt selgub iga informatsiooni osakese hind ja olulisus alles siis, kui selle saab ühendada muu infoga, mis võib saabuda mingil ajahetkel tulevikus. Seoses sellega, et reaalajas ei pruugi võimalik olla ühendada kõiki olemasolevaid infokilde, kuna vajalikud vasted puuduvad, siis üritatakse talletada kogu olemasolev info ja seda määramata ajaks. Seda selleks, et tulevikus oleks võimalik vajalikud infokillud ühendada. Protsessi, mille käigus need infokillud ühendatakse mustriteks ning mille alusel pakutakse välja võimalikke isikuid, kes võivad olla seotud terroristlike aktide ettevalmistamisega, nimetatakse info kaevandamiseks ehk otsimiseks. Pärast info otsimist analüüsitakse juba olemasolevaid andmeid, et selekteerida välja need osad, mis on seotud mingi kindla käitumisega. Edasi otsitakse sobivaid käitumismustreid teistest andmete kogumitest, et ennetada võimalikke juhtumeid, kus sarnane käitumine võib tõenäoliselt esineda.[109]

Suurandmete kasutusala huvitavaks näiteks on ka isikute käitumise nn muster-analüüs. NSA programm "kaasreisija" kasutab selleks matemaatilisi lahendusi kaardistamaks telefonikasutajate suhtlust ja võrdleb neid teiste olemasolevate andmetega leidmaks olulisi seoseid ja korrelatsioone. Programmi eesmärgiks on otsida välismaalt saabuvate ning valitsusasutustele huvipakkuvate isikute kontaktide seoseid kodumaiste ehk kohalike kasutajatega.[110]

[108] M. Hu 2014, lk 801.
[109] M. Hu 2014, lk 834.
[110] D. Lyon, lk 3.

Eelpool kirjeldatud tegevust saab kriminaalõiguslikus kontekstis vaadata kui ennetavat preventsiooni, kus julgeoleku tagamise eesmärgil läbi viidava jälitustegevuse käigus, mis on suunatud teatud isikute grupile, kontrollitakse võimalikke kahtlusaluseid. Tegevust vaadeldakse kui legitiimset eeldust, mis aitab ennetada kuritegude toimepanemist ning olla kuritegevuse vastases võitluses kurjategijatest samm eespool. Senikaua, kuni isikule konkreetset kahtlustust ei esitata ei riku, juriidiliselt kitsalt võetuna, tegevus ka süütuse presumptsiooni. Laiemalt vaadatuna ja just sellest aspektist, kuidas tavainimesed sellist andmete alusel otsuste vastuvõtmist intuitiivselt mõistavad, on tunnetuslikus mõttes tegemist rikkumisega. Siinjuures võib vastu argumenteerida, et suurandmete kontekstis ei ole selline andmete analüüs rikkumine, kuna kogumis ei välistata kedagi ning kontroll toimub kõigi mõistes ühetaoliselt. Samas on probleemiks see, et otsuseid võidakse vastu võtta tuginedes vaid masina poolt töödeldud andmete analüüsi tulemile.[111]

USA Ülemkohtu otsuses *Daubert v. Merrell Dow Pharmaceuticals, Inc* rõhutas kohus, et kohtunikud peavad kindlaks tegema kohtule esitatud andmete põhise tõendi asjakohasuse ja olulisuse konkreetse asja kontekstis. Kohus peab läbi valdkonna eksperdi kontrollima, et esitatud andmete kogumi puhul on kasutatud teaduspõhist metoodikat, mis peab olema kontrollitav ning ka seda, et valitud meetodi kasutamine on piisav ehk see on sobiv ja kasutatav muude esitatud faktide kontekstis.[112] Seega USA-s peab kohus asitõendite uurimisel veenduma, kas nende fikseerimisel kasutatud teaduslik meetod oleks usaldusväärne. Kohus peab kontrollima, kas esitatud tõendis on kasutatud teaduslikku meetodit ehk metodoloogiat, mis on teaduslikult asjakohane. Samuti peab kohus kontrollima, kas meetod on üldiselt aktsepteeritav, kas kasutatud meetodit või teaduslikku põhjendust saab konkreetses kaasuses kasutada ning kas see on seotud konkreetse kaasuse asjaolude ja faktidega. Eriti tõhus peaks kontroll olema siis, kui tõendamisel on meetodina kasutatud suurandmete analüüsi vahendeid.[113] Sarnast metoodikat tõendite hindamisel võiks kohus kasutada ka EV-s, veendudes tõendite esitamisel nende kogumise metoodika ning esitatud kujul tõlgendamise õigsuses.

[111] M. Hildebrandt 2015, lk 97.
[112] J. J. Berman, lk 185.
[113] M. Hu 2014, lk 786, 787.

## 2.2 Suurandmete kasutusalad Eesti Vabariigi ja Euroopa Liidu kontekstis

Tänapäeval on suurandmed aina enam leidmas kasutust ka avalikus sektoris. Peamiselt kasutavad suurandmeid õiguskaitseasutused, kes saavad olemasoleva info põhjal läbi viia indiviidide põhiseid analüüse ja vajadusel näiteks kokku panna potentsiaalse terroristi profiili.[114] Sellega seonduvalt on riikide valitsused ja valitsusasutused üha enam investeerimas info kogumisse, talletamisse ning analüüsi. Põhjenduseks tuuakse enamjaolt kuritegevuse ja terrorismi vastane võitlus. Euroopa kontekstis on näiteks Inglismaa investeerinud märkimisväärselt videotehnoloogiasse tänavakaamerate paigaldamise näol. Ainuüksi Londonis on neid kokku 1,85 miljonit, mis teeb ühe kaamera 32 inimese kohta. Kaamerate salvestiste analüüsimiseks kasutatakse nn tehisintellekt tehnoloogiat, mille ülesandeks on hõlbustada ja ennetada teatud liiki käitumise põhjal kuritegude toimepanemise avastamist.[115]

Oluliseks infoallikaks, millele valitsusasutused, eriti terrorismi vastu võitlevad üksused, eriliselt suurt tähelepanu pööravad on erinevad suhtluskeskkonnad ning seal toimuv suhtlus mitmete gruppide ja kogukondade vahel. Viimast põhjendatakse radikaliseerumise vastase ennetustegevusega, kuna ekstremistlike vaadetega grupid, nagu näiteks radikaalse islami toetajad, valge rassi ülemvõimu toetajad või ka radikaalsete vaadetega loomaaktivistide grupid, on veebikeskkondades väga aktiivsed. Läbi suhtluskeskkondade otsitakse endale mõttekaaslasi, täiendavaid toetajaid ning uusi liikmeid. Internet on muutnud selliste gruppide liikmete omavahelise suhtluse lihtsamaks ja kiiremaks ning kauged vahemaad või riigipiirid ei ole suhtluses ja info edastamises enam takistuseks.[116]

Tagamaks tasakaalu riikliku julgeoleku ja kuritegude ennetamise õiguslikus raamistikus on vajalik, et inimõiguste riiveid kasutataks proportsionaalselt võimaliku olemasoleva ohu suhtes. Süütuse presumptsiooni tagamiseks peab kehtiv õiguslik raamistik vastama tingimusele, kus kogutud informatsiooni ja andmeid kasutatakse kuritegude avastamiseks vaid õiguslikult ettenähtud korra kohaselt ja seda võimalikult lühikese ajaperioodi jooksul ning ainult võimaliku kuriteoga seotud tuvastatud isikute suhtes.[117]

---

[114] Craig/Ludloff, lk 13,14.
[115] Craig/Ludloff, lk 19.
[116] I. Brown. Communications Data Retention in an Evolving Internet. International Journal of Law and Information Technology, Vol. 19, Oxford University Press 2010, No 2, lk 98.
[117] S. Mcgarvey. The 2006 EC Data Retention Directive: A Systematic Failure. Hibernian Law Journal, Vol. 10, 2011, lk. 166. Arvutivõrgus:

Eesti ühiskonda võib nimetada infoühiskonnaks[118], kus on laialdaselt levinud arvutite massiline kasutamine. Statistikaameti andmetel oli 2012. aasta alguses EV-s arvuti- ja internetikasutajaks kaheksa tööealist inimest kümnest, kodus omab arvutit ja internetiühendust 75% leibkondadest, sealjuures on arvuti ja internet olemas üle 90% lastega peredest. Kui EL-i keskmine arvuti- ja internetikasutajate määr on 73%, siis Eesti määr kaheksa tööealise inimesega kümnest on 78%. Laialdase arvutikasutamisega kaasneb võimalus, et internetikasutuse käigus loodavaid andmeid kasutatakse konkreetse isiku suhtes tõendite kujundamisel ka kriminaalmenetluses. Mõistetavalt tähendab see riigipoolset isikute erasfääri sekkumist, mille intensiivseim vorm on jälitustegevus.

Demokraatlikus ühiskonnas võib teostatav jälgimine olla vajalik, kuid kontrollida tuleb, kes ja/või mis otstarbel seda teostab ning kuidas seda läbi viiakse.[119] Kodanike varjatud jälgimist võib läbi viia kui see on ülekaalukalt vajalik demokraatlike institutsioonide kaitseks ning kui seda teostatakse hoolika kaalutlusõiguse alusel ehk *ultima ratio* põhimõttel.[120] Nimelt on jälitustoimingutega kogutud tõenditele on kehtestatud rangemad reeglid, kui teistele kriminaalmenetluse käigus kogutavatele tõenditele.

Õigusselguse tagamise eesmärgil on EV seadusandja pidanud õigeks avada jälitustegevuse olemus konkreetsete jälitustoimingute regulatsiooni abil kriminaalmenetluse seadustikus[121] (edaspidi „KrMS“). KrMS § 126[1] lg 1 kohaselt on jälitustoiming isikuandmete töötlemine seaduses sätestatud ülesande täitmiseks, eesmärgiga varjata andmete töötlemist seaduses sätestatud ülesande täitmiseks, eesmärgiga varjata andmete töötlemise fakti ja sisu andmesubjekti eest. Jälitustoimingute seaduslikkuse aluseks on *ultima ratio* põhimõtte järgimine, mis on sätestatud KrMS § 126[1] lg 2. Selle kohaselt on jälitustoimingu teostamine lubatud, kui andmete kogumine muude toimingutega või tõendite kogumine muude

http://www.heinonline.org.ezproxy.members.marshallcenter.org/HOL/Page?handle=hein.journals/hiblj10&div=9&start_page=119&collection=journals&set_as_cursor=0&men_tab=srchresults (31.08.2016).

[118] Infoühiskond on koondmõiste rõhutamaks info ja infokäitluse mahtude ja tähtsuse suhtelist suurenemist tänapäeva ühiskonnas. See on kõikehõlmav ning haarab kogu sotsiaalset reaalsust. Infoühiskonna peamiseks tunnuseks on arvutite massiline kasutamine ja kõikjale ulatuvad ülemaailmsed, personaalsed kommunikatsioonikanalid (Internet ja sellel baseeruvad struktuurid) ning elektroonilised teenused. Vikipeedia – Infoühiskond. Arvutivõrgus: https://et.wikipedia.org/wiki/Info%C3%BChiskond (03.01.2017).

[119] D. H. Flaherty. Protecting Privacy in Surveillance Societies. USA: The University of North Carolina Press 1989, lk 12.

[120] EIKo 5029/71, *Klass and others v. Germany*, p 46.
Arvutivõrgus: http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-57510 (19.11.2016).

[121] Kriminaalmenetluse seadustik. – RT I 2003, 27, 166 … RT I, 31.12.2016, 46. Arvutivõrgus: https://www.riigiteataja.ee/akt/106012016019 (22.02.2016).

menetlustoimingutega ei ole võimalik. Kriminaalmenetluse välist jälitustegevust määratleb seadusandja teabe kogumisena ja töötlemisena julgeolekuasutuste seaduses[122] (edaspidi „JAS“)[123] nimetatud asutuste tegevuse eesmärkide kaudu.[124] Kriminaalmenetluse käigus kasutatav jälitustegevus peab olema lubatud vaid erandjuhtudel ja üksnes ülekaaluka avaliku huvi korral.[125] Vastasel juhul sekkub riik informatsiooni salajase kogumise ja töötlemisega inimese privaatsfääri ning riivab seeläbi põhiseadusega tagatud perekonna ja eraelu puutumatust.[126]

Riigi julgeoleku seisukohast on väga oluline eristada terminoloogiliselt jälitustegevust ning teabehanget. Teabehanke mõiste tuleneb JAS § 9 lg 2 ning hõlmab riigi julgeoleku seisukohast kõige ohtlikumate kuriteoliikide ennetamist veel enne kuriteo ettevalmistamise staadiumisse jõudmist. See eristab teabehanget oluliselt KrMS-is reguleeritud jälitustegevusest, mis hõlmab jälitustoiminguid. Teabehanke käigus kogutakse infot julgeolekut ohustavate kuritegude kohta, et neid haldusmenetluses ennetada. Teabehanke muutumisel jälitustegevuseks on tegemist olukorraga, kus mingil põhjusel ei olnud haldusmenetluse ennetavad meetmed piisavad ja tuleb tarvitusele võtta tugevamalt vabadusi piirav meede – kriminaalmenetlus. Jälitustegevuse ja teabehanke erinevust rõhutab ka asjaolu, et jälitustegevuseks kui isiku põhiõiguste piiramiseks annab jälitusasutusele prokuratuuri kaudu loa maakohtu kohtunik, sest tegevuse eesmärk on tõendi hankimine süüteo toimepanemise kohta. Teabehankes, mis on haldusmenetluse eriliik, lahendab halduskohtunik ilma prokurörita küsimuse isiku põhiõigused *versus* riigi julgeolek laiemalt, ilma et tegu oleks jõudnud karistusõiguslikult karistatavasse staadiumisse. Teabehankeliselt algab kuriteo tõkestamine oluliselt varem kui politseitöös. Selline teabehankeline tegevus on JAS § 4 mõttes kuriteo ärahoidmine mis tahes seaduslikul viisil enne selle toimepanemist.[127]

---

[122] Julgeolekuasutuste seadus. – RT I 2001, 7, 17 … RT I, 17.12.2015, 39. Arvutivõrgus: https://www.riigiteataja.ee/akt/117122015039 (27.12.2016).

[123] JAS § 2 lg 1 järgi on julgeolekuasutuste tegevuse eesmärk tagada riigi julgeolek põhiseadusliku korra püsimisega mittesõjaliste ennetavate vahendite kasutamise abil ning julgeolekupoliitika kujundamiseks ja riigikaitseks vajaliku teabe kogumine ja töötlemine. Arvutivõrgus: https://www.riigiteataja.ee/akt/117122015038?leiaKehtiv (20.06.2016).

[124] M. Kruusamäe, T. Reinthal. Kohtupraktika analüüs: Jälitustegevuse kohtulik eelkontroll Eestis. Tartu, mai 2013, lk 4. Arvutivõrgus: http://www.riigikohus.ee/vfs/1503/6_Lisa%205_Jalitustegevuse%20analuus.pdf (20.06.2016).

[125] EIKo 4378/02, *Bykov v. Russia*, p 78. Arvutivõrgus: http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-91704 (13.01.2017).

[126] E. Truuväli, jt. Eesti Vabariigi põhiseadus: kommenteeritud väljaanne. 2. tr. Tallinn: Juura 2008, lk 222.

[127] E. Heldna. Julgeolekuasutuste kogutud informatsiooni kasutamine kriminaalmenetluses ja jagamine uurimisasutustega. Juridica 2016/X, lk 720.

KrMS § 126[1] lg 4 järgi on jälitustoiminguga saadud teave tõend, kui selle saamisel on järgitud seaduses sätestatud nõudeid. Igasugune menetlusrikkumine jälitustegevuses toob kaasa tõendi lubamatuse. Riigikohtu kriminaalkolleegiumi (edaspidi „RKKK“) tõlgenduse järgi loetakse igasugused kõrvalekalded seadusega jälitustegevusele seatud regulatsioonist automaatselt kriminaalmenetlusõiguse oluliseks rikkumiseks.[128] Sellised tõendid jäetakse tõendikogumist välja. Jälitustoiminguga kogutavate tõendite puhul tuleb hinnata iga konkreetse menetluse raames ülalmainitud toimingute vajalikkust ja võimalust koguda tõendeid põhiõigusi vähem riivaval moel.

Valitsusasutused koguvad ning kasutavad aina enam digitaalselt kogutud andmeid ja kõrgtehnoloogilisi meetodeid suurandmetest otsingute teostamiseks.[129] Teostatud analüüside kaudu suunatakse julgeoleku- ja politseiasutuste ressursse sinna, kus kuritegude toime panemise tõenäosus on kõige suurem. Otsingute teostamise kasutatava informatsiooni kogumist viiakse läbi ka võrguliikluse kuulamise kaudu. Võrgu ja ka veebiliikluse pealtkuulamist kasutatakse informatsiooni kogumiseks. Näiteks on pealtkuulamise kaudu võimalik näha teiste inimeste omavahelist suhtlust, paroole, uurida, millega nad tegelevad, mis hostidega suhtlevad ja millise intensiivsusega. Seda informatsiooni saab hiljem ära kasutada.[130]

Kriminaalmenetluse eelses faasis saavad suurandmeid ja nende pinnalt teostavate analüütiliste otsuste tulemeid jälitustegevuses, oma pädevuse piires, kasutada järgnevad asutused:[131]

- Politsei- ja Piirivalveamet (edaspidi „PPA“);
- Kaitsepolitseiamet (edaspidi „KAPO“);
- Maksu- ja Tolliamet;
- Konkurentsiamet;
- Sõjaväepolitsei;
- Keskkonnainspektsioon;
- Justiitsministeeriumi vanglate osakond ja vangla.

[128] RKKKo 3-1-1-22-10 p 14.5. Arvutivõrgus: http://www.nc.ee/?id=11&tekst=222525397&fontSize=3 (14.01.2017).
[129] Fairfieldt/Luna, lk 984.
[130] E. Laaneoks. Sissejuhatus võrgutehnoloogiasse. Tartu Ülikool: Matemaatika-informaatikateaduskond, arvutiteaduse instituut 2010, lk 183. Arvutivõrgus: file:///C:/Users/kasutaja/Downloads/Sissejuhatus_vorgutehnoloogiasse.pdf (20.03.2017).
[131] Kriminaalmenetluse seadustik. – RT I 2003, 27, 166 … RT I, 31.12.2016, 46, § 126[2] lg 1.

KrMS § $126^2$ lg 1 nimetatud alusel võivad ülaltoodud asutused jälgida varjatult isikut, asja või paikkonda, koguda varjatult võrdlusmaterjali ja teha esmauuringuid, teostada varjatult asja läbivaatust ning asendada selle varjatult. KrMS § $126^2$ lg 2 alusel võivad PPA ja KAPO lisaks veel ka vaadata varjatult läbi postisaadetisi, vaadata või kuulata salaja pealt teavet ja kasutada politseiagenti ning seda karistusseadustikus[132] (edaspidi „KarS“) ettenähtud kuritegude lõikes.

Jälitustoiminguga riivatakse alati isiku põhiõigusi. Näiteks piirab varjatud sisenemine eluruumi EV põhiseaduses[133] (edaspidi „PS“) § 33 sätestatud korteripuutumatust ning postisaadetise varjatud läbivaatus või kõnede salajane pealtkuulamine PS § 43 sätestatud kommunikatsioonivahendite abil edastatava teabe saladust. Kuna jälitustoiminguid tehakse aga salaja, siis ei saa isik oma põhiõiguste riivest teada ning see kujutab endast informatsioonilise enesemääramise õiguse riivet. Enesemääramise põhimõte tagab üldiselt igaühe õiguse teada saada, kes ta on; otsustada, kes ta olla tahab, kellena riik teda kohtleb ja kuidas ise ennast teistele inimestele esitleda. Informatsiooniline enesemääramine üldjoontes tähendab igaühe õigust ise otsustada, kas ja kui palju tema kohta andmeid kogutakse ja salvestatakse.[134]

Suurimaks suurandmete kasutajaks kriminaalmenetluse eelses faasis on KAPO, kelle ülesandeks on teabe kogumine ja töötlemine JAS-is ettenähtud juhtudel ja korras.[135] JAS § 6 kohaselt on KAPO ülesanneteks:

- riigi põhiseadusliku korra ja territoriaalse terviklikkuse vägivaldse muutmise ärahoidmine ja tõkestamine;
- riigi vastu suunatud luuretegevuse ennetamine ja tõkestamine;
- terrorismi ja selle rahastamise ning toetamise ärahoidmine ja tõkestamine;
- riigi julgeolekut ohustava korruptsiooni ärahoidmine ja tõkestamine ning nende kuritegude tõkestamine, mille kohtueelne uurimine on KAPO pädevuses.

JAS § 25 lg 2 ja 3 kohaselt võib KAPO kui julgeolekuasutus oma pädevuse piires kuriteo tõkestamiseks piirata isiku õigust sõnumi saladusele, kui on olemas piisavad andmed

---

[132] Karistusseadustik. – RT I 2001, 61, 364 … RT I, 31.12.2016, 14. Arvutivõrgus: https://www.riigiteataja.ee/akt/184411?leiaKehtiv (22.03.2017).

[133] Eesti Vabariigi põhiseadus. – RT 1992, 26, 349 … RT I, 15.05.2015, 2. Arvutivõrgus: https://www.riigiteataja.ee/akt/115052015002?leiaKehtiv (24.02.2016).

[134] M. Rondel. Informatsioonilise enesemääramise õigus ja jälitustegevus: isiku õigus teada saada tema suhtes tehtud jälitustoimingutest. Juridica 2016/X, lk 713.

[135] Kaitsepolitseiameti põhimäärus. – RT I, 15.02.2017, 6. § 8 p 8. Arvutivõrgus: https://www.riigiteataja.ee/akt/107112014001 (27.12.2016).

ettevalmistatava või toimepandava kuriteo kohta. Lisaks on KAPO-l õigus teabe varjatud kogumisel meetodi ja vahendina teostada ka telekommunikatsioonivõrgu kaudu edastatavate sõnumite ning edastaja või vastuvõtja kohta andmete kogumist päringuga telekommunikatsioonivõrgu operaatorile või telekommunikatsiooniteenuse osutajale[136].

EV-s kehtiva ESS § 111[1] lg 1 alusel on sideettevõtja kohustatud säilitama andmeid, et oleks võimalik teha järgmiseid toiminguid:

- sideallika seiramine ja tuvastamine;
- side sihtpunkti tuvastamine;
- side kuupäeva, kellaaja ja kestuse kindlaksmääramine;
- sideteenuse liigi kindlaksmääramine;
- sideteenuse kasutaja terminalseadme või oletatava terminalseadme kindlaksmääramine;
- terminalseadme asukoha kindlaksmääramine.

Eeltoodu põhjal hangitud andmeid võidakse kasutada füüsiliste isikute profileerimiseks ja nende tuvastamiseks, eelkõige juhul, kui neid kombineeritakse serveritesse saabuvate kordumatute identifikaatorite ning muu teabega.[137]

Julgeoleku- ja politseiasutused võivad kuritegevuse vastases võitluses ning tõendina kohtus kasutada lisaks muid erinevatest allikatest saadud andmeid, näiteks valvekaamerate salvestused või muude uurimistoimingute kaudu saadud andmeid. KrMS § 63 lg 1 kohaselt on tõend kahtlustatava, süüdistatava, kannatanu, tunnistaja või asjatundja ütlus, ekspertiisiakt, eksperdi antud ütlus ekspertiisiakti selgitamisel, asitõend, uurimistoimingu, kohtuistungi ja jälitustoimingu protokoll või videosalvestis, samuti muu dokument ning foto või film või muu teabetalletus. Tõendina saab kasutada kinnipidamiste või pealtkuulamiste ning jälgimise teel saadud andmeid. Samuti ka maksulaekumiste, sõidukite kasutamise või isiku haigusloo ga seonduvad andmed.

[136] Kaitsepolitseiameti poolt teabe varjatud kogumisel kasutatavad meetodid ja vahendid ning teabetoimiku pidamise ja säilitamise kord. – RTL 2001, 70, 945 … RT I, 07.02.2013, 9, § 2. Arvutivõrgus: https://www.riigiteataja.ee/akt/27091?leiaKehtiv (12.03.2017).

[137] Euroopa Parlamendi ja Nõukogu määrus (EL) 2016/679, 27. aprill 2016, millega kehtestatakse füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus) ELT L 119, preambul 30. Arvutivõrgus: http://eur-lex.europa.eu/legal-content/ET/TXT/HTML/?uri=CELEX:32016R0679&from=ET (26.04.2017).

Pilveteenuse tekkimine ja otsingumootorite loomine, mis võimaldavad teostada kogu veebimaterjali ulatuses otsinguid, on aidanud kaasa sellele, et suurandmetest on moodustunud unikaalne andmete kogum. Andmed on alatiselt olemas ning need on kättesaadavad, millal iganes neid on vaja kasutada.[138]

Väiksemate andmemahtude kogumeid on üldjuhul võimalik tõendite kujunemisel julgeoleku- ja politseiasutuste poolt lähemalt uurida ning nende õigsust tõendada. Suurandmete puhul ei ole selline lähenemine aga alati võimalik, kuna andmete mahud on pidevas muutumises – need võivad suureneda, pärinevad mitmetest allikatest ning ei ole täpselt kontrollitavad. Suurandmete kasutamisel tuleb arvestada sellega, et osa olemasolevast infost ei pruugi sobituda uuritava sündmuse asjaoludega ning ei võimalda seega otsuste kujundamist. Tagamaks kasutatavate andmete asjakohasust konkreetse menetluse raames, tuleb andmetele teostada kvaliteedi kontrolli, mida on aga võimalik teostada vaid teades, milliste asjaolude tõendamiseks neid kasutatakse.

EV-s on sisejulgeoleku tagamiseks ja ennetamaks võimalikke tahtlikke ründeid ning Schengeni viisaruumi kompenseerimismeetmetena julgeoleku- ja politseiasutustel juurdepääs rongi-, laeva- ja lennureisijate nimekirjadele.[139] Antud õiguste olemasolu on põhjendatud vajadusega tagada sisejulgeolekut ning tõhustada terrorismivastast võitlust, kus proportsionaalseks meetmeks on ka infotehnoloogilised analüüsi vahendid.

Julgeolekuasutustel on võimalik kasutada ka erinevate otsingusõnade abil veebikeskkonda monitoorivaid rakendusi ning nende abil tuvastada nende abil neile huvi pakkuvaid postitusi. Ühe sellise Eestis kasutatava keskkonna näitena meediamonitooringu kontekstis võib välja tuua uue põlvkonna analüüsiteenuse STATION[140].

[138] J. J. Berman, lk 205.
[139] Riigipiiri seadus. – RT I 1994, 54, 902 … RT I, 06.04.2016, 11, § $9^3$. Arvutivõrgus: https://www.riigiteataja.ee/akt/106042016011?leiaKehtiv (12.03.2017).
[140] STATION mõtestab Eesti inforuumi pidevalt jälgides ja analüüsides üle 2500 kajastuse päevas. See aitab kasutajal keskenduda vaid olulisele infole aidates kogu informatsioonist selekteerida välja kasutaja eelistustele vastavat informatsiooni.

Võimaldades julgeoleku- ja politseiasutuste töös suurandmeid kasutada tuleb tagada efektiivne andmete kasutamise kontroll ning tuvastada, et kasutatavad meetodid on vajalikud ja proportsionaalsed arvestades ühiskonnas avalduvat kasu, mida sellega saadakse.[141]

EV-s on senini suurandmete töötlemist riiklikul tasandil planeeritud kasutada poliitikaotsuste kujundamiseks. Poliitikaotsuste kujundamisel suurandmete analüüsi kaudu võidakse esmapilgul saavutada otsuste kujundamisel efektiivsus ja ratsionaalsus, kuid ohuks on, et selles ei arvestata võimalikku inimlikku faktorit kui tundmatut tegurit. Viimasega mitte arvestamine võib kaasa tuua inimeste jaoks negatiivse mõjuga otsuseid, kuna otsuste tegemisel väljakujunenud ühiskondlik struktuur ei pruugi olla ratsionaalne, kuid see on siiski ühiskonna stabiilsuse aluseks.

EV-s leidis suurandmete alusel poliitikaotsuste kujundamise temaatika kajastamist Vabariigi Valitsus 2015. aasta tegevuskavas. Dokumendis on suurandmete tegevusena välja toodud eesmärk luua ja võtta kasutusele analüüsivõimekust edendavaid IKT-lahendusi. Näiteks uurida süvaanalüütika ning suurandmete trendiga kaasnevaid võimalusi andmete reaalajas jälgimiseks ja ennustatavate poliitikaotsuste tegemiseks.[142] Samuti on EV-s suurandmete kasutamist, töötlemist ning nende alusel ennustavate otsuste tegemist käsitletud 2014. aastal valminud uuringus „Lingitud Eesti". Uuringu eesmärgiks oli leida ja pakkuda välja lahendus linkandmete[143] tehnoloogiate laiemaks kasutuselevõtuks. See sisaldas soovitusi avaliku ja erasektori andmekogude, veebisaitide ja muude inforessursside ümberkorraldamiseks ning neid toetavate riigi poolsete meetmete rakendamiseks. Linkandmeid vaadeldi seal kui tehnoloogilist suundumust, mis on seotud ülemaailmsete valdkondadega nagu tulevikuinternet (*Future Internet*, FI), asjade Internet (*Internet of Things*), suurandmed (*Big Data*) ja avaandmed (*Open*

[141] Big Data, Crime and Security. Houses of Parliament. July 2014, No 470. Arvutivõrgus: http://www.google.ee/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=0ahUKEwj8vdKdxOrKAhVDG5oKHeU-CboQFgggMAE&url=http%3A%2F%2Fresearchbriefings.files.parliament.uk%2Fdocuments%2FPOST-PN-470%2FPOST-PN-470.pdf&usg=AFQjCNEJdsdCcBFCr6tEtx7yyDS_hDAcNA (22.02.2016).

[142] Vabariigi Valitsuse korraldus „Valitsusasutustele ja valitsusasutuste hallatavatele riigiasutustele 2015. Aastaks määratud tööjõu- ja majandamiskulude jaotus, investeeringute ja investeeringutoetuste objektiline liigendus ning ministeeriumide ja nende valitsemisala riigiasutuste 2015. aasta tegevuskavad" Lisa 3. Arvutivõrgus: https://www.riigiteataja.ee/aktilisa/3311/2201/4001/581klisa3.pdf (20.01.2017).

[143] Linkandmed on internetis leiduvad andmed, mis on omavahel seostatud. Linkandmetevahelised seosed ei ole mõeldud inimestele lugemiseks, vaid on tehtud nii, et neid oleks lihtne automaatselt arvutitega töödelda ja moodustada suuremaid andmemassiive, millest infot pärida. Linkandmetes nähakse võimalikku lahendust probleemile, kuidas järjest kasvavas veebitulevate andmete mahus orienteeruda, saades sellest maksimaalset kasu. (Linkandmed. Wikipedia. Arvutivõrgus: https://et.wikipedia.org/wiki/Linkandmed (12.03.2017)).

*Data*).[144] Dokument tõi ka välja, et EV-s on suurandmete hõive ja analüütika tehnoloogiad kasutuselevõtu algfaasis.[145]

## 2.3 Sideandmete kogumise erisused ja õiguslik raamistik

Jälitustoimingute korral peavad sideettevõtjad võimaldama korrakaitseorganile juurdepääsu sidevõrgule, mis võimaldab valida sõnumeid ja kanda neid reaalajas üle nende asutuste tsentraalsetesse või kaasas kantavatesse jälgimisseadmesse originaal ehk muutmata kujul. Samuti peavad sideettevõtjad tagama mobiiltelefoni võrgus kasutatavate terminalseadmete tuvastamise reaalajas (nn positsioneerimine). Seega on korrakaitseorganil võimalik jälgida samaaegselt jälgitava sõnumeid, tema liikumist ja asukohta. Elektroonilise side liiklus- ja asukohaandmete töötlemisel võidakse isiku kohta saada rohkem teada kui mõne temaga seotud sõnumi lugemisel. Elektroonilise side liiklus- ja asukohaandmete põhjal võib saada teavet isiku eraelu intiimsete detailide kohta.[146]

Sideteenuste ja sidevõrkude pakkujate tegevusega kaasnevate või nende töödeldud andmete säilitamisega seonduv on Euroopa kontekstis tõstatanud mitmeid diskussioone ja kohtuvaidlusi. Põhiliseks neist, mille osas arutelud on toimunud, on 2006. aasta 15. märtsil Euroopa Parlamendi ja Nõukogu poolt vastu võetud direktiiv 2006/24/EÜ[147], mille koostamiseks andsid olulise tõuke 2004. aasta Madridi ja 2005. aasta Londoni terrorirünnakud.

Direktiivi 2006/24/EÜ eesmärgiks oli ühtlustada teenusepakkujate kohustused säilitada teatavaid sideandmeid nii, et oleks tagatud nende kättesaadavus vastavalt liikmesriikide riiklikule õigusele määratletud raskete kuritegude uurimiseks, avastamiseks ja kohtus menetlemiseks. Direktiivi 2006/24/EÜ kohaselt pidid liikmesriigid kehtestama reeglid, millega telekommunikatsiooni ettevõtetele pannakse kohustus säilitada kõik andmeliiklus- ja asukohaandmed (edaspidi „sideandmed“) kindlaks määratud perioodi jooksul ning teha sellised andmed teatud tingimustel kättesaadavaks õiguskaitseasutustele. Ühtlasi avati selles ka

---

144 Lõpparuanne: Uuring „Lingitud Eesti“. Tallinn 2014, lk 10. Arvutivõrgus https://riigikantselei.ee/sites/default/files/content-editors/TOF/TOF_uuringud/lingitud_eesti_lopparuanne_2.0.pdf (04.01.2017).

145 Lõpparuanne: Uuring „Lingitud Eesti“, lk 2.

146 U. Lõhmus 2016/III, lk 182.

147 Euroopa Parlamendi ja Nõukogu direktiiv 2006/24/EÜ, 15. märts 2006, üldkasutatavate elektrooniliste sideteenuste või üldkasutatavate sidevõrkude pakkujate tegevusega kaasnevate või nende töödeldud andmete säilitamist, millega muudetakse direktiivi 2002/58/EÜ – ELT L 105/54. Arvutivõrgus: http://eur-lex.europa.eu/legal-content/ET/TXT/HTML/?uri=CELEX:32006L0024 (22.04.2017)

elektroonilise side liiklus- ja asukohaandmete mõiste. Nendeks on andmed, mis võimaldavad tuvastada:

- sideallika;
- side sihtpunkti;
- side kuupäeva, aja ja kestuse;
- sideliigi;
- kasutaja sidevahendi;
- mobiilside vahendi asukoha.

Eesti õigusesse võeti direktiiv 2006/24/EÜ üle 15. novembril 2007. aastal ESS-iga[148], mis reguleerib elektrooniliste sideandmete kogumist.[149]

Andmed, mida üldkasutatavate elektrooniliste sideteenuste või üldkasutatavate sidevõrkude pakkujad peavad direktiivi artiklite 3 ja 5 kohaselt säilitama, on eelkõige andmed, mis on vajalikud sideallika ning side sihtpunkti seiramiseks ja tuvastamiseks, side kuupäeva, aja ja kestuse ning sideliigi kindlaksmääramiseks, kasutaja sidevahendi kindlaksmääramiseks ja mobiilsidevahendi asukoha kindlaksmääramiseks. Samuti kuuluvad nende andmete hulka abonendi või registreeritud kasutaja nimi ja aadress, telefoninumbrid, millelt ja millele helistati, ning internetiteenuste puhul IP-aadress. Antud andmed võimaldavad muu hulgas teada saada, millise isikuga ja millise sidevahendi kaudu abonent või registreeritud kasutaja suhtles ning teha kindlaks side toimumise aja ja koha. Samuti võimaldavad andmed tuvastada, kui sageli abonent või registreeritud kasutaja teatud isikutega mingil ajavahemikul suhtles, teha väga täpseid järeldusi isikute eraelu kohta, kelle andmeid säilitatakse (nt nende igapäevaelu harjumuste, alalise või ajutise elukoha, igapäevaste või muude liikumiste, tegevuste, sotsiaalsete suhete ja ühiskonnagruppide jms kohta, kellega nad läbi käivad).[150]

EV kontekstis paneb ESS § 111[1] sideettevõtjale kohustuse säilitada andmeid, mis võimaldaksid tuvastada ja seirata sideallikat, side sihtpunkti ning määrata kindlaks side kuupäeva, kellaaja, kestuse, sideteenuse liigi, sideteenuse kasutaja terminalseadme ja terminalseadme asukoha. Isiku asukoha tuvastamine läbi positsioneerimise on politsei jaoks menetluse läbiviimisel

[148] Elektroonilise side seadus. – RT I 2004, 87, 593 … RT I, 23.03.2017, 5.
[149] U. Lõhmus 2016/III, lk 176.
[150] EKo C-293/12 ja C-594/12, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, p 26, 27. Arvutivõrgus: http://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=ET&mode=lst&dir=&occ=first&part=1&cid=853378 (22.02.2016).

oluline instrument. Nimelt võib vastavalt KrMS[151] § 90[1] menetlust läbi viiva asutuse ametnik, kui see on vältimatult vajalik kriminaalmenetluse eesmärgi saavutamiseks, teha päringuid elektroonilise side ettevõtjale üldkasutatava elektroonilise side võrgus kasutatavate identifitseerimistunnustega seotud lõppkasutaja tuvastamiseks vajalike andmete saamiseks.

Õiguskaitseorganid on pikka aega väitnud, et andmete säilitamine ning nende kättesaadavaks tegemine on vajalik ja tõhus abinõu kuritegude, eriti organiseeritud kuritegude ja terrorismikuritegude uurimiseks ning ka ärahoidmiseks. Samas tekitas eelmainitud direktiiv juba alates selle jõustumisest vastuväiteid, sest kommunikatsiooni liiklus- ja asukohaandmete säilitamise kohustuses nähti ülemäärast sekkumist põhiõigustesse, eelkõige privaatsusõigusse. Samuti tõstatus direktiivi vastuvõtmisega küsimus, kas jälgimisühiskond on tänases ajas ja ruumis paratamatu.[152] Euroopa Inimõiguste Kohus (edaspidi „EIK“) on lahendis *S. ja Marper v. Ühendkuningriik* märkinud, et Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni[153] ehk Euroopa inimõiguste konventsiooni (edaspidi „EIÕK“) artikliga 8 eraelule antud kaitse nõrgeneb vastuvõetamatult. Nimelt tänapäeva teaduse ja tehnoloogia saavutusi kasutatakse esmajoones tulu teenimiseks arvestamata selle mõju eraelule.[154]

Euroopa Kohtu Suurkoja otsusega[155] tunnistati direktiiv 2006/24/EÜ kehtetuks. Kohus analüüsis otsuses direktiivi kehtivust EL Põhiõiguste Harta (edaspidi „harta“)[156] artiklite 7, 8 ja 11 valguses ehk direktiivi artiklis 3 sätestatud üldkasutatavate elektrooniliste sideteenuste või üldkasutatavate sidevõrkude pakkujate kohustust säilitada direktiivi 2006/24/EÜ artiklis 5 loetletud andmeid, et teha need pädevatele siseriiklikele asutustele vajadusel kättesaadavaks. Teostatud analüüs tõstatas küsimused, mis on seotud harta artiklis 7 ettenähtud eraelu ja sõnumite saladuse austamisega, artiklis 8 ette nähtud isikuandmete kaitsega ja artiklis 11 ettenähtud sõnavabaduse austamisega.[157]

---

[151] Kriminaalmenetluse seadustik. – RT I 2003, 27, 166 … RT I, 31.12.2016, 46.

[152] U. Lõhmus. Elektroonilise side andmete säilitamise lõpetamata saaga. Juridica 2015/X, lk 735.

[153] Inimõiguste ja põhivabaduste kaitse konventsioon. – RT II 2000, 11, 57. Arvutivõrgus: https://www.riigiteataja.ee/akt/78154 (22.02.2016).

[154] EIKo 30562/04 ja 30566/04, *S. ja Marper v. Ühendkuningriik*, p 112. Arvutivõrgus: http://curia.europa.eu/juris/document/document_print.jsf;jsessionid=9ea7d2dc30db69c838cfc5564f1a96a6f2276d03d122.e34KaxiLc3qMb40Rch0SaxuNb3b0?doclang=ET&text=&pageIndex=0&part=1&mode=DOC&docid=150642&occ=first&dir=&cid=13384 (22.03.2017).

[155] EKo C-293/12 ja C-594/12, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*.

[156] Euroopa Liidu Põhiõiguste Harta. – 2012/C 326/02. Arvutivõrgus: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0389:0403:et:PDF (22.02.2016).

[157] EKo C-293/12 ja C-594/12, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, p 24.

Euroopa Kohtu Suurkoda leidis analüüsis, et andmete säilitamine eesmärgiga teha need vajadusel pädevatele siseriiklikele asutustele kättesaadavaks vastab üldist huvi pakkuvale eesmärgile. Testides proportsionaalsuse põhimõtte kaudu, kas õigusaktiga taotletavate õiguspäraste eesmärkide saavutamiseks on need sobivad ja vajalikud, jõudis kohus järeldusele, et õigusakt peab sätestama selged ja täpsed reeglid meetme ulatuse ning kohaldamise kohta, sh kehtestama miinimumnõuded. Ehk isikutel, kelle andmeid säilitatakse, oleksid piisavad tagatised, mis võimaldaksid neil tõhusalt kaitsta oma isikuandmeid kuritarvituste ohu, ebaseadusliku juurdepääsu ja kasutamise eest.[158]

Otsuse vahetuks mõjuks oli direktiivi 2006/24/EÜ kehtetuks tunnistamine. Selle asemele Euroopa Komisjon uut direktiivi välja töötama ei asunud, vaid andis 16. septembri 2015. aastal pressiteates teada, et ta ei esita uusi ettepanekuid elektroonilise side andmete säilitamise reguleerimiseks. Seega jäid kõnealust valdkonda reguleerima kaks direktiivi: Euroopa Parlamendi ja Nõukogu 24. oktoobri 1995. aasta direktiiv 95/46/EÜ üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta ning Euroopa Parlamendi ja Nõukogu 12. juuli 2002. aasta direktiiv 2002/58/EÜ, millega reguleeritakse isikuandmete töötlemist ja eraelu puutumatuse kaitset elektroonilise side sektoris.[159]

Direktiivi 2006/24/EÜ kehtetuks tunnistamise otsuses leidis kajastust, et puuduvad objektiivsed kriteeriumid, mis võimaldaks tagada, et ainult pädevatel siseriiklikel asutustel oleksid andmetele juurdepääsud ning nad saaksid hiljem andmeid kasutada üksnes raskete kuritegude ennetamise, avastamise või kohtus menetlemise eesmärgil. Samas on see oluline, et õigustada põhiõiguste riive ulatust ja raskust.[160] Antud kriteeriumite olemasolu on Eesti kontekstis analüüsinud ka õiguskantsler. Õiguskantsler toob oma analüüsis välja, et kuna avaldus oli seostatud Euroopa Komisjoni otsusest tulenevate järeldustega, siis tuleb rõhutada, et nimetatud otsuses toodud seisukohad puudutavad üksnes direktiivis sisalduvat ja ei ole üks-üheselt laiendatavad direktiivi 2006/24/EÜ rakendamiseks kehtestatud riigisisesele õiguslikule regulatsioonile ehk ESS-ile. Direktiivi 2006/24/EÜ suhtes tehtud järeldused ei saa olla üheselt Eesti õiguskorda ülekantavad põhjusel, et see sätestas paljudes küsimustes üksnes raamnõuded,

[158] EKo C-293/12 ja C-594/12, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, p 44, 54.
[159] U. Lõhmus. Elektroonilise side andmete säilitamise saaga sai lahenduse, Eestis siiski veel mitte. Juridica 2016/X, lk 698-708.
[160] EKo C-293/12 ja C-594/12, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, p 60.

jättes EL liikmesriikidele nende sisustamisel olulise kaalutlusruumi. ESS-i regulatsioon läheb direktiivist 2006/24/EÜ ja selles sätestatud miinimumnõuetest aga mitmetes küsimustes kaugemale. Selle kehtetus ei muuda seda, et ESS-i regulatsioon igal juhul PS-i vastane oleks ning tuleks seetõttu siseriiklikult kehtetuks tunnistada. Samuti ei saa rääkida ESS-i automaatsest kehtetusest. Õiguskantsler on seisukohal, et andmete ennetava kogumise ja säilitamise regulatsioon, nagu see on ette nähtud ESS § 111[1], ei ole selgelt ebamõõdukas ega PS-iga vastuolus. Kuigi andmeid säilitatakse valimatult kõigi sideteenuse osutajate ja kõigi sideseansside kohta, ei sisalda säilitatav teave sõnumite sisu ning riive on tasakaalustatud objektiivse vajadusega tagada kuritegevuse vastane võitlus. Arvestades avaliku korra ning inimeste õiguste ja vabaduste kaitsmist kaasaja tehnoloogia arenguga kaasnenud olukorraga on ESS-iga kehtestatud meetmed vajalikud, kuna teabe saamiseks puuduvad sageli mõistlikud alternatiivid.[161]

Õiguskantsleriga sarnasele järeldusele on jõudnud ka EV Riigikohus, mis on välja toonud[162], et eelkirjeldatud andmete kogumine, säilitamine ja kriminaalmenetluses kasutamine riivavad õigust eraelu puutumatusele PS § 26 mõistes. PS lubab selle põhiõiguse piiramist seaduses sätestatud juhtudel ja korras tervise, kõlbluse, avaliku korra või teiste inimeste õiguste ja vabaduste kaitseks, kuriteo tõkestamiseks või kurjategija tabamiseks. RKKK leidis, et kriminaalasjas sideettevõtjalt andmete taotlemine vastab PS § 26 mõttes kuriteo tõkestamise või kurjategija tabamise eesmärgile. Vaieldamatult on meede sobiv eeltoodud eesmärkide tagamiseks ehk soodustab kurjategijate tabamist ja edasiste kuritegude tõkestamist. Abinõu on vajalik, sest tegemist on efektiivse meetmega saamaks objektiivseid tõendeid isikute suhtlemise fakti ja viibimiskoha osas, mille kogumine muul viisil ei ole kindel ega tagatud (nt ei ole sündmusel tunnistajaid, süüdistatavad keelduvad ütluste andmisest jmt).

21. detsembril 2016. aastal tehtud otsuses *Tele2 Sverige AB v. Post-och telestyrelsen and Secretary of State for the Home Department v. Tom Watson and others* leidis Euroopa Kohtu Suurkoda, et hartaga ei ole kooskõlas olukord, mille kohaselt liikmesriik nõuab kõiki isikuid puudutavate kõikide sideseansside andmete säilitamist. Säilitamise kohustuseks peaks olema

[161] Ü. Madise. Õiguskantsleri seisukoha edastamine. Tallinn: Õiguskantsleri Kantselei, 2015. Arvutivõrgus: http://oiguskantsler.ee/sites/default/files/field_document2/6iguskantsleri_seisukoht_vastuolu_mittetuvastamise_kohta_elektroonilise_side_andmete_kogumine_sideettevotete_poolt.pdf (22.02.2016).
[162] RKKKo 3-1-1-51-14 p 22. Arvutivõrgus: http://www.nc.ee/?id=11&tekst=222577237 (24.02.2016)

piiritletud teatud liiki seadmete, teatud isikute valimi või muu osas.[163] Samuti nõudis kohus, et andmete kasutamine peab olema proportsionaalne ja vajalik ning olema lubatud ainult raskete kuritegude ennetamiseks, avastamiseks ja uurimiseks. EV-s kehtiv regulatsioon sellist eristamist ette ei näe.

Sideandmete säilitamise regulatsiooni peamised aspektid Eestis lähtuvalt ESS § 111[1]:

- andmeid säilitatakse kõikide isikute, kõikide seadmete ja kõikide sideseansside kohta;
- andmeid säilitatakse aasta jooksul alates sideseansi toimumisest;
- andmete kasutamine on lubatud erinevatele asutustele erinevate menetluste raames (sh kriminaal-, väärteo-, tsiviilkohtu-ning haldusmenetlus, tausta- ning julgeolekukontroll jt).

Kehtiva korra alusel on Eestis sideandmetele juurdepääs tulenevalt ESS § 111[1] lg 11:[164]

- uurimisasutustel, jälitusasutustel, prokuratuuril ja kohtul kriminaalmenetluses vajaliku teabe kogumiseks;
- julgeolekuasutustel põhiseadusliku korra kaitse eesmärgil;
- Andmekaitse Inspektsioonil, Finantsinstpektsioonil, Keskkonnainspektsioonil, PPA-l, KAPO-l ning Maksu- ja Tolliametil väärteomenetluses vajaliku teabe kogumiseks;
- Finantsinspektsioonil piiratud juhtudel riikliku järelevalve teostamise eesmärgil;
- kohtul tsiviilvaidluste lahendamise eesmärgil;
- jälitusasutustel kriminaalmenetluse väliste toimingute tegemiseks isiku suhtes, kelle puhul on põhjendatud alust arvata, et ta paneb toime kuriteo või isiku, kes on kuulutatud tagaotsitavaks;
- pädevatel asutustel tausta- ja julgeolekukontrolli teostamise eesmärgil.

Vastavalt eeltoodule toimub andmetele juurdepääs ilma eelneva kohtuloata (erandiks andmete kasutamine väärteomenetluses), teatud juhtudel annab loa prokuratuur. Seadustes puuduvad selgelt piiritletud kriteeriumid, millistel juhtudel on eri liiki menetluses andmete kasutamine lubatud ning selge regulatsioon sõltumatu järelevalve teostamiseks. Osade menetluste puhul

[163] EKo C-203/15 ja C-698/15, *Tele2 Sverige AB v. Post-och telestyrelsen and Secretary of State for the Home Department v. Tom Watson and others*. Arvutivõrgus: http://curia.europa.eu/juris/document/document.jsf?text=&docid=186492&pageIndex=0&doclang=ET&mode=lst&dir=&occ=first&part=1&cid=79169 (16.01.2017).
[164] Elektroonilise side seadus. – RT I 2004, 87, 593 … RT I, 23.03.2017, 5.

toimub andmetele juurdepääs isiku nõusoleku alusel, aga samas ei ole andmesubjektide õigused osade menetluste puhul nõuetekohaselt tagatud (nt teavitamine, andmetele juurdepääs jt).

*Tele2 Sverige AB v. Post-och telestyrelsen and Secretary of State for the Home Department v. Tom Watson and others* raames esitati Euroopa Kohtule ka taotlus selgitada, kas EL direktiivi 2002/58/EÜ artikli 15 lõiget 1 tuleb harta artikleid 7 ja 8 ning artikli 52 lõiget 1 arvesse võttes tõlgendada nii, et sellega on vastuolus riigisisese õiguse sätted, mis näevad kuritegevuse vastu võitlemise eesmärgil ette kohustuse säilitada üldiselt ja vahet tegemata kõikide klientide ning registreeritud kasutajate kõik liiklus- ja asukohaandmed. Nimelt sätestatakse direktiivi 2002/58/EÜ artikli 15 lõikes 1, et liikmesriigid võivad võtta seadusandlikke meetmeid, millega piiratakse sama direktiivi mitmes artiklis sätestatud klientide ning kasutajate kommunikatsiooni liiklus- ja asukohaandmete konfidentsiaalsust, kui selline piiramine on vajalik, otstarbekas ning proportsionaalne abinõu selleks, et kaitsta riigi julgeolekut, riigikaitset, avalikku korda, kuritegude või elektroonilise sidesüsteemi volitamata kasutamise ennetamist, uurimist, avastamist ja kohtus menetlemist. Kohus tõlgendas direktiivi 2002/58/EÜ kohaldamisala lähtuvalt selle ülesehitusest ning kinnitas, et selle üldist ülesehitust arvestades ei saa järeldada, et artikli 15 lõikes 1 nimetatud meetmed on direktiivi kohaldamisalast välistatud, sest vastasel juhul jääks see säte ilma oma soovitavast toimest. Direktiivi 2002/58/EÜ artikli 15 lõige 1 eeldab, et andmete säilitamine kuritegevuse vastu võitlemise eesmärgil kuulub selle kohaldamisalasse, sest see lubab liikmesriikidel võtta neid meetmeid ainult selles ette nähtud tingimustel.[165]

Tulenevalt *Tele2 Sverige AB v. Post-och telestyrelsen and Secretary of State for the Home Department v. Tom Watson and others* kohtuotsuses kehtestatud tingimustest, mille kohaselt ei toimuks kõikide sideseansside andmete säilitamist, vaid seda peaks teostama vaid teatud liiki seadmete ka isikute valimi osas ei ole autori arvates otstarbekas. Andmete säilitamiskohustusele riigisiseses õiguses mistahes piiravate kriteeriumite kehtestamine võib tuua kaasa diskrimineerimiskeelu rikkumise ning vähendada oluliselt andmete kättesaadavust mõjutades negatiivselt õiguskaitseasutuste tööd. Autor toetab EV õiguskantsleri ja Riigikohtu seisukohti, et sideettevõtjad peavad andmeid säilitama ning põhjendatud kahtluste olemasolul tegema andmed valitsusasutustele kuritegude uurimiseks ja ka ennetamiseks kättesaadavaks. Säilitada tuleb võimalus koguda andmeid kõikide isikute, seadmete ja sideseansside kohta ning säilitada

[165] U. Lõhmus 2016/X, lk 698-708.

neid alates sideseansi toimumisest aasta jooksul. Arvestades Euroopa Kohtu lahendi mõju ning lähtudes ESS §111[1], tuleks EV-s analüüsida, kas kehtiva õiguse kohaselt võib juurdepääsu omavatel asutustel, arvestades raske kuriteo määratlust olla selline õigus ettenähtud mahus olemas. Vajadusel tuleks juurdepääsu piirata ning kontrolli meetmeid andmetele juurdepääsu osas tõhustada.

Suurandmete kogumine ja kasutamine on midagi paratamatut, mis kaasneb tänapäeva ühiskonnaga ning selles leviva laialdase arvutikasutamisega. See omakorda võib kaasa tuua olukorra, kus riik võib sekkuda läbi info kogumise isikute erasfääri. Viimane võib kaasa tuua süütuse presumptsiooni riiveid seoses ennatlike järeldusotsuste kujundamisega kogutud andmete pinnalt. Arvestades isiku kohta olemasolevaid andmeid kujundatakse nende pinnalt toimingute läbiviimiseks seisukohad ning nende kaudu põhjendatakse kohtule teabehanke läbiviimiseks loa saamise vajadust. Seoses toimingute salastatusega ei pruugi isik, kelle osas neid teostatakse, oma põhiõiguste riivest teadlik olla.

## 2.4 Isikuõiguste kaitse võimalused ja Euroopa Liidu ühtsed meetmed

92% eurooplastest peab oma e-kirjade ja võrgus jagatud sõnumite konfidentsiaalsust oluliseks.[166] Ühiskondlik areng, kus info töötlemine on muutunud tänu arenevale tehnoloogiale hõlpsaks, on viinud selleni, et suuremaid jõupingutusi tegemata on võimalik võrdlemisi kiiresti töödelda isikute kohta käivad andmeid.[167]

Interneti tehniline olemus muudab võimatuks iga kande päritolu kontrollimise. Kui üks riik suudab tsenseerimist vajavale kandele oma territooriumil juurdepääsu piirata, siis Interneti kasutajad saavad sellest lihtsalt mööda minna, valides selleni jõudmiseks mingi teise riigi ülekande.[168] Reguleerimaks sensitiivse informatsiooni kaitset on EL-is vajalik rakendada ühtseid meetmed, milleks on vastu võetud erinevad direktiivid.

[166] Komisjoni ettepanek võtta elektroonilise side valdkonnas vastu kõrgetasemelised eraelu kaitse normid ja ajakohastada EL-i institutsioonide andmekaitsenorme. Euroopa Komisjon – Pressiteade. Brüssel, 10. jaanuar 2017. Arvutivõrgus: www.europa.eu/rapid/press-release_IP-17-16_et.pdf (14.01.2017).
[167] M. Rondel, lk 709.
[168] R. Ollila. Freedom of Speech and Protection of Privacy in Convergence of Electronic Communications. Rovaniemi: Acta Universitatis Lapponiensis 41 2001, lk 300.

Direktiivi 95/46/EÜ[169] eesmärgiks on kaitsta üksikisikuid isikuandmete töötlemise eest ja ühtlustada liikmesriikides rakendatavaid meetmeid. Direktiivi 95/46/EÜ preambula punktide 7 ja 8 kohaselt on eraelu puutumatuse õiguse kaitse tase seoses isikuandmete töötlemisega liikmesriigiti erinev ning takistuste kõrvaldamiseks isikuandmete liikumisel peab selliste andmete töötlemisega seotud üksikisikute õiguste ja vabaduste kaitse olema kõigis liikmesriikides samal tasemel. Direktiivi preambula punkt 9 toob välja, et siseriiklike õigusaktide ühtlustamisega saavutatakse samaväärne kaitstuse tase ning liikmesriigid ei saa enam takistada isikuandmete vaba liikumist ühest liikmesriigist teise põhjustel, mis on seotud üksikisikute õiguste ja vabaduste, eelkõige eraelu puutumatuse õiguse kaitsmisega. Näiteks on direktiivi hästi rakendatud Saksamaa Liitvabariigis, mille põhiseaduse artikkel I ja II kaitsevad isikuid personaalsete andmete piiramatu käitlemise eest ning mis on kohaldatavad ka tänapäeva modernses infoühiskonnas[170].

Direktiivi 2002/58/EÜ[171] eesmärgiks on kaitsta põhiõigusi ja selles järgitakse eelkõige harta artiklites 7 ja 8 sätestatud õigusi ehk era- ja perekonnaelu, kodu ja edastatavate sõnumite saladust ning isikuandmete kaitset. Isikuandmeid tuleb töödelda asjakohaselt ning kindlaks määratud eesmärkidel, asjaomase isiku nõusolekul või muul seaduses ettenähtud õiguslikul alusel. [172] Direktiivi 2002/58/EÜ kohaldatakse ainult traditsiooniliste telekommunikatsioonivõrgu operaatorite suhtes. See ei mõjuta liikmesriikide võimalust kuulata õiguspäraselt pealt elektroonilist sidet kooskõlas inimõiguste ja põhivabaduste kaitse Euroopa konventsiooniga. Meetmed peavad olema asjakohased, rangelt proportsionaalsed kavandatud eesmärgiga, vajalikud demokraatlikus ühiskonnas ning nendega peaksid kaasnema piisavad tagatised kooskõlas inimõiguste ja põhivabaduste kaitse Euroopa konventsiooniga.[173]

Privaatsuse all käsitletakse laia spektrit erinevaid probleeme ning õigusi ja kohustusi. Privaatsus viitab isikut ümbritseva ruumi puutumatusele, isiku õigusele langetada otsuseid ilma teiste inimeste sekkumiseta ja isiku õigusele kontrollida teda puudutava informatsiooni

[169] Euroopa parlamendi ja nõukogu direktiiv 95/46/EÜ, 24. oktoober 1995, üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta – ELT L 281. Arvutivõrgus: http://eur-lex.europa.eu/legal-content/ET/TXT/HTML/?uri=CELEX:31995L0046&from=et (16.02.2017).
[170] R. Ollila, lk 261.
[171] Euroopa parlamendi ja nõukogu direktiiv 2002/58/EÜ, 12. juuli 2002, isikuandmete töötlemist ja eraelu puutumatuse kaitset elektroonilise side sektoris (eraelu puutumatust ja elektroonilist sidet käsitlev direktiiv). – ELT L 201, lk 37-47 (eestikeelne eriväljaanne: ptk 13, kd 029, lk 514-524). Arvutivõrgus: http://eur-lex.europa.eu/legal-content/ET/TXT/PDF/?uri=CELEX:32002L0058&from=ET (14.01.2017).
[172] Euroopa Liidu Põhiõiguste Harta – 2012/C 326/02.
[173] Euroopa parlamendi ja nõukogu direktiiv 2002/58/EÜ, p 11.

liikumist ja avaldamist.[174] Õigus privaatsusele ei ole oma loomult absoluutne õigus, mis tähendab seda, et õigusliku aluse olemasolul on riive lubatud. Riive on õiguspärane, kui see on kooskõlas seadusega ja demokraatlikus riigis vajalik, riigi julgeoleku huvides, ühiskondliku turvalisuse huvides, riigi majandusliku heaolu huvides, korratuse või kuriteo ärahoidmiseks, tervise, kõlbluse ning kaasinimeste õiguste ja vabaduste kaitseks.[175]

Identiteet on unikaalsete tunnuste kogum, mille alusel isik eristub kõikidest teistest isikutest. Identiteet koosneb komponentidest, mille järgi on isikut võimalik tuvastada või mille järgi isik ennast määratleb. Näiteks on nendeks komponentideks isiku nimi, riigi poolt antud identifitseeriv numbrikombinatsioon (EV-s isikukood), etniline kuuluvus, isiku välimus, füüsilised omadused (pildid isikust), tema iseloom, käitumine, sotsiaalne võrgustik ning muud võimalikud personaalsed tunnused.[176]

Delikaatsete isikuandmete sisu identifitseerib andmesubjekti tema intiimse sfääri kaudu ning delikaatsete isikuandmete töötlemisel on seetõttu põhiõiguste riive intensiivsem. Delikaatsed isikuandmed on andmed, mis kirjeldavad andmesubjekti poliitilisi vaateid, usulisi ja maailmavaatelisi veendumusi, etnilist ja rassilist päritolu, terviseseisundit või puuet, pärilikku informatsiooni, biomeetrilisi andmeid, seksuaalelu, süüteo toimepanemist või selle ohvriks langemist enne avalikku kohtuistungit või õigusrikkumise asjas otsuse langetamist või asja menetluse lõpetamist.[177]

Direktiivi 2002/58/EÜ ei kohaldata andmetöötlusele, mis ei lange Euroopa õiguse kohaldumisalasse nagu näiteks EL lepingu V ja VI jao sätted politseikoostöö ja õigusalase koostöö kriminaalasjades.[178] Samuti ei kohaldada direktiivi 95/46/EÜ, kui see toimub sellise tegevuse käigus, mis jääb väljapoole ühenduse õigust, nagu näiteks EL lepingu V ja VI jaotises osutatud tegevused, ja igal juhul sellise töötlemise suhtes, mis on seotud avaliku korra, riigikaitse, riigi julgeoleku (sealhulgas riigi majanduslik heaolu, kui töötlemine on seotud riigi julgeoleku küsimustega) ja riigi toimingutega kriminaalõiguse valdkonnas.[179] Sarnane põhimõte jääb kehtima ka peale 25. maid 2018, mil hakkab kehtima Euroopa isikuandmete

[174] C. J. Bennet. Regulating Privacy. Data Protection and Public Policy in Europe and the United States. Ithaca: Cornell University Press 1992, lk 13.
[175] M. Männiko, lk 35.
[176] M. Männiko, lk 18, 19.
[177] M. Männiko, lk 43.
[178] M. Männiko, lk 73.
[179] Euroopa parlamendi ja nõukogu direktiiv 95/46/EÜ, art 3 p 2.

kaitse üldmäärus (2016/679/EÜ), millega hakatakse kohaldama kaitsenorme elektroonilise side teenuste pakkujate suhtes, mis kõnealuse direktiiviga hetkel kaetud ei ole (nt *WhatsApp, Facebook Messenger, Skype, Gmail, iMessage* või *Viber*).[180]

Ülaltoodud mitte kohaldumine ei ole aga absoluutne. Näiteks on Euroopa Kohtu otsuses *Tele2 Sverige AB v. Post-och telestyrelsen and Secretary of State for the Home Department v. Tom Watson and others*[181] kohus välja toonud direktiivi 2002/58/EÜ artikli 15 lg 1 tõlgenduse, mis loob erandi riiklikku andmete kogumise ja säilitamise osas, kui need on vajalikud julgeoleku, riigikaitse, avaliku korra, kriminaalkuritegude või elektroonilise sidesüsteemi volitamata kasutamise ennetamiseks, uurimiseks, avastamiseks või kohtus menetlemiseks. Kohtu seisukohast tulenevalt tuleb harta artikleid 7, 8 ja 11 ning direktiivi artikli 52 lõiget 1 arvesse võttes tõlgendada selliselt, et sellega on vastuolus need liikmesriigi õigusnormid, mis reguleerivad liiklusandmete ja asukohaandmete kaitset ning turvalisust ja millega antakse pädevate ametiasutuste juurdepääs säilitatavatele andmetele, piiramata seda juurdepääsu üksnes raske kuritegevuse vastu võitlemisega. Samuti tuleb ette näha, et andmetele juurdepääsu saamise eeltingimuseks on kohtu või sõltumatu haldusasutuse eelnev kontroll.

Andmed, mida elektroonilise side teenuste osutajad peavad säilitama, võimaldavad kindlaks teha side lähte- ja sihtkoha, kuupäeva, kellaaja ja kestuse, sideteenuse liigi ning kasutatud seadme ja mobiilsideseadme kasutamise asukoha. Muuhulgas kuuluvad nende andmete hulka abonendi või registreeritud kasutaja aadress, helistaja telefoninumber ja valitud number ning internetiteenuste IP-aadress. Täpsemalt võimaldavad need andmed teada saada, millise isikuga ja millise sidevahendi kaudu lepinguline klient või registreeritud kasutaja suhtles ning seeläbi teha kindlaks sideseansi toimumise aja ja koha. Samuti võimaldavad need andmed tuvastada, kui sageli lepinguline klient või registreeritud kasutaja teatud isikutega mingil ajavahemikul suhtles.[182]

Oluline on, et andmete kogumisel kasutatavad meetmed oleksid vajalikud, proportsionaalsed ja täpsed saavutatava eesmärgi suhtes ning nende kogumisel ei ületataks etteantud volitusnormi

[180] Komisjoni ettepanek võtta elektroonilise side valdkonnas vastu kõrgetasemelised eraelu kaitse normid ja ajakohastada EL-i institutsioonide andmekaitsenorme.
[181] EKo C-203/15 ja C-698/15, *Tele2 Sverige AB v. Post-och telestyrelsen and Secretary of State for the Home Department v. Tom Watson and others*.
[182] EKo C-203/15 ja C-698/15, *Tele2 Sverige AB v. Post-och telestyrelsen and Secretary of State for the Home Department v. Tom Watson and others*, p 98.

piire.[183] Indiviidide1 peab olema õigus kontrollida ja omada informatsioonile juurdepääsu ning samuti õigus keelduda sellise info kogumisest ja levitamisest. Indiviidide olulistest õigustest annab ülevaate alljärgnev loetelu: [184]

- õigus individuaalseks iseseisvuseks;
- õigus olla unustatud;
- õigus privaatsusele;
- õigus kontrollida enda kohta olemasolevat informatsiooni;
- õigus piirata olemasolevale informatsioonile juurdepääsu;
- õigus isikuga seonduvate andmete eksklusiivsele kontrollile;
- õigus piirata inimesele suunatud informatsiooni käitlemist;
- õiguslik ootus konfidentsiaalsusele;
- õigus nautida üksindust, intiimsust, anonüümsust, reserveeritust ja saladust.

Tulenevalt eeltoodust saab tuua välja, et suurandmete kasutusalad on EV-s ja EL tasandil USA kontekstist vaadatuna kitsamad, sest andmete kogumist viiakse läbi piiratumalt ning andmete kogumisele on EL-is ette nähtud õiguslik raamistik, mis sätestab isikuandmete kaitse piirid lubades julgeoleku- ja politseiasutustel andmete kogumist viia läbi vaid raskete kuritegude uurimistega seonduvalt. Õiguslikud alused, mida iga riik saab kriminaalmenetluses kasutatavate tõendite kogumise ja kasutamise korda sätestades kehtestada peavad olema kooskõlas hartaga tagades vajaliku põhiõiguste kaitse ulatuse.

EV-s on suurandmete kasutusala kriminaalmenetluses kasutatav läbi teabehanke ja jälitustoimingute läbiviimise, kus olemasolevaid andmeid saab kasutada konkreetse isiku osas võimaliku kuriteokahtluse tuvastamiseks. Andmete analüüsi tulemina suunatakse igapäevaselt ka politseiressursse sinna, kus on suurim tõenäosus, et kuritegusid võidakse toime panna. Ehk kogu kuritegevusega seotud andmete analüüsi pinnalt teostatakse võimalikke ennetusotsuseid. Samuti saavad julgeoleku- ja politseiasutused tõendina kasutada muid erinevatest allikatest saadud andmeid, näiteks valvekaamerate salvestused või muude menetlustoimingute kaudu saadud andmeid.

[183] R. Ollila, lk 274.
[184] D. H. Flaherty, lk 7, 8.

# 3. SÜÜTUSE PRESUMPTSIOON

Presumptsioon omab mitut tähendust. Õiguses kasutatakse seda eelduse väljendamiseks[185], st presumptsioon on eeldus, mis on õige niikaua, kuni ei ole tõendatud vastupidist.[186] Presumptsioon koosneb erinevatest õiguslikest tehnikatest ja doktriinidest. Presumptsiooni käsitletakse kui mehhanismi vähendamaks võimalikku eksimise riski kriminaalmenetlustes. Selleks tuleb identifitseerida faktid ning sisustada need kehtestatud tõendamisstandardi kaudu, kus iga fakt peab olema kontrollitav ja tõendatav.[187]

Lähtudes klassikalisest jaotusest saab süütuse presumptsiooni jagada kolme gruppi: [188]

- Presumptsioonid kui faktid – tõstatuvad kui üldtuntud, mitte kui õiguslikud konstruktsioonid, mida kohus võib konkreetsete olemasolevate faktide alusel kujundada.
- Ümberlükkamatu õiguse presumptsioon – kujuneb kindlate tõendite baasil, kus kohus on kohustatud kontrollima kõikide faktide olemasolu. Ehk sõltumata konkreetsetest esitatud tõenditest eemaldatakse kontrolli käigus võimalikud vasturääkivused.
- Ümberlükatav õiguse presumptsioon – tugineb kesksele riskijaotuse presumptsioonile, kus kohtu poolt faktide kontrollimine võib kaasa tuua fakt-fakti vastu olukorra, kus täiendavate tõendite esitamise võimalus on seetõttu raskendatud.

Riik tagab õiguse kehtimise läbi õigusliku raamistiku ning süütuse presumptsioon on selle raamisiku aluseks tõendite kujunemise normatiivsete aktide loomisel. Antud õigusliku raamistiku loomine ning kehtestatud tõendite kujunemise standardi loomisel on süütuse presumptsioon ja põhjendatud kahtluse tuvastamine kaks tugisammast, millele loodavate normatiivsete aktide konstruktsioon toetub.[189]

Läänemaailmas väljendub riigivõim seadustes, mis on ülimuslikud kõigi indiviidide suhtes ning süütuse presumptsioon on lisakaitse üksikisikule riigi omavoli eest. Süütuse presumptsioon

[185] Д. Н. Ушакова. Толковый словарь русского языка. Том 3. Москва 1994, lk 735.
[186] С. М. Локшина. Краткий словарь иностранных слов. 6-е изд. Москва 1978, lk 218.
[187] P. Roberts, A. Zuckerman. Criminal Evidence. Oxford: Oxford University Press 2004, lk 340.
[188] Roberts/Zuckerman, lk 341, 342.
[189] Roberts/Zuckerman, lk 347, 348.

tähistab inimeste üldist võrdsust ehk inimõigust, mis tuleneb sellest, et ollakse inimesena sündinud.[190]

Viimase kolmekümne aasta jooksul on läbi kirjanduse, filmide ja televisiooni ühekülgselt levitatud ning loodud arusaama, et süüdistuse esitamine võib ühtlasi tähendada ka seda, et isik on teo toime pannud. Ühiskonnal on lihtne loobuda süütuse presumptsioonist ning uskuda süüdistuse esitajaid. Lihtsam on mitte analüüsida kahtlusaluste motiive, vaid leida võimalike kahtlusaluste hulgast isik, kes olemasolevate asjaolude alusel tundub kõige rohkem süüdi olevat. Ülejäänud veenvate alibitega isikud välistatakse antud valikute hulgast.[191]

## 3.1 Ajalooline taust ja sisustamine tänapäeval

Ajalooliselt on süütuse presumptsiooni käsitletud kui tõendamise reeglit. Õiguskeskkond loob kuriteo asjaolude tuvastamisele piirangud, mis on seotud nii tõendite kogumise, kui ka kriminaalmenetluses kahtlustatava suhtes kohaldavate sunnivahendite määramise osas.[192]

Süütuse presumptsiooni esmaseks allikaks peetakse rooma juristide reeglit „*praesumptio boni viri*“ ehk süüdistatavat ei saa kohus süüdi pidada enne, kuni ei ole tõendatud vastupidist.[193] Selle reegli arendamisel formuleeriti 3. sajandil pKr printsiip „*ei incumbit probatio qui dicit, non qui negat; cum per rerum naturam factum, negatis probation nulla sint*“ – tõendama peab see pool, kes teo toimumist kinnitab, mitte see kes eitab, kuna eituse tõendeid ei pea looma.[194] Antud reegel kehtib ka tänases tsiviilkohtumenetluses, kus nõude alust peab tõendama hageja, mitte kostja. Antud põhimõte on kasutuses kriminaalmenetluses, kus tõendamisvajadus asetseb süüdistajal ning süüdistatav ei ole kohustatud enda süütust tõendama.

Rooma õiguses oli süütuse presumptsiooni printsiip universaalne ehk see oli rakendatav nii tsiviil- kui ka kriminaalprotsessides. Klassikalisel perioodil (umbes 140 eKr – 3. sajandi lõpp pKr) laienes printsiibi kasutamine ka eraõiguslikele vaidlustele. Seda kinnitab XII tahvli

[190] J. Saar. Õiguskultuur ja kuritegevuse kontroll. Juridica 2013/I, lk 59.
[191] C. A. Corcos. Prosecutors, prejudices and justice. Observations on Presuming Innocence in Popular Culture and Law. University of Toledo law review. Louisiana State University Law Centre, Vol. 34, 2003, lk 795.
[192] Kergandberg/Sillaots, lk 14.
[193] А. М. Ларин. Презумпции Невиновности. Москва: Наука, 1982, lk 12.
[194] А. М. Ларин, Е. И. Темнов. Латинские Юридические Изречения. Москва, Юрист, 1996, lk 144.

seaduse tekstide analüüs, kus sisaldusid mõningad süütuse presumptsiooni sätted.[195] Eelnevat toetab ka asjaolu, et samal ajavahemikul toimusid muudatused vastutuse institutsiooni sisustamisel kahju tekitamise osas. Sellised tegevused nagu vargus, rööv, kehaliste vigastuste tekitamine ja laim viidi tsiviilprotsessist üle kriminaalprotsessi.[196] Süütuse presumptsioon tagab selle, et isiku süüd ei eeldata, vaid see tuleneb tõenditest, mis on kokku kogutud ning mille põhjal saab järeldada, et isik võib olla seotud teo toimepanemisega.

Süütuse presumptsiooni üheks autoriks peavad osad õigusteadlased Vana-Kreeka oraator Demosthenest, kes väljendas enda kõnes, et seadus nimetab tapjaks ainult seda, kelle kohta on tõendeid, et ta selle toime pani. Tapjaks ei tohi kedagi pidada senikaua, kuni tema süü ei ole tõendatud ja ta pole kohtu poolt süüdi mõistetud.[197] Demosthenese definitsiooni aga ei kirjutatud ühtegi seadusesse ning see jäi vaid oraatori üheks arvamuseks paljude hulgast. Samas, kui tänapäeval kirjeldatakse ja defineeritakse süütuse presumptsiooni, siis on kasutusel just tema sõnastatud printsiip.

Süütuse presumptsioon, kui õiguslik konstruktsioon, sõnastati esmakordselt 18. sajandil Itaalia juristi Cesare Beccaria poolt, kes esines piinamiste vastastes kriminaalprotsessides. 1764. aastal valmis tema teos kuritegudest ja karistusest, kus oli sõnastatud, et kedagi ei tohi nimetada kurjategijaks seni, kuni tema kohta ei ole jõustunud süüdimõistev kohtuotsus. Ühiskond ei saa jätta süüdistatavat ilma kaitseta seni, kuni ei ole otsustatud, et isik on teo ka toime pannud.[198]

Laiema tähenduse omandas süütuse presumptsioon siis, kui see kajastati Prantsusmaal inimese ja kodaniku õiguste 1789. aasta deklaratsioonis.[199] Osa õigusteadlasi on senini seisukohal, et just Prantsusmaa deklaratsioon ongi esmaseks õigusallikaks, kus süütuse presumptsiooni printsiip esmakordselt legaliseeriti. Samas, nagu eelnevalt on välja toodud, oli süütuse presumptsiooni printsiip kasutusel ka juba varasemalt. Esimeseks õigusallikaks, kus printsiip oli kehtestatud, võib lugeda Inglismaa kuninga poolt 1215. aastal välja antud õigusakti *Magna Charta Libertatum*, mille § 39 märkis, et ükski vaba inimene ei saa olla kinni peetud või

[195] В. А. Томсинов. Хрестоматия по истории государства и права зарубежных стран (Древность и Средние века). Москва: Зерцало, 1999, lk 136.
[196] З. М. Черниловский. Всеобщая история государства и права. Arvutivõrgus: http://www.gumer.info/bibliotek_Buks/Pravo/Chernil/ (10.01.2017).
[197] Г. Ю. Семигин. Антология мировой политической мысли. Том 1. Москва 1999, lk 202-203.
[198] Ч. Беккариа. О Преступлениях и наказаниях. Москва 2009, lk 108.
[199] U. Lõhmus 2014, lk 59.

paigutatud vanglasse ilma seaduse alusel tehtud kohtuotsuseta.[200] Seega saab välja tuua, et süütuse presumptsiooni printsiip oli normatiivselt reguleeritud ning kasutusel Inglismaa õiguses juba enne Prantsusmaal vastuvõetud inimese ja kodaniku õiguste 1789. aasta deklaratsiooni.

Kui enamustes Euroopa riikide karistusõiguses kohaldati süütuse presumptsiooni põhimõtteid, siis erandiks oli 16.-18. sajanditel Saksamaa karistusseadustik *Constitutio Criminalis Carolina*, mille sätete kohaselt pidi süüdistatav ise oma süüd tõendama.[201]

Tänapäeval tunnistavad süütuse presumptsiooni kõik olulised rahvusvahelised inimõiguste dokumendid. Ühinenud Rahvaste Organisatsiooni (edaspidi „ÜRO“) 1948. aasta inimõiguste ülddeklaratsiooni artiklis 11 on märgitud, et iga inimest, keda süüdistatakse mingis karistatavas teos, käsitletakse süütuna seni, kuni tema süü ei ole seaduse kohaselt tõendatud. Ehk kuni tema süü kindlakstegemiseni seaduslikus korras avalikul kohtulikul arutamisel, kus tal on tagatud kõik võimalused enda kaitseks.[202] ÜRO kodaniku- ja poliitiliste õiguste rahvusvahelise pakti artikli 14 lg 2, EIÕK artikli 6 lg 2 ja harta artikli 48 lg 1 sõnastused on sarnased. Ehk iga süüdistatavat peetakse süütuks seni, kuni tema süü ei ole seaduse kohaselt tõendatud. EV PS sõnastab süütuse presumptsiooni mõnevõrra erinevalt. PS § 22 lg 1 järgi ei tohi kedagi käsitada kuriteos süüdiolevana enne, kui tema vastu on jõustunud süüdimõistev kohtuotsus. Seda sõnastust kordab ka KrMS § 7 lg1.[203]

Süütuse presumptsioon on põhiõigus, mis on sätestatud inimõiguste ja põhivabaduste kaitse Euroopa konventsioonis ning hartas. EL-i lepingu artiklis 6 sätestatakse, et liit austab inimõiguste ja põhivabaduste kaitse Euroopa konventsiooniga tagatud ning liikmesriikide ühesugustest põhiseaduslikest tavadest tulenevaid põhiõigusi.[204] Näiteks 1993. aasta seisuga oli süütuse presumptsioon defineeritud enam kui 67 riigi põhiseaduses.[205]

---

[200] Д. М. Петрушевский. Великая хартия вольностей и конституционная борьба в английском обществе во второй половине XIII века. Москва: Сабашниковы, 1915, lk 17-23.
[201] Inimeste ja kodanikuõiguste deklaratsioon 1789. Arvutivõrgus: http://www.concourt.am/hr/rus/un/6_5.htm (10.01.2017).
[202] E. Truuväli, jt., lk 225, 227.
[203] U. Lõhmus 2014, lk 60.
[204] Roheline Raamat – Süütuse presumptsioon. Euroopa Komisjon. Brüssel, 26. aprill 2006. Arvutivõrgus: http://eur-lex.europa.eu/legal-content/ET/TXT/HTML/?uri=CELEX:52006DC0174&from=EN (12.02.2017).
[205] J. D. Jackson, S. J. Summers, The Internationalisation of Criminal Evidence Beyond the Common Law and Civil Law Traditions. UK: Cambridge University Press 2012, lk 199.

Süütuse presumptsioon on kaalukas õiguslik tugisammas individuaalsete õiguste ja õigluse tagamisel kriminaalmenetluses. Presumptsiooni kui õigusliku faktiga opereeritakse igas õiguslikus süsteemis. Euroopa Kohus on loonud kaks printsiipi, mis tasakaalustavad teineteist – ühelt poolt ei ole Euroopa inimõiguste kontekstis süütuse presumptsioon absoluutne õigus, samas aga tagab kohus siseriiklikus õiguses piisava järelvalvetaseme süütuse presumptsiooni kasutuse osas.[206] Eeltoodust tulenevalt saab järeldada, et süütuse presumptsioonist on käesolevaks hetkeks kujunenud üks olulisi menetlusõiguslikke kaitsemeetmeid, mis tagab indiviidi võrdse kohtlemise menetluse ja kohtupidamise kontekstis. Menetlust teostav asutus peab hindama nii süüstavaid kui ka õigustavaid tõendeid ning välistama selle, et isikut ei oleks võimalik ennatlikult esmaste tõendite pinnalt süüdiolevana käsitleda.

Süütuse presumptsiooni eesmärgiks on tagada, et karistusõigust ei kuritarvitataks ja isiku süüdimõistmiseks oleksid kehtestatud riiklikud normid, mis kindlustaksid, et kedagi ei käsitletaks süüdiolevana enne jõustunud kohtuotsust. Kuritegelikkust saab defineerida üksnes teatud kultuuri- ja ühiskonnasuhetes, sest õigusnorm kujuneb, toimib ja muutub ühiskonna tekkimise, olemise ning arenemise ajaloolises protsessis[207]. Kriminaalmenetluse kontekstis peavad normid tagama ühiskonna põhiväärtuste kaitse, mille üheks alustalaks on ka süütuse presumptsioon.

Õiguses otsivad inimesed individuaalselt või kollektiivselt reegleid, nõudeid ja soove, mis oleksid neile sobivad.[208] Ühiskonna seisukohalt on karistusõiguse näol tegemist sotsiaalsete normidega, mis on suunatud ühiskonna põhiväärtuste kaitsele ning neid väärtusi kõige tõsisemalt kahjustavate tegude – süütegude – ärahoidmisele ja tõkestamisele.[209] Sama kaua, kui on eksisteerinud inimkond ja inimsuhted, on pidevalt arenenud ka sotsiaalse koosluse negatiivne külg – kuritegevus.[210] Iga ühiskond kujutab endast inimkooslust, mille stabiilseks arenemiseks on vaja korda, normaalseid elutingimus.[211]

Õigust on kontseptuaalselt kujutatud kui neutraalset regulatsiooni instrumenti, mis on vahendiks nii valitsuste kontrollimiseks, kui ka instrumendiks, et limiteerida riigi õigusi luues

[206] Roberts/Zuckerman, lk 384-385.
[207] E. Raska. Õiguse apoloogia: sissejuhatus regulatsiooni sotsioloogiasse. Tartu: Fontese Kirjastus 2004, lk 22.
[208] M. Deflem. Sociology of Law. Cambridge: Cambridge University Press 2008, lk 102.
[209] J. Sootak. Karistusõigus: üldosa. Tallinn: Juura 2010, lk 34.
[210] I. Tammelo. Õiglus ja Hool. Tartu: Ilmamaa 2006, lk 15.
[211] J. Sootak. Sanktsiooniõigus: karistusõiguslikud regulatsioonid ja nende kohaldamine. Tallinn: Juura 2007, lk 13.

seeläbi alused õigusliku ootuse kujunemiseks kodanike hulgas. Tehnoloogiat aga on kujutatud kui neutraalset instrumenti jõudmaks teatud tulemini. Tegemist on autonoomse, väljaspool inimeste kontrolli oleva instrumendiga, mis võib tekitada erinevaid väljundeid olenevalt kohalikest faktoritest.[212]

Seoses tehnoloogia arenguga on nähtavalt muutunud süütuse presumptsiooni sisustamine kriminaalmenetluse eelses faasis ja selle läbiviimise käigus. Muutus on seotud andmeside jälgimise laialdasema kasutamisega ning see on endaga kaasa toonud uued trendid kriminaalõiguses.[213] Olemasolevaid andmeid saavad õiguskaitseasutused kasutada mitmel eesmärgil:[214]

- reaktiivselt – andmeid kasutatakse näiteks uurimisel ja vastutusele võtmisel. Selleks, et õiguskaitseasutustel oleks võimalus ajas piisavalt tagasi minna, peab õiguskaitseasutustel olema võimalik säilitada andmeid piisavalt pika aja jooksul;
- reaalajas – andmeid kasutatakse kuriteo ärahoidmiseks, isikute jälgimiseks või vahistamiseks;
- proaktiivselt – andmeid kasutatakse hindamiskriteeriumide analüüsimisel ja koostamisel.

Tulenevalt autori erialasest kogemusest ja tegevusvaldkonnast saab tänasel hetkel tuua välja kaks peamist trendi – suurenenud on julgeoleku- ja politseiasutuste võimekused andmeside jälgimisega seotud toimingute läbiviimisel ning levib suundumus, et kriminaalmenetluses kasutatakse rohkem proaktiivseid meetmeid. Seoses eelpooltooduga on märkimisväärselt muutunud ka julgeoleku- ja politseiasutuste poolt kasutatavad uurimismeetodid, mis põhinevad üha enam spetsiifilisel jälgimistehnikatel, andmebaaside põhistel otsingutel ja profileerimisel. Sellega seonduvalt on kriminaalluure muutunud kriminaalmenetluse keskseks osaks. See on endaga kaasa toonud ohu, kus potentsiaalseks kuriteo toimepanijaks võidakse lugeda igaühte ning seda sõltumata isiku osas kehtivast süütuse presumptsiooni põhimõttest.[215] Isikute

[212] M. Hildebrandt. Criminal Law and Technology in A Data-Driven Society. The Oxford Handbook of Criminal Law. Oxford: Oxford University Press 2014, lk 175.
[213] A. Galetta. The changing nature of the presumption of innocence in today's surveillance societies: rewrite human rights or regulate the use of surveillance technologies? European Journal of Law and Technology, Vol. 4, 2013, No 2, lk 3, 4. Arvutivõrgus: http://ejlt.org/article/view/221/377 (11.02.2017).
[214] Euroopa Parlamendi ja Nõukogu direktiiv 2011/0023 (COD), 02. veebruar 2011, mis käsitleb broneeringuinfo kasutamist terroriaktide ja raskete kuritegude ennetamiseks, avastamiseks, uurimiseks ja nende eest vastutusele võtmiseks. Arvutivõrgus: http://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX%3A52011PC0032 (26.04.2017).
[215] A. Galetta, lk 3, 4.

profileerimist võidakse läbi viia algoritmide põhise info alusel, mistõttu võib see kaasa tuua süütuse presumptsiooni muutumise süüdiolemise presumptsiooniks.[216] Seda võimaldab julgeoleku- ja politseiasutuste juurdepääs erinevatele andmekogudele, milles olevaid avalikke andmeid koondades on võimalik kasutajad profileerida.[217] Profileerimise käigus saadav informatsioon aga ei pruugi olla nii usaldusväärne kui füüsilised tõendid, kuna informatsiooni pinnalt järeldusotsuste tegemine nõuab asjakohase konteksti sisustamist ning eeldab selle sisustajalt vajalikke teadmiste ja oskuste olemasolu.

Süütuse presumptsiooni printsiip on erinevates õigussüsteemides väga tihedalt seotud kehtiva tõendamisstandardiga, mis peab tagama minimaalsed alused, et nende pinnalt oleks võimalik süüdimõistvaid otsuseid teha. Selleks peab süüdistaja tõendama põhjendatud kahtluse olemasolu, mis on iga süüdistuse aluseks ning kõrvaldamata kahtlust tuleb tõlgendata süüdistatava kasuks.[218]

Õiglase kohtuasja tagavad printsiibid nagu süütuse presumptsioon, kohtu sõltumatus, mõlema poole ehk nii kaitsja, kui süüdistaja võrdsed võimalused tõendeid esitada ning sisemine ja välimine läbipaistvus otsuste kujundamisel.[219] Suurandmete ajastul võivad need printsiibid seoses andmete kasutamise, analüüsi ja nende pinnalt otsuste kujundamisega muutuda. Süütuse presumptsioon, kui õiglase kohtupidamise alus, võib seeläbi kõrvale kalduda võrdse kohtlemise põhimõttest, mis on õiglase kohtuasja arutamise aluseks.

Kokkuvõtvalt käsitletakse süütuse presumptsiooni õiguses kui ühte põhiõigustest, mis on tugevalt mõjutatud nii moraalsetest, sotsiaalsetest kui ka poliitilistest arusaamadest. Süütuse presumptsiooni sisustamine toimub läbi asitõendite põhise kaitsemeetmete kasutamise, mis peavad tagama selle, et inimest ei loetaks süüdi olevaks enne, kui tema süü on tõendatud.

## 3.2 Süütuse presumptsioon kui tagatis õiglasele kohtupidamisele

Platon ja Celsus on sõnastanud põhimõtte, mille kohaselt peab õiguse sisuks peab olema õiglus. Professor Eduard Raska on käsitlenud õigust kui väärtust, mida iseloomustab sotsiaalsel alusel

[216] M. Hildebrandt 2014, lk 184.
[217] E-teenused kui infosüsteem. Kokkuvõte: E-teenusele esitatavad nõuded. Arvutivõrgus: http://e-teenus.weebly.com/kokkuvotildete.html (26.04.2017).
[218] A. Galetta, lk 4.
[219] M. Hildebrandt 2014, lk 186.

inimeste koostöö, luues solidaarsuse põhiselt toimiva ühiskonna, kus iga indiviid ühiskonna osana tunnetab lubatut ja lubamatut ning kus tekivad õiguspärased ootused ja õiguskuulekuse raamid.[220] Üks varasemaid inimõigusi on õigus nõuda kohtu kaudu õigluse saavutamist.[221] Tänapäeval peetakse aga üha rohkem selle peamiseks eesmärgiks õigusrahu säilitamist.[222]

Süütuse presumptsioon osutab viisile, kuidas tuleb kohelda isikut, keda pole veel süüdi mõistetud[223]. Õigusteoreetiliselt kehtib õigusruumis arusaam, et igaüht loetakse süütuks seni, kuni ei ole tõendatud vastupidist[224]. Isiku kohtlemisel tuleb arvestada võimalusega, et kohus ei pruugi teda süüdi mõista. See võimalus tuleneb tõsiasjast, et faktiliselt kuriteo toimepanija võib osutuda tõendite järgi süütuks, kuna tema vastu esitatud tõendid ei ole kohtu jaoks tema süüdimõistmiseks piisavad. Kriminaalmenetluse keskseks osaks on tõendamine, sest nii süüdimõistev kui ka õigeksmõistev kohtuotsus peavad tuginema tõenditele.[225] Kriminaalmenetluses mõeldakse tõendite kogumise staadiumi all kuriteojälgede leidmise faasi, milliste hindamine on tunnetustegevuse väljendus, millele antakse karistusõiguslik hinnang.[226] Olles ausa kohtupidamise osaks, sisustatakse süütuse presumptsiooni läbi tõendite kujundamise standardi, tagades et kõik indiviidid oleksid kaitstud võimalike alusetute riigipoolsete sunnimeetmete rakendamise eest.[227]

EIÕK-is on süütuse presumptsioon õiglase kohtumenetluse üheks aluseks. Seega võiks eeldada, et süütuse presumptsioon laieneb vaid kohtumenetlusele. Ometi on EIK laiendanud EIÕK artikli 6 kaitseala ka väljapoole kohtumenetlust. Hartas pole süütuse presumptsioon paigutatud õiglast kohtulikku arutamist sätestavasse artiklisse 47, vaid koos kaitseõigusega artiklisse 48. Mõlemad artiklid kuuluvad aga jaotisesse, mille pealkiri on õigusemõistmine.[228]

EIÕK-i praktika kohaselt ei tohiks enne süüdimõistvat kohtuotsust olla ühtki õiguslikku hinnangut isiku süü kohta. Näiteks süüdistatavat ei tohiks pidada eelvangistuses, välja arvatud kaalukatel põhjustel. Kui isikut peetakse eelvangistuses, peaksid tema eelvangistuse tingimused

[220] E. Raska. Olemise õigus. Tallinn: Sisekaitseakadeemia 2010, lk 5, 7.
[221] H. J. Uibopuu. Inimõiguste rahvusvaheline kaitse – käsiraamat ja õpik ülikoolidele. Tallinn; Saltzburg: Juura 2000, lk 7.
[222] E. Kergandberg. Kriminaalmenetlus kui kullakaevandus. Juridica 2016/II, lk 104.
[223] U. Lõhmus. Põhiõigustest kriminaalmenetluses. Tallinn: Juura 2012, lk 40.
[224] Kerr/Earle, lk 70.
[225] U. Lõhmus 2012, lk 40.
[226] E. Kergandberg, P. Pikamäe. Kriminaalmenetluse seadustik: Kommenteeritud väljaanne. Tallinn: Juura 2012, lk 199.
[227] Jackson/Summers, lk 199.
[228] U. Lõhmus 2014, lk 59, 61.

olema kooskõlas tema eeldatava süütuks olemisega. Tema süü tõendamise kohustus on riigil ja kahtlused tõlgendatakse süüdistatava kasuks. Isikul peab olema võimalus keelduda küsimustele vastamast. Üldiselt tuleb eeldada, et süüdistatav ei pea andma iseenda vastu tunnistusi. Süüdistatava vara ei tohi konfiskeerida ilma nõuetekohase menetluseta.[229]

Kooskõlas EV PS § 22 lg 2 ja KrMS § 7 lg 2 sätestatuga ei pea keegi kriminaalmenetluses tõendama oma süütust. Juhul kui kohtualune otsustab end aktiivselt kaitsta peab ta, kas ise esitama tõendeid oma väidete õigsuse kinnitamiseks või vähemalt looma menetlejale reaalse võimaluse nende väidete kontrollimiseks.[230] RKKK arvamuse kohaselt esineb teatud juhtudel ka pööratud tõendamiskoormus, kus mingite asjaolude tõendamise kohustus võib lasuda ka süüdistataval. Näiteks raamatupidamiskohustuse rikkumine võib teatud juhtudel tähendada, et süüdistatav, kes tugineb teatud maksunduslikult olulistele faktidele, peab neid ise tõendama. KrMS § 7 lg 2 ja 3 ning KrMS § 22 lg 2 sisalduvate süütuse presumptsiooni lisalausetes sisalduvate õiguste riive kindlapiirilises võimalikkuses (nt teatud piiratud juhtudel nn ümberpööratud tõendamiskoormises) ei ole põhjust kahelda.[231] Süütuse presumptsiooni riivena ei saa käsitada süüteomenetlust ennast: selle alustamist, menetluslike sunnivahendite kohaldamist, süüdistusakti koostamist, isiku kohtu alla andmist jne.[232]

Eesti kontekstis räägib PS § 22 kuriteost, kuid EIÕK järgi on kuriteo mõistel autonoomne tähendus. Teo võib tunnistada kuriteoks ka siis, kui see riigisisese õiguse järgi on klassifitseeritud väärteoks või distsiplinaarüleastumiseks. Samuti kasutatakse seda kaitserelvana ka olukordades, kus süüteomenetlust pole veel alustatud.[233]

Süütuse presumptsiooni kaitseala saab tõlgendada kitsalt või laialt. Kitsa ja laia tõlgenduse erinevus seisneb selles, et kitsa tõlgenduse järgi on süüdistataval õigus eeldada, et teda peetakse süütuks üksnes kohtumenetluse ajal kuni otsuse langetamiseni. Süütuse presumptsiooni kaitseala laia tõlgenduse järgi laieneb süütuse presumptsiooni mõju kaugemale kui kitsa tõlgenduse järgi. Näiteks ei lõpe mõju süüdimõistmisega esimese astme kohtus vaid lõpliku jõustuva otsusega.[234]

---

[229] Roheline Raamat – Süütuse presumptsioon, p 2.
[230] U. Lõhmus 2014, lk 61, 63.
[231] RKKKo 3-1-1-70-11 p 18.1. Arvutivõrgus: http://www.nc.ee/?id=11&tekst=222539134 (14.01.2017).
[232] RKKKo 3-1-1-94-14e p 6. Arvutivõrgus: http://www.nc.ee/?id=11&tekst=222578518 (22.03.2017).
[233] U. Lõhmus 2014, lk 59, 61.
[234] U. Lõhmus 2014, lk 65.

Süütuse presumptsiooni tavatsetakse paigutada nii-öelda kõigi ja igaühe põhiõiguste hulka. Samas hõlmab antud põhiõiguse isikuline kaitseala eeskätt vaid füüsilisi isikuid, kelle süüteoasja menetletakse ehk nii kahtlustatavat, süüdistatavat ja kohtualust kriminaalmenetluses, kui ka menetlusalust isikut väärteomenetluses. Arvestades, et KarS-is sätestatakse juriidilise isiku kriminaalvastutuse võimalus, hõlmab süütuse presumptsiooni kaitseala PS § 9 lg 2 tulenevalt ka juriidilisi isikuid, kelle kuriteoasja menetletakse.[235]

Süütuse presumptsioon hõlmab endas ka enesesüüstamise vastast kaitset, mis tähendab nii õigust vaikida, kui õigust mitte esitada enda vastu süüstavaid tõendeid. Selles kohaldatakse maksiimi *nemo tenetur prodere seipsum* ("kedagi ei tohi sundida tunnistama enda vastu"). Süüdistatav võib keelduda küsimustele vastamisest ja tõendite andmisest. Süüdistuse esitaja peab tõendama oma juhtumi sunni- või survemeetodite abil saadud tõendeid kasutamata. Julgeoleku ja avaliku korra tagamine ei saa õigustada nende õiguste tõkestamist.[236] Kuigi sunnivahendite kasutamisega seonduv ei kuulu vahetult süütuse presumptsiooni esemelise kaitseala klassikalistesse piiridesse, tuleb sunnivahendite kohaldamisel muuhulgas arvestada ka süütuse presumptsiooniga, kui ausa kohtumenetluse osaga. Mistahes sunnivahendi kasutamine kriminaalmenetluses kujutab endast alati mingi konkreetse põhiõiguse piirangut (nt eluaseme puutumatus, isikuvabadus, kehaline puutumatus jne). Seega tuleb sunnivahendite kasutamisel arvestada põhiõiguste piiramise üldiste tingimustega, kus süütuse presumptsioon toimiks omalaadse täiendava garantiina riigivõimu poolse ülemäärase toime keelu väljendusena.[237]

Süütuse presumptsiooni esemeline kaitseala hõlmab oma terviklikkuses süütegude menetlust. Valitseva arusaama kohaselt ei laiene süütuse presumptsiooni toime eraisikute käitumisele ning seega ei loeta üldiselt süütuse presumptsiooni universaalselt sobivaks vahendiks ühiskonnas viisaka ning üksteisest lugupidava käitumise tagamisel. Levimas on arusaam, et süüteomenetluse kajastamisel peab meedia arvestama süütuse presumptsiooniga. Kellegi käsitlemine kurjategijana ei tohi meedia vahendusel enne süüdimõistvat kohtuotsust aset leida.[238]

[235] Kergandberg/Sillaots, lk 54, 55.
[236] Roheline Raamat – Süütuse presumptsioon, p 2.4.
[237] Kergandberg/Sillaots, lk 54.
[238] Ü. Madise, jt. Eesti Vabariigi Põhiseadus: kommenteeritud väljaanne. Tallinn: Juura 2012, lk 287.

Kokkuvõtvalt on süütuse presumptsioon süüdistatava menetlusõiguslik kaitsevahend riigi sunnivõimu vastu, et hoida ära ekslikke süüdimõistmisi ning säilitada kriminaalkohtusüsteemi legitiimsus. Süütuse presumptsioon on poliitilise kõlbelisuse toetaja, mis aitab säilitada riigi ja kodanike vahelist usaldust.[239]

## 3.3 Põhjendatud kahtluse tuvastamine kriminaalmenetluses

Kriminaalmenetluse normid peavad ühelt poolt andma võimaluse teha kindlaks süüdistatava süü ning aitama rakendada riiklikku karistusnõuet. Teisalt peab vastav õiguslik regulatsioon tagama, et süüdi ei mõistetaks süütut isikut ning et tema õigusi piirataks menetluse käigus nii vähe kui võimalik. Samas konflikt, ühelt poolt avalike huvide ning teiselt poolt kahtlustatava ja süüdistatava erahuvide vahel, jääb teatud määral alati vältimatuks.[240]

Kohtupraktikas ja teoorias juhinduvad Mandri-Euroopa riigid standardist, et süüdistatava süü peab olema tõendatud väljaspool põhjendatud kahtlust. Süü on tõendatud väljaspool põhjendatud kahtlust, kui kriminaalasja tõendid tekitavad veendumuse kuriteo toimepanemise osas.[241] Kellegi kuriteos süüdiolek ning kurjategijaks nimetamine peab alati olema tõendatud väljaspool põhjendatud kahtlust ehk see peab olema jõustunud süüdimõistva kohtuotsusega.[242]

Põhjendatud kahtluse olemasolu on vajalik, et julgeoleku- ja politseiasutused saaksid kahtlusaluse vahistada. Toiminguid saab kriminaalmenetluses läbi viia ka juhul, kui on olemas põhjendatud kahtlus, et kuritegu ollakse ette valmistamas.[243] Üldjuhul kujundavad ametnikud põhjendatud kahtluse välja läbi informatsiooni kogumise ja tegevuste jälgimise. Võimalik kahtlus individualiseeritakse inimese osas konkreetses kohas, kus tegevus toimub. Põhjendatud kuriteokahtlus on vahistamise, kui eeskätt kahe olulise põhiõiguse – üldise vabadusõiguse ja süütuse presumptsiooni – kõige tõsisema riive lubatavuse absoluutne eeltingimus.[244] Põhjendatud kuriteokahtlus vahistamise eeldusena tähendab seda, et vahistamine ei tohi teenida kriminaalmenetluse väliseid eesmärke[245].

---

[239] U. Lõhmus 2014, lk 61.
[240] M. Sillaots. Kaitsja võimalikust rollist ja seisundist Eesti tulevases kriminaalmenetluses. Juridica 2000/II, lk 83.
[241] U. Lõhmus 2014, lk 64.
[242] R. Maruste. Konstitutsionalism ning põhiõiguste ja –vabaduste kaitse. Tallinn: Juura 2004, lk 385.
[243] D. J. Steinbock, lk 28.
[244] N. Aas. Riigi peaprokuröri ülevaade Riigikogu põhiseaduskomisjonile seadusega prokuratuurile pandud ülesannete täitmise kohta 2010. aastal. Tallinn 2011, lk 2.
[245] N. Aas, lk 2.

Kuni suurandmete kasutusele võtmisele toimus põhjendatud kahtluse kujunemine läbi piiratud andmete olemasolu. Tänapäeval võimaldab aga suurandmete kasutamine kujundada otsuseid andmete kogumite põhjal. Kogutud andmete kaudu teostatavate analüüside pinnalt on võimalik teha järeldusotsuseid, pakkudes välja võimalikke isikuid, kes võiksid kuritegude toime panemisega seotud olla. Sellise tegevusega võidakse aga rikkuda süütuse presumptsiooni põhimõtteid, sh välistada põhjendatud kahtluse olemasolu. Isikud võivad sattuda menetluseelsesse teabe kogumise huvisfääri tulenevalt eelnevalt kogutud andmetest, mis ei tähenda, et nad oleksid olnud uuritaval ajahetkel kuritegude toime panemisega seotud.

Näiteks USA politsei, uurides röövimiste seeriat mingis kindlas piirkonnas, saab teostada patrullauto arvutist eelnevalt vahistatud isikute kontrolle. Auto arvutis oleva näotuvastus tarkvara abil skaneeritakse tänaval liikuvaid inimesi ja võrreldakse neid andmebaasis olemasolevate isikutega. Juhul kui andmebaas tuvastab vaste, siis kuvatakse ekraanile isiku andmed ning kogu olemasolev temaga seotud informatsioon, sh info temaga seotud kuritegeliku taustaga isikute ehk võimalike kaasosaliste kohta. Antud info põhjal on politseil olemas alus isiku kontrollimiseks ja kinni pidamiseks. Lisaks, kui kahtlustatava sõiduk on varustatud GPS seadmega, siis on võimalik tuvastada tema viimased asukohad ning vaadelda sõiduki marsruuti. Samuti on võimalik sõiduki liikumist vaadelda läbi numbrimärkide süsteemi tuvastamaks, kas kahtlusalune on külastanud näiteks röövimiste järgselt pandimaju vms. Antud info põhjal võib aga politsei teha ka valesid otsuseid, kuna antud uuritava kuriteoga seoses ei pruugi isikul, hoolimata oma kriminaalsest taustast, olla mingit seost.[246]

EV-s on politsei sõidukites kasutusel e-Politsei lahendus, mis tagab auto arvuti kaudu juurdepääsu järgmistele registritele:[247]

- liiklusregister – andmed sõidukite, nende omanike ja kasutajate ning juhilubade kohta;
- liikluskindlusturegister – andmed kehtivate liikluskindlustuse lepingute kohta;
- rahvastikuregister – isikuandmed, kontaktandmed, sugulus teiste isikutega;
- haigekassa registrid – isikute kontaktandmed;
- kinnisturegister – andmed kinnisvara ja nende omanike kohta;
- karistusregister – andmed karistatud isikute kohta;
- kinnipeeturegister – andmed arreteeritud ja vangistatud isikute kohta, nende asukoht;

[246] A. G. Ferguson, lk 330.
[247] Kogu riigi infosüsteem ühes autos. Riigi infosüsteemi teejuht: Eesti IT-edulood. Riigi Infosüsteemide Amet 2010. Arvutivõrgus: https://www.ria.ee/teejuht/eesti-it-edulood/kogu-riigi-infosusteem-uhes-autos (12.03.2017).

- relvaregister – üksikasjalikud andmed registreeritud relvade kohta;
- politsei andmebaas – andmed tagaotsitavate isikute ja sõidukite kohta.

Politsei põhiinfosüsteemi kaudu on e-politseil ligipääs mitmetele EL-i ning rahvusvahelistele andmebaasidele:[248]

- *Schengen*-i infosüsteem (SIS);
- viisainfosüsteem (VIS);
- *Interpol*-i infosüsteem;
- *Europol*-i infosüsteem;
- *EUCARIS* (Euroopa autoregistreid ühendav infosüsteem).

Ülaltoodud infotehnoloogilisi lahendusi kasutatakse liiklusjärelvalve läbiviimiseks ja avaliku korra tagamiseks. Nendega on võimalik tuvastada näiteks isikute tagaotsimisinfot, juhtimisõiguse andmeid, sõiduki andmeid, riiki sissesõidukeeldusid, viisakleebiseid ja palju muud.[249] Näiteks saab politsei auto registreerimisnumbri kaudu oletada, kas kinnipeetavas sõidukis võib olla tagaotsitav isik või isegi relv.[250]

EV kontekstis on uurimistoimingu teostamise üheks eelduseks põhjendatud kuriteokahtluse olemasolu ja toimingu tegemiseks tuleb kuriteokahtluse äratuntavust hinnata *ex ante*, mitte aga *ex post*.[251] KrMS ei sea piiranguid sellele, missuguste tõenditega saab konkreetseid tõendamiseseme asjaolusid tuvastatuks lugeda,[252] kuid põhjendatud kahtluse tekkeks peab kriminaalasjas esinema tõsiselt võetav tõenduslik alus. Kriminaalmenetluse läbiviimisel on oluline, et jälitustoimingutega oleks võimalik alustada juba põhjendatud kahtluse olemasolul. Ka Riigikohus on välja toonud, et jälitustoiminguks antud loa seaduslikkuse kontrollimisel tuleb hinnata, kas loa andmisel ja selle aluseks oleva taotluse esitamisel oli olemas põhjendatud kahtlus, et toime on pandud KrMS § 110 lg 1 sätestatud tingimustele vastav kuritegu[253]. Põhjendatud või siis ka kõrvaldamata kahtluse nõue ei tähenda seda, et kohtul tuleks isiku

[248] Kogu riigi infosüsteem ühes autos. Riigi infosüsteemi teejuht: Eesti IT-edulood. Riigi Infosüsteemide Amet 2010.
[249] BNS. Politsei võtab patrullsõidukites kasutusele uue e-politsei lahenduse. Postimees 26. juuni 2016. Arvutivõrgus: http://www.postimees.ee/3743991/politsei-votab-patrullsoidukites-kasutusele-uue-e-politsei-lahenduse (12.03.2017).
[250] Kogu riigi infosüsteem ühes autos. Riigi infosüsteemi teejuht: Eesti IT-edulood. Riigi Infosüsteemide Amet 2010.
[251] RKKKo 3-1-1-93-15 p 60. Arvutivõrgus: http://www.nc.ee/?id=11&tekst=222579510 (22.03.2017).
[252] RKKKo 3-1-1-136-13 p 12. Arvutivõrgus: http://www.nc.ee/?id=11&tekst=RK/3-1-1-136-13 (22.03.2017).
[253] RKKKo 3-1-1-79-16 p 14. Arvutivõrgus: http://www.nc.ee/?id=11&tekst=222582407 (22.03.2017).

süüküsimuse käsitlemise aluseks võtta süüdistatava jaoks soodsaim versioon olukorras, kus puuduvad igasugusedki kaitseversiooni kinnitavad toetuspunktid.[254]

Süütegude menetluse aluseks saab lugeda süüteokahtlust ning süüteo asjaolude uurimist viiakse läbi vaid põhjendatud kahtluse olemasolul. Süütuse presumptsioon ja kuriteokahtlus on omavahel pöördvõrdelises seoses. Näiteks kohtuniku siseveendumuse kujunemisprotsessis muutub antud seos pidevalt ehk kuriteokahtluse tugevnemisega pöördvõrdeliselt nõrgeneb süütuse presumptsioon kuni täieliku lõppemiseni.[255]

Autori arvates on kriminaalmenetluse kontekstis mõistetav, et raskete kuritegude ennetamiseks tuleb ulatusliku andmeanalüütikat ja andmekogude riskasutust teostades läbi viia nii teabehanke- kui ka jälitustoiminguid. Sealjuures tuleb arvestada, et sellised andmed on kiiresti aeguvad ja ei pruugi kontekstiga suhestuda. Samuti võib tegemist olla oletustel põhinevate masinandmetöötluse tulemitega, mille analüütiku poolne hindamine ei pruugi olla asjakohane ning konteksti arvestades vajalikul kiirusel teostatav.

Süütuse presumptsiooni tagamiseks on vajalik leida tasakaal riikliku julgeoleku ja kuritegude ennetamise õiguslikus raamistikus, et meetmete kasutamisega kaasnevad inimõiguste riiveid oleksid kasutatavad proportsionaalselt võimaliku olemasoleva ennetatava ohu suhtes. Süütuse presumptsiooni tagamiseks peab õiguslik raamistik vastama tingimusele, kus kogutud informatsiooni ja andmeid kasutatakse kuritegude avastamiseks vaid õiguslikult ettenähtud korra kohaselt, võimalikult lühikese ajaperioodi jooksul ning ainult konkreetselt tuvastatud isikute suhtes.[256]

Andmete analüüsi alusel kujundatavad võimalikud ennustusotsused peavad olema piisavalt kontrollitud ning suhestuma ka teiste võimalike kahtlust kinnitavate tõenditega. Suurandmete analüüsi kaudu kujundatavad otsused võivad olla piisavad põhjendatud kahtluse olemasolu kinnitamiseks. Samas sõltumatut kontrolli teostav institutsioon ehk kohus ei tohiks, ilma enda poolse täiendava kontrollita, anda julgeoleku- ja politseiasutustele luba teabehanke- ja jälitustoimingute läbiviimiseks, kui need tuginevad loa taotlemisel ainult andmeanalüütika ning andmekogudes sisalduval infol.

---

[254] RKKKo 3-1-1-64-16 p 11. Arvutivõrgus: http://www.nc.ee/?id=11&tekst=222582177 (22.03.2017).
[255] Kergandberg/Sillaots, lk 51.
[256] S. Mcgarvey, lk 166.

# 4. SUURANDMETE HINDAMINE, NENDE PÕHJAL TEHTUD OTSUSED JA KUJUNENUD TÕENDITE USALDUSVÄÄRSUS

On paratamatu, et kuuletutakse sellele, mis on võimsam. Õigus ilma võimuta on võimetu, võim ilma õiguseta on aga türanlik. Järelikult tuleb hoolt kanda, et see mis on õige oleks võimas ja see mis on võimas oleks õiglane.[257] Kriminaalmenetluse põhiolemuseks on teatud napi sotsiaalse ressursi jagamine ehk tegemist on riigipoolse karistusõigusliku reageeringuga toimepandud kuriteole, kus riik on menetluse läbiviimisel võimupositsioonil.[258]

## 4.1 Suurandmete töötlemisega kaasnevad mõjud isikute õigustele

Suurandmete ajastul on sihtmärgiks digitaalsed andmed. Saavutamaks otsuste kujundamiseks vajalikku täpsust on suurandmete kontseptsioon üles ehitatud kogu olemasoleva info kokku koondamisele.[259] Suurandmete kontekstis on kogu olemasoleva teabe kogumine protsess, mis võimaldab kõiki võimalike olemasolevaid infomustreid ühendada.[260]

Suurandmete kasutamine võimaldab teha ennustusotsustusi. Pikas perspektiivis võib ennustusotsuste tegemine asendada vajaduse koguda iseseisvalt tõendeid. Üha enam toimub andmete põhiste otsustuste vastuvõtmine läbi korrelatsioonide kaudu kujunevate mustrite analüüsi. Sellest tulenevalt kasutatakse aina vähem füüsilist jälgimist ja selle käigus tuvastavaid fakte ning analüüsi teostaja ehk analüütiku taju ja tema poolseid hinnanguid kogutud andmetele.[261] Eeltoodud erisus võrreldes suurandmete kasutamisega seisneb selles, et füüsilise jälgimisega seotud andmete puhul püstitati küsimus või hüpotees ning seejärel hinnati võimalikke olemasolevaid andmeid, mis võiksid kaasa aidata püstitatud küsimuse lahendamisele.[262] Suurandmed võimaldavad aga püstitatud küsimusi viia andmete juurde, saades tõendeid tehnoloogiapõhistest sisenditest. Saadavad sisendid saadakse käitumismustritel

[257] K. Linask, jt (tõlkijad). Aja jälg: Kui õiglane on õigus. Tallinn: Juura 2007, lk 5.
[258] Kergandberg/Sillaots, lk 11.
[259] M. Hu 2014, lk 780.
[260] M. Hu 2015, lk 1690, 1691.
[261] D. Frank. Privacy, Due Process and the Computational Turn: The philosophy of law meets the philosophy of technology. Routledge 2013, lk 164.
[262] M. Hu 2014, lk 780.

põhineva analüüsi, andmebaasides otsingu, statistilise modelleerimise, algoritmide, ennustava analüüsi või muude superarvuti rakenduse võimekuste ja tehisintellekti vahendite abil.[263]

Olenemata eeltoodust ei kaota suurandmed ära siiski vajadust inimeste poolt nende kontrollimisele ja ka infoallikate üle vaatamisele. Nimelt on üheks kriitiliseks aspektiks suurandmete kasutamisel otsuste vastuvõtmise tõlgendamine ning see, kes lõplikud otsused teeb. Senini, kui uurimise läbiviimiseks ei olnud andmeid piisavalt, neid oli täiendavalt liiga kallis hankida ja nad ei olnud digitaalsel kujul kättesaadavad, siis on olnud mõistetav, et otsuseid tehakse vastava valdkonna ametnike poolt nende kogemuspõhise analüüsi toel.[264]

Suurandmed võimaldavad vajadusel saavutada tulemeid ka suures koguses näiliselt tähtsusetu informatsiooni alusel. Näiteks selleks, et pakendada narkootilisi aineid on narkootikumidega kauplejal vaja plastikkotte ja kaalu. Tulirelvast tulistamiseks on vaja padruneid, autosse sissemurdmiseks on vargal vaja tööriistu. Jälgides ning analüüsides antud toodete müügiinfot on julgeoleku- ja politseiasutustel võimalik tuvastada erinevaid käitumismustrid ning identifitseerida kurjategijad, kui need vastavasisulisi oste sooritavad.[265] Sellist meetodit saab kasutada piirkondade põhiselt, milleks vaadeldakse registreeritud kuritegude toimepanemise andmeid. Analüüsides uuritavas piirkonnas toimepandud narkootiliste ainete müügikohti on võimalik seeläbi tuvastada narkootiliste ainete müügiga seotud isikuid. Tuvastamaks võimalikke seoseid võrreldakse eelpool nimetatud andmeid julgeoleku- ja politseiasutuste andmebaasides oleva infoga. Sarnaselt eeltooduga on võimalik kahtlusaluseid tuvastada tarkvara abil, mis kasutab käitumismustrite analüüsi, võrreldes saadud infot juba varasemalt kogutud andmebaasides sisalduva infoga[266].

Suurandmeid on võimalik koguda ka läbi „asjade interneti“ ja „targa kodu“ seadmete. Üheks selliseks näiteks on *Google Home* seade, mis on Internetti ühendatud ning varustatud mikrofoni ja kõlariga. See võimaldab teostada läbi nn „targa assistendi“ otsinguid häälkäskluste abil, hankides andmeid pilvelahenduste kaudu. Seadme automaatsed seadistused võivad parema teenuse kvaliteedi nimel edastada seadme kasutamise andmeid seadme tootjale. Lisaks võib

[263] M. Hu 2014, lk 802.
[264] A. McAfee, E. Brynjolfsson. Big Data: The Management Revolution. Harvard Business Review, Oktoober 2012, lk 65. Arvurivõrgus: http://www.rosebt.com/uploads/8/1/8/1/8181762/big_data_the_management_revolution.pdf (16.03.2016).
[265] A. G. Ferguson, lk 395.
[266] A. G. Ferguson, lk 331.

seade salvestada soovimatult eelsalvestatud otsingusõnade kuulmisel asukohas toimuvat.[267] Eelmainitu abil kogutavat teavet soovivad kasutada ka julgeoleku- ja politseiasutused leidmaks võimalusi näiteks salvestada ning kuulata pealt seadme asukohas toimuvat ka siis, kui seade on näiteks unerežiimis.[268] Läbi *WikiLeaks* avalikustamiste tulid välja ka USA Luure Keskagentuuri (edaspidi „CIA“) poolt kasutatavad häkkimise meetodid, millest üheks oli näiteks läbi *Samsung SmartTV* teostatav asukohamonitooring.[269]

Suurandmete alusel väljatoodud korrelatsioonid ei taga automaatselt põhjendatud kahtluse olemasolu. Selleks, et vältida vääraid andmeid peavad analüütikud vaatlema info tõenäosust. Kontrollimata info kohene seostamine isikuga võib viia erinevate eksimusteni. Näiteks on osadel inimestel nimekaim või isegi nimekaimud, mistõttu võivad nad andmebaasides olla seotud kriminaalse taustaga isikutega. Ennetav infopõhine analüüs peab kinnitama seose olemasolu info konteksti ja kahtlustatava vahel. Eeltoodust tulenevalt ei saa kohus usaldada kontrollimata assotsiatiivseid seoseid, mis on vaid algoritmide analüüsi teel loodud. Kõik esitatud andmed peavad olema põhjalikult kontrollitud ja tõendamist vajavad seosed tuvastatud.[270] Suurandmete põhjal kujundatava esialgse kahtluse kujundamisel võib tekkida probleem, et teatud isikuid võidakse olemasolevainfo põhjal kontrollimiseks järjepidevalt kinni pidada. Näiteks varasemalt kriminaalkorras karistatud isikuid võidakse kinni pidada olemasolevate andmete põhjal tekkivate seoste alusel, ilma et nad konkreetsel ajahetkel ja kohas toimuva kuriteo toimepanemisega seotud oleksid.[271]

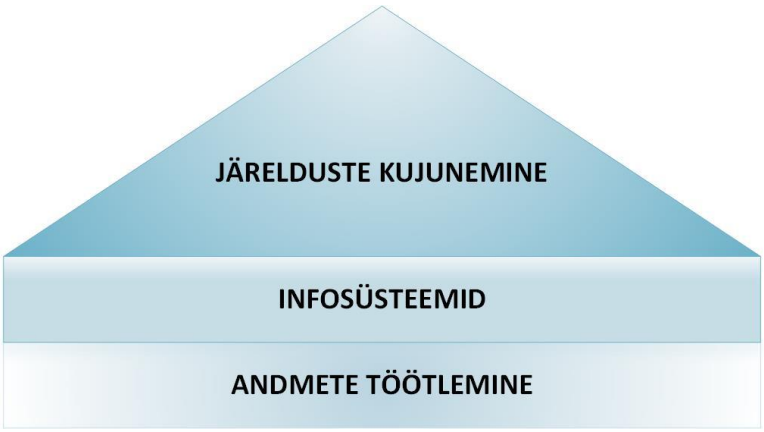
Käesoleval hetkel on suurandmed mõjutamas lääne ühiskondades aja jooksul kinnistunud õiguslikke kaitsemeetmeid nagu süütuse presumptsioon ja tõendamiskoormist väljaspool põhjendatud kahtlust. Suurandmete põhine lähenemine võimaldab kahtlusaluseid tuvastada läbi kategooriate ja algoritmide. Kui isiku kohta on julgeoleku- ja politseiasutuste andmebaasides kirje juba kord loodud, siis on sealsed andmed aluseks erinevate analüüside pinnalt teostatavate otsuste kujundamiseks. Juhul kui isik on toime pannud kuriteo, siis isegi peale seda, kui karistus

[267] F. Lardinois. Google Home brings Google´s smarts to your living room. TechCrunch, November 3, 2016. Arvutivõrgus: https://techcrunch.com/about/#about-tc (17.03.2017).
[268] B. Heater. Can your smart home be used against you in court? TechCrunch, March 12, 2017. Arvutivõrgus: https://techcrunch.com/2017/03/12/alexa-privacy/ (17.03.2017).
[269] M. Burns. Alleged CIA leak re-demonstrates the dangers of smart TVs. March 7, 2017. Arvutivõrgus: https://techcrunch.com/2017/03/07/recent-cia-leak-demonstrates-again-the-dangers-of-smart-tvs/ (17.03.2017).
[270] A. G. Ferguson, lk 409.
[271] A. G. Ferguson, lk 401.

on ära kantud või kuritegu aegunud säilib tema kohta kirje politsei hallatavates infosüsteemides. Antud informatsiooni on vajadusel võimalik edaspidiselt otsuste kujundamisel kasutada.

## 4.2 Otsuste kujunemine ning hindamine suurandmete alusel

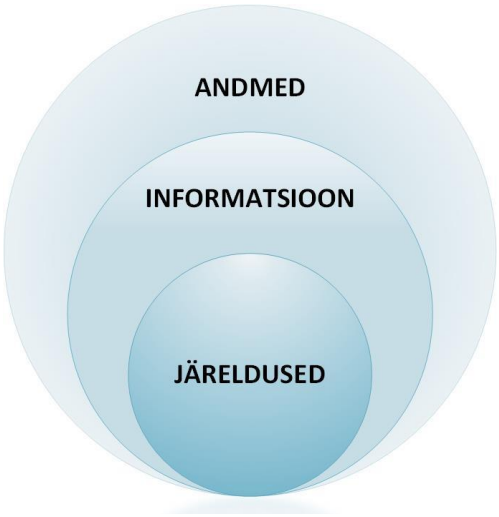
Tehnoloogia arenguga seotud info kogumine on toonud kaasa uue ajastu, millega on kaasnenud sotsiaalne transformatsioon. Selle aluseks on teistmoodi mõtlevad modernsed inimesed, kelle mõttemaailm on fundamentaalselt traditsioonilisest ühiskonnaliikmest erinev, olles sõltuvuses informatsioonist ja sellest, kuidas seda jaotatakse.[272] Toimunud arenguga on kaasnenud järjest suurem andmete töötlus, mille jaoks loodud infosüsteemid on olemasoleva infrastruktuuri aluseks. Nende alusel kujundatakse otsused ning saadavad järeldused on selle tulemiks. Järeldused tekivad aga läbi andmete töötlemise infosüsteemides (joonis 1).[273]




Joonis 1 – Seos informatsiooni ning selle töötlemisel kujunevate järelduste vahel.[274]

Järelduste maht, mille alusel otsuseid kujundatakse, moodustab andmekogumis struktureerimata suurandmetest läbi informatsiooni töötluse väiksemahulise osa ning seda illustreerib alljärgnev joonis: [275]

[272] X. Li, lk 66.
[273] X. Li, lk 67.
[274] X. Li, lk 67.
[275] X. Li, lk 67.



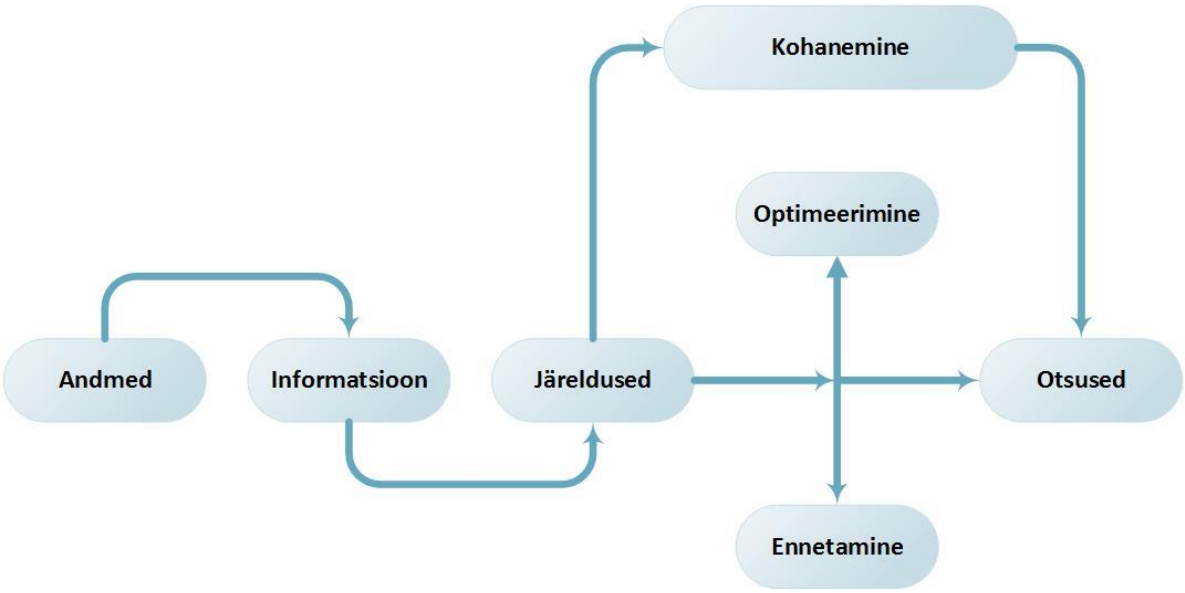

Joonis 2 – Struktureerimata andmetest vajalike järelduste kujunemine.

Informatsiooni pinnalt otsuste kujundamiseks on vajalik, et informatsioon oleks: [276]

- elektrooniline;
- digitaalne;
- töödeldav;
- automatiseeritud;
- võrku ühendatud;
- otsuste kujundamiseks töödeldud;
- kontekstis hinnatud/väärtustatud.

Andmete analüütik peab kontrollima analüüsi aluseks olevaid andmeid ning tuvastama nende päritolu ja viisi, kuidas need on analüüsiks ette valmistatud. Analüütik vastutab, et analüüsi läbiviimise käigus kasutatud andmed oleksid nende pinnalt järeldusotsuste tegemiseks kvaliteetsed. Analüütik teeb andmete kontrolli keeruliseks suurandmete struktuur, mis tuleneb erinevatest formaatidest ja allikatest, mistõttu on otsuste kujundamiseks relevantse ja vajaliku informatsiooni selekteerimine raskendatud. Näiteks on erinevad allikad sensori andmed, mobiilsed seadmed, veebipõhised rakendused, pildid, audio- ja video failid, blogid, uudised ning sotsiaalmeedia. [277] Analüüsi pinnalt teostatavate otsuste kujunemist ja hindamist illustreerib alljärgnev joonis:[278]

[276] X. Li, lk 68.
[277] M. Toivonen, lk 8.
[278] M. Toivonen, lk 8.




Joonis 3 – Andmetest otsuste kujunemise protsess.

Andmetest otsuse kujunemise protsess ei pruugi alati olla tõene. Analüütik peab indikaatoreid, andmeallikaid ning andmeanalüütika ja visualiseerimise töövahendeid valides tegema teadlikke valikuid ning puuduste esinemise korral rakendama vajalikke piiranguid andmete kasutamisel[279].

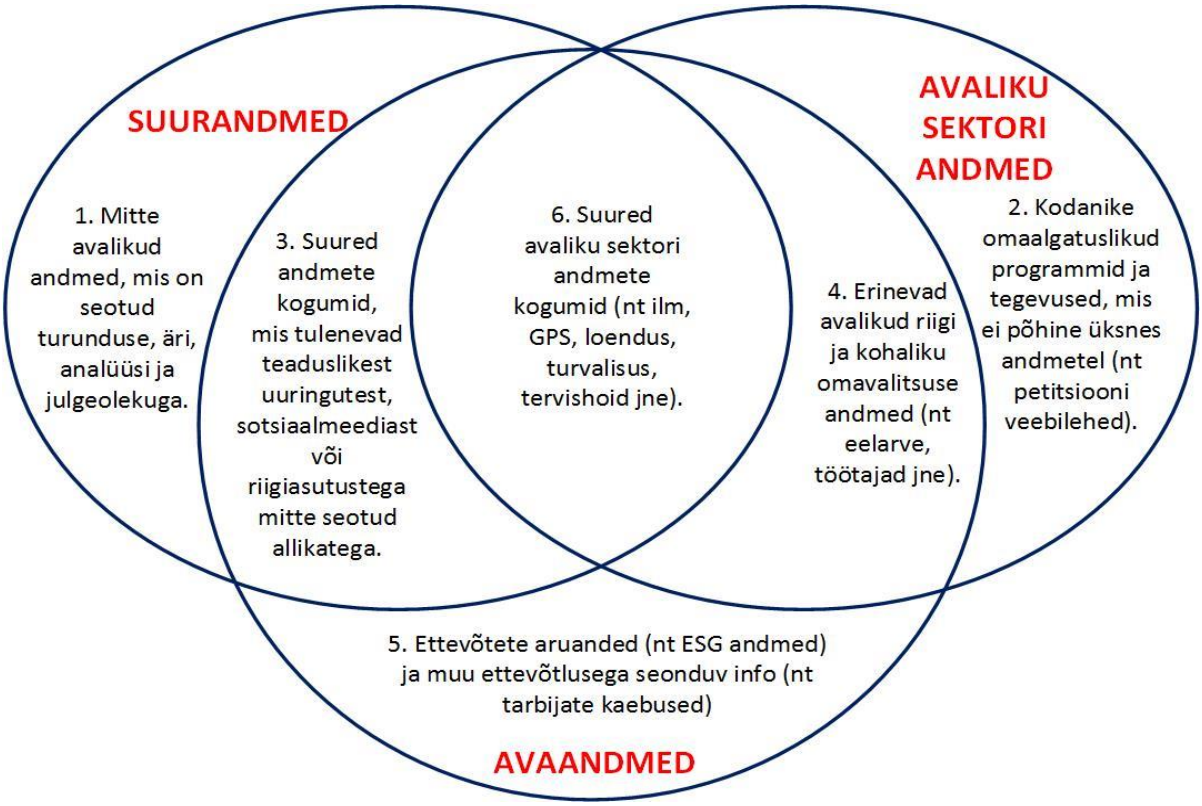
Otsuste kujundamist on võimalik teostada ka läbi anonümiseeritud andmekogumite, mis on kergemini ligipääsetavad nii teadustöö kui ka statistiliste analüüside läbiviimiseks ning ka eraettevõtetele teenuse pakkumiseks. Selleks, et analüüsitavad andmed ei sisaldaks isikuandmeid on võimalik need anonüümseks muuta ning seeläbi ei loeta neid andmeid enam isikuandmeteks.[280]

Andmete anonümiseerimine võimaldab suurandmeid analüüsida ning organisatsioonidel teostada uuringuid või töötada välja tooteid ja teenuseid[281]. Anonümiseeritud andmete pinnalt on võimalik teostada erinevaid järelmeid. Näiteks läbi mobiilpositsioneerimise andmete, mis on kättesaadavad avaandmetena, on võimalik erinevates piirkondades tuvastada kõnekaartide kasutamist ja nende liikumist. Läbi avaliku numbripäringu[282] on võimalik selekteerida

[279] I. Liiv. Andmetest poliitika kujundamiseni: Uuring suurandmete ja teiste uuenduslike andmepõhiste meetodite võimalustest kujundada tõendustele tuginevat poliitikat. 2016, lk 8. Arvutivõrgus: https://e-estonia.com/wp-content/uploads/2014/02/Data4policy_Raport_est_final.pdf (08.01.2017).
[280] Suurandmed ja privaatsus, lk 3.
[281] Suurandmed ja privaatsus, lk 8.
[282] EV-s veebilehekülg https://nba.tja.ee/numbriparing.aspx (16.03.2017).

erinevate telefonioperaatorite lepingulisi kliente. Samuti on võimalik asukohapõhiselt tuvastada konkreetse ettevõttega seotud isikud ja nende liikumist. Selleks vaadeldakse ajaliselt konkreetse piirkonna mobiilpositsioneerimise andmeid võrreldes neid erinevate kellaaegade lõikes.

Suurandmete ja avaandmete seost illustreerib joonis 4, mis toob välja seosed suurandmete ja avaandmete vahel ning nende suhestumise avaliku sektorti poolt avalikustatavate andmetega.[283]




Joonis 4 – Suurandmeid, avalikustatud avaliku sektori andmeid ja avaandmeid illustreeriv seos.

EV kontekstis võib siin näitena välja tuua OÜ Positium LBS, mis pakub anonümiseeritud mobiilpositsioneerimise andmetel kujundatavat rahvastiku paiknemise ja liikumise mustrite teenust. Selle abil aidatakse nii eraettevõtjatel kui ka avalikul sektoril kaardistada inimeste liikumise kontekstis kujundatavaid otsuseid. Anonümiseeritud andmed võimaldavad ühiskonna või klientuuri kohta järeldusi teha ilma, et konkreetsed andmed oleksid isikuga seotud. Piisab,

[283] J. Gurin. Big data and open data: what's what and why does it matter? The Guardian, April 15, 2014. Arvutivõrgus: https://www.theguardian.com/public-leaders-network/2014/apr/15/big-data-open-data-transform-government (16.03.2017).

kui ühe inimese kirjed on omavahel mingi identifikaatoriga (nt koodiga) ühendatud ning antud protsessi, kus inimest identifitseerivad kirjed nimetatakse anonümiseerimiseks.[284]

Lisaks on võimalik indiviide manipuleerida mõjutades nende otsustusprotsessi, mida teostakse läbi otsingumootorite algoritmide, mille abil kuvatakse teatud sõnade puhul otsingutulemustes mõjutatud uudistega seonduvaid linke. Uuringud on näidanud, et kui üks inimene usaldab otsingumootori poolt väljapakutud tulemust on sellest mõjutatud peagi ka tema tutvusringkond. Eeltoodut illustreerib Inglismaa Ühendkuningriigi EL-ist väljaastumise rahvahääletuse eelne EL-ist väljaastujate pooldajate poolt läbi viidud kampaania. Kampaania raames koguti *Facebook*-ist kokku miljonite Inglismaa Ühendkuningriigi elanike andmed ning koostati profiilid inimeste osas, keda on võimalik ja tasub mõjutada hääletama EL-ist lahkumise poolt.[285]

Otsuste kujundamises on sotsiaalselt kõige rohkem mõjutatavad alates 1985. aastast sündinud isikud, kes jagavad läbi elektrooniliste kanalite endast varem sündinutest rohkem informatsiooni. Nad ei muretse eriti valitsusasutuste poolt teostatavate jälgimiste üle sellises mahus kui neist vanemad isikud. Nende puhul kaalub riive üle elektrooniliste kanalitega kasutamisega kaasneva kahju. Näiteks üle 85% USA ülikooli tudengitest omab *Facebook*-i kontot, kuhu nad talletavad fotosid enda elust, erinevaid postitusi endast ja oma sõpradest ning seovad neid omavahel tuues sellega seonduvalt välja oma tutvusringkonna kellega nad suhtlevad. Selline tegevus on kaasa toonud selle, et kehtinud põhimõte „minu kodu on minu kindlus“ ei ole enam kandev. Seda peamiselt seetõttu, et infotehnoloogia arenguga seonduvalt on andmed kõigile avalikult kättesaadavaks muutunud.[286] Samuti kommunikeeruvad noored rohkem neile tundmatute isikutega, hoolimata sellest, et nad ei ole nendega väljaspool küberkeskkonda kohtunud. Olenemata sellest, et noored saavad aru, et kõik nende *Facebook*-i lehel avaldatud pildid ja kanded võivad neile kompromiteerivaks osutuda ning tulevikus mõjutada nende tööalaseid perspektiive avaldavad nad neid seal ikkagi.[287]

---

[284] L. Kamm. Privaatsust säilitav andmeanalüüs. Sirp, 08. mai 2015. Arvutivõrgus: http://www.sirp.ee/s1-artiklid/c21-teadus/privaatsust-sailitav-andmeanaluus/ (28.02.2017).
[285] R. Poom. Brexit ja Trump on omavahel seotud, neid ühendab varju hoidev ajupesumiljardär. Eesti Päevaleht 28. veebruar 2017. Arvutivõrgus: http://epl.delfi.ee/news/valismaa/brexit-ja-trump-on-omavahel-seotud-neid-uhendab-varju-hoidev-ajupesumiljardar?id=77371654 (28.02.2017).
[286] J. Zittrain, lk 233.
[287] J. Zittrain, lk 234.

Otsuste pinnalt tõendite kujunemine ja hindamine saab aluse olemasolevate andmete analüüsist. Selle eesmärgiks on olemasolevatest andmetest välja selekteerida kogu kaasusega seonduv informatsioon. Tuvastamaks seoseid mineviku kontekstis ning tegemaks ennetusotsuseid tuleviku kontekstis on vajalik andmete pikaajaline hoiustamine. Analüüsiks on vajalik teostada olemasolevate andmete eeltöötlemine, puhastamine ja struktureerimine. Need on protsessid, mille käigus muundub analüüsitav info teadmisteks, mis koosneb faktidest ja seostest, mis on andmete analüüsi käigus tuvastatud[288].

Alapeatüki lõpetuseks võib kokkuvõtlikult tõdeda, et tänapäeva maailmas on aina enam realiseerumas E. Kergandbergi öeldu: „Tänane õhtumaine ühiskond on dilemma infonälg versus privaatsusjanu lahendamisel teinud otsuse esimese kasuks ehk privaatsuse kahjuks“. [289] Inimesed on selle valiku teinud teadlikult, kuna elektrooniliste infokanalite kaudu teostatav suhtlus kaalub üle võimaliku privaatsuse riivega kaasneva kahju. Seega peab õigus tagama, et isikute õigused oleksid vajalikus mahus kaitstud ning nende privaatsusega seonduv riive oleks võimalikult minimaalne arvestades kaasnevat info kogumise paratamatust.

## 4.3 Suurandmete põhjal tehtud otsuste usaldusväärsus

Ühiskonnaprotsesside vaatlemiseks ja otsuste kujundamiseks säilitatakse erinevate riikide valitsusasutuste andmebaasides suurel hulgal erineva segmentatsiooniga andmeid. Teatud vaatluse vormid on demokraatlikus ühiskonnas legitiimsed ja vajalikud, kuid samas võib nende kumulatiivne mõju indiviidide õigustele olla negatiivne.[290]

Aja jooksul kujunevad andmekogumid võimaldavad saavutada tulemeid, mille alusel on võimalik piirata konkreetsete isikutega seotud tegevusi. Näiteks kui konkreetne huvipakkuv isik on aktiivselt tegev poliitikas ning tema vastased soovivad teda diskrediteerida, siis on võimalik eelnevalt kogutud andmeid koondada ja kasutada õigel ajahetkel sõnumite kujundamiseks ning seda sooviga heita tema poliitilisele tegevusele konkreetsel ajahetkel negatiivset varjundit. Vastavasisuliste andmete kogumine võib ühiskonnas kaasa tuua isikute

[288] M. Toivonen, lk 8.
[289] E. Kergandberg. Natuke privaatsusest ja mõnevõrra enam selle jälitustegevuslikust riivest isikuandmeid töötleva Eesti avaliku võimu poolt. Juridica 2005/VIII, lk 544-553.
[290] D. H. Flaherty, lk 1, 3.

suhtes läbiviidava kontrolli teostamisel valitsemisasutuste suurema võimu ning vajadusel nende tegevuse suunamise planeerimise.[291]

Tänapäeva tehnika areng, mis on seotud automatiseeritud andmete kogumisega, on suuresti võimaldanud ja lihtsustanud, elektroonilisi kanaleid kasutades, suhtlust erinevate ametkondadega. Suhtluse käigus salvestatakse isikuga seotud erinevaid andmeid, mis on valitsusasutustele kättesaadavad ning mida on võimalik kasutada erinevate administratiivsete ülesannete täitmiseks, nagu näiteks analüüside läbiviimine ja ennetusotsuste kujundamine. Mida rohkem isikutega seotud personaalset informatsiooni ja dokumentatsiooni koguneb, seda efektiivsemaks muutub kogutud andmete pinnalt teostav analüüs ning vajadusel otsingute vastete leidmine, mille sihtmärgiks võib olla igaüks.[292]

Elektrooniliste kanalite kaudu edastatava info väärtus ei pruugi aga olla tõene ning vajab seetõttu nii isikute kui ka infot kasutatavate asutuste poolset järelkontrolli. Otsuste kujundamiseks kasutatavad andmed peavad pärinema usaldusväärsetest allikatest ja sobituma teostatava uuringu raamidesse, kuna elektrooniliste kanalite kaudu talletunud informatsioon ei pruugi olla tõene. Näitena saab tuua läbi massimeediakanalite VF-i poolt teostatavat elanikkonna mõjutamist. EV suunal teostatakse seda näiteks järjepidevalt läbi telekommunikatsiooni, samas Visegrádi riikidele suunatud väärinformatsiooni edastuse viisid on teistsugused. Nende riikide elanikkonna ja poliitika kujundajate mõjutamiseks on loodud sadu erinevaid internetilehekülgi, mille kaudu väärinformatsiooni edastust teostatakse. Skandinaavia suunal toimub väärinformatsiooni edastus läbi isikute, kes kommenteerivad artikleid või algatavad erinevates suhtluskeskkondades arutelusid, luues sellega valedel alustel tõstatuvat ühiskondlikku resonantsi. Vastavasisulise informatsiooni loomist teostavad VF-i poolt finantseeritavad veebibrigaadid, mis koosnevad anonüümsetest kommentaatoritest. Eelmainitud riikides ja regioonis tegutsevad ka VF-i mõjusfääris olevaid poliitikuid, kes olles propagandast mõjutatud edastavad iseseisvalt väärinfo põhjal kujundatud sõnumeid. [293] Propagandana saab käsitleda kaalutletud ja süstemaatilist püüet kujundada vastuvõetavaid

[291] D. H. Flaherty, lk 9.
[292] D. H. Flaherty, lk 1, 3.
[293] G. Gotev. Commission: Russian propaganda has deeply penetrated EU countries. Euroactiv, July 14, 2016. Arvutivõrgus: https://www.euractiv.com/section/global-europe/news/thurs-commission-official-russian-propaganda-has-deeply-penetrated-eu-countries/ (26.02.2017).

sümboleid manipuleerida inimeste tunnetustega ja suunata nende käitumist nii, et saavutatakse reaktsioon, mis aitab propagandistil oma kavatsusi täita.[294]

Väärinformatsiooni esitamist meedias on välja toonud ka endine *Russia Today* (edaspidi „RT") töötaja, kelle sõnul keskendub RT oma levipiirkonna riikides enamjaolt peavoolumeedia välistele teemadele, millega üritatakse sisustada ja luua kujutelm objektiivsest meediakanalist.[295] Tegelikkuses on RT näol tegemist VF-i poolt riiklikult rahastatava ja välismaale suunatud ingliskeelse telekanaliga.[296] Kajastatavate uudistega seonduvalt luuakse kanali kaudu ühiskonnas väärettekujutus nagu ei eksisteeriks objektiivseid teemakäsitlusi ning kõik faktid esitatakse võimul olevatele isikutele vajalikus kontekstis ja mahus. RT-s käsitletavaid uudiseid töödeldakse selleks, et manipuleerida vaatajaskonnaga soovides tekitada neis usaldamatust ja arusaama, et võimueliit on korrumpeerunud ning kodanike arvamus ei ole neile oluline. Tulenevalt sellest, et RT vaatajate hulk on viimastel aastatel jõudsalt kasvanud on nende rahvusvahelisele üldsusele suunatud meediakajastused muutunud aina laiapõhjalisemateks ja samas ka radikaalsemaks. Ei kardeta luua valearusaama, tekitada vastandumist ühiskonnas ning sellega seonduvalt naeruvääristada demokraatlikku ühiskonnakorraldust ja selle toimimist. Sobivate meediakajastuste loomiseks manipuleeritakse faktidega, millel puuduvad usaldusväärsed allikad. Samuti võetakse arvamusi inimestelt, keda kuvatakse kui valdkondlikke eksperte, kuid tegelikkuses nad seda ei ole.[297]

Eeltoodud meetodeid kasutati ka 2016. aastal toimunud USA presidendi valimiste kampaania raames. Kampaania meediakajastuste käigus ja küberruumis edastati rohkelt väärinformatsiooni. Näiteks sattus üks demokraatide arvutisüsteeme VF-i valitsusega seotud häkkerite rühmituse rünnaku alla. Rünnaku põhjuseks oli soov vältida H. Clintoni võimule saamist, kuna tema poliitilised vaated ei olnud kooskõlas VF-i juhtkonna huviga. Samas vastaskandidaadi D. Trumpi osas ei avaldatud ühtegi meediakajastust, milles oleks teda seoses varasema eluga negatiivselt kuvatud.[298]

---

[294] I, Halilov. Propagandisliku narratiivi muutmine konfliktisituatsioonis: Ukraina kriisi näitel. Tartu Ülikool: Sotsiaal- ja haridusteaduskond, riigiteaduste instituut 2015, lk 17. Arvutivõrgus: https://dspace.ut.ee/bitstream/handle/10062/47120/halilov_indrek_ma_2015.pdf? (23.03.2017).

[295] K. Zbytniewska. Former RT presenter: Russian disinformation is a weapon. Euroactiv, Detsember 22, 2016. Arvutivõrgus: http://www.euractiv.com/section/global-europe/interview/former-rt-presenter-russian-disinformation-is-a-weapon/ (26.02.2017).

[296] I, Halilov, lk 3.

[297] K. Zbytniewska. Viidatud töö.

[298] K. Zbytniewska. Viidatud töö.

Kui eelmainitud meediakajastused võetakse aluseks ühiskonna meelestatuse tuvastamiseks uuringute läbiviimisel, siis aluslähtematerjal, mida uuringute käigus kasutatakse ei ole tegelikkusega kooskõlas ning sellega seonduvalt võidakse poliitilisel tasandil võtta vastu ebausaldusväärseid otsuseid. Sellisel kujul tekkinud olukorda saavad ära kasutada ka erinevad siseriiklikud äärmuslikult meelestatud liikumised, luues sarnase metoodika alusel siseriiklikult vaenu õhutavaid sõnumeid.

EV kontekstis saab näitena eeltoodu ilmestamiseks tuua riigis baseeruva ettevõtte FT News Group OÜ, mille tegevusalaks on rootsi keelse veebiportaali haldamine. Tegemist on ühe Rootsi radikaalseima paremäärmusliku propagandistliku veebileheküljega, mis asetab halba valgusesse sisserändajaid ning kritiseerib riigi poliitikat. Veebiportaal esindab islamofoobiat, võõrviha ja VF-i praegust poliitikat kujundavaid seisukohti.[299]

Lisaks eelpool kirjeldatud tahtlikule väärinformatsiooni levitamisele massimeediakanalites on suureks probleemiks ka küberründed, mis on suunatud konkreetsetele sihtmärkidele. Sihtmärkideks võivad olla näiteks kriitilise tähtsusega objektid või konkreetselt valitud isikud. Isikute vastu suunatud ründe eesmärgiks võib olla soov saavutada juurdepääs nendega seotud andmetele, muuta isiku poolt loodud andmeid või avaldada informatsiooni ja teostada tehinguid isiku nimelt. Eeltoodud tegevusele aitab kaasa järjepidevalt kasvav Interneti ning sotsiaalmeedia kasutajate hulk, mis loob soodsad võimalused erinevate õigusrikkumiste toimepanemiseks.[300] Virtuaalsed IT-alased lahendused on sageli suurel määral seotud füüsilise maailmaga ning inimesed võivad kogeda, kuidas ründed toovad kaasa reaalseid ja käega katsutavaid tagajärgi.[301] Näiteks on igal isikul võimalik Internetist leida erinevaid teenusepakkujaid, kes võimaldavad teostada jälgimist, kasutades selleks vastavat tarkvara lahendust. Ühe sellise tarkvara lahendusena võib välja tuua *Loverspy*, mis võimaldab jälgida kogu sihtarvutis toimuvat tegevust, muuhulgas ka saabuvat ja saadetavat e-posti, arvuti kasutaja külastatud veebilehti, sisestatud salasõnu jne. Kogu eelnevalt väljatoodud kogutud informatsioon saadetakse aga teenuse eest tasujale. Samuti on soetajal kaughalduse kaudu

[299] T. Jõesaar. Rootsi trollivabriku salapäraseid rahaasju aetakse Eestist. Eesti Päevaleht, 27. veebruar 2017. Arvutivõrgus: http://epl.delfi.ee/news/eesti/rootsi-trollivabriku-salaparaseid-rahaasju-aetakse-eestist?id=77360858 (27.02.2017).
[300] J. Clough. Principles of Cybercrime. Cambridge: Cambridge University Press 2010, lk 5.
[301] E. Kodar. Küberründed jõu kasutamise õiguse ja humanitaarõiguse raames – millised on mängureeglid? Diplomaatia nr 85, September 2010. Arvutivõrgus:http://www.diplomaatia.ee/artikkel/kuberrunded-jou-kasutamise-oiguse-ja-humanitaaroiguse-raames-millised-on-mangureeglid/ (22.02.2016).

võimalik pääseda ligi sihtarvutis asuvatele failidele ning isegi lülitada sisse sihtarvuti veebikaamera.[302]

Globaliseerumine ja IT-lahenduste igapäevaellu integreerimine on kaasa toonud arvutivõrkude vastu suunatud rünnete kasvu. Rünnete teostajateks on enamjaolt kas riigid või riikide esindajad, terroristid, küberkurjategijad ning vahel isegi tavalised arvutikasutajad seda ise teadmata. Kuna küberrünnetega ei kaasne kineetilise jõu kasutamist, ei kvalifitseeru need klassikaliseks sõjaliseks rünnakuks (nt relvastatud rünnak). Näiteks kui riigi A sõjaväe häkkerid kasutavad küberruumi, et rünnata riiki B, saab seda määratleda terrorismi või kui muud kuriteona kvalifitseeritavat tegu. Ühe sellise rünnaku näitena saab välja tuua 2013. aastal toimunud seeriarünnakuid, kus Hiina "kübersõdalased" ehk rahva vabastusarmee üksus 61398 tungis mitmeid aastaid erinevatesse USA ettevõtete võrkudesse, et varastada sealt tehnoloogiatega seonduvaid andmeid. Varastatud andmeteks olid erinevad toodete joonised, tehniliste tootmisprotsesside andmed, meditsiiniliste kliiniliste uuringute tulemused, ettevõtete hinnakujundusega seotud dokumentatsioonid jne. Uuringud näitavad, et Hiina jätkab siiani teadlikult küberspioonide ettevalmistamist ning koolitamist hankimaks tundlikku majandust ja tehnoloogiaid puudutavat informatsiooni.[303]

Küberründeid võivad läbi viia ka riiklikult sponsoriseeritud üksused, mis on suunatud riiklikult oluliste taristute vastu. Näiteks võib ühe ründena välja tuua ussviiruse „Stuxnet", millega rünnati Iraani tuumaprogrammi ning mis avastati alles 2010. aastal. Seoses rünnaku keerukusega on eksperdid teinud järeldusi, et tegemist võis olla riikide toetusel toime pandud rünnakutega.[304]

Küberkeskkonnas teostatud andmete vargust saab vaadelda kui küberkeskkonnas sooritatud küberkuritegu, mille näol on tegemist ühe uusima kuritegevuse liigiga. Sellega seonduvalt on uue distsipliinina arenenud küberkriminoloogia valdkond, mis on loomas uut iseseisvat ja unikaalset positsiooni tõendite kujunemisel kriminaalmenetluses.[305] Seoses kriminaalõiguses kehtiva põhimõttega „*nullum crimen, nulla poena sine lege*" peavad küberkuriteod olema

[302] J. Clough, lk 36.
[303] S. W. Brenner. Cyberthreats and the Decline of the National-State. New York: Routledge 2014, lk 4, 5.
[304] P. Mueller, B. Yadegari. Report: The Stuxnet Worm. The University of Arizona: Arizona Computer Sciance 2012. Arvutivõrgus: https://www2.cs.arizona.edu/~collberg/Teaching/466-566/2012/Resources/presentations/2012/topic9-final/report.pdf (27.02.2017).
[305] X. Li, lk 53.

inkorporeeritud kriminaalõigusesse ning see on, arvestades kriminaalpoliitiliste vajadustega, mõjutanud ja aidanud uuendada konventsionaalset kriminaalõigust. Tegemist on ühiskonna arenguga kaasneva sotsiaalse fenomeniga. [306]

Kriminaalõiguse eesmärgiks on kaitsta individuaalseid, kollektiivseid ja ühiskondlikke huve. Seoses küberkuritegevuse arenguga on kriminaalõiguses vajalik rakendada täiendavaid meetmeid. Nimelt toovad infosüsteemide haavatavus ja nende vastased ründed eriti teravalt esile sotsiaalsed faktorid ja tegevused, mis on motiveeritud erinevatest huvidest lähtuvalt. Seetõttu on oluline ühiskonnani viia arusaam, et küberkuritegevusega kaasneb riigi poolne sanktsioonide rakendamine ning läbi kriminaalkaristuse määratletakse küberruumis vajalikud isikute tegevusega seonduvad piirid. Tulenevalt potentsiaalsest kahjust, mida küberkuritegevus ja -kurjategijad teha võivad, peavad julgeoleku- ja politseiasutused eriti tõhusalt nende vastu võitlema.[307]

Seoses IKT arenguga muutuvad olemasolevad teadmised pidevalt ajas ja ruumis. Hetkel olemasolevad teadmised võivad juba homme olulisel määral täieneda, kuna järjepidev ning kiire tehnika- ja tehnoloogiaareng võimaldab aina enam tõhustada info käitlemist. Antud areng ühiskonna ja poliitilises protsessis peab olema kontrollitav läbi andmekaitse õigusnormide, tagades ühiskonna liikmetele enda õiguste kaitseks mõistetavad mehhanismid.[308]

Lähtudes teadmisest, et küberkeskkonnas esineb valedel alustel põhinevat informatsiooni ning arvestades asjaoluga, et suurandmete näol on tegemist struktureerimata ja pidevalt muutuva andmehulgaga võib sellistele andmetele tuginedes ning järeldusotsuseid kujundades luua järeldusi, mis ei ole tõesed. Viimaste pinnalt tehtud otsused on aga juba eos väärad. Sarnaselt massimeedias avaldatud väärinformatsioonile võib küberrünnakute tõttu muutuda ka Internetis olemasolev informatsioon ning see võidakse rünnaku läbiviijate poolt paigutada neile vajalikku konteksti. Samuti võidakse manipuleerida võrku ühendatud seadmete kaudu veebilehekülgede või andmebaaside toimimist.

[306] X. Li, lk 56.
[307] X. Li, lk 57.
[308] Wedde, P. jt. Digitalisierung Der Grundrechte? Zur Verfassungsvertraglichkeit der Informations- und Kommunikationstechnik. Westdeutcher Verlag GmbH, 1990, lk 6, 7.

## 4.4 Suurandmete põhjal tehtud otsuste ja saadud teadmiste mõju süütuse presumptsiooni tagamisele

Tänapäeva ühiskonnas on kogutavate andmete maht kasvanud ning seda teostatakse eesmärgiga koguda neid kokku võimalikult suures mahus. Selliseid andmeid saab odavalt kopeerida ning hoiustada otsinguid võimaldavates andmekogumites, mis on läbi interneti lihtsalt kõigile ligipääsetavad. Samuti hoiustatakse ka andmeid kauem, kui vaid esmase informatsiooni selekteerimiseni.[309] Andmete kogumine on seotud nii arvutite statistilise arvutusvõimuse tõusuga, mida toetab andmete salvestamise jätkuv langustendents, kui ka tehnoloogia arenguga, mis võimaldab suurandmeid analüüsida.

Rakendades andmete analüüsi tehnoloogiaid moodustuvad järjest suuremad erinevate andmete kogumid, mida nii ettevõtted, kui ka valitsusasutused saavad kasutada andmetes esinevate korrelatsioonide avastamiseks. Selline areng toetab ühelt poolt innovaatiliste lahenduste leidmist ja kasutuselevõttu ning võimaliku majanduskasvu, kuid teiselt poolt tõstatab see ka mitmeid kriitilisi küsimusi seoses andmete turvalise hoiustamise, privaatsuse ja eetiliste dilemmadega. Suurandmed tuginevad superarvutitele ja tehisintellekti õppimisvõimele, mistõttu võib inimvõimetel olla keeruline mõtestada suurandmete mahtu ilma algoritmiliste tööriistade ja analüüsi toeta[310].

Suurandmete alusel on võimalik läbi analüüsi selekteerida välja konkreetse isikuga seonduv ning tuvastada tema käitumismustrid ja suhtlusringkond. Läbi käitumismustrite korrelatsiooni on võimalik teostada ennustusi isikute võimalike käitumiste osas Samuti võimaldavad suurandmed analüüside abil teostada info põhjal kuritegude ennetamisega seonduvaid otsustusi. Samas ei saa suurandmete põhjalt tehtud otsuste pinnalt kindlalt väita, et konkreetne indiviid või isikute grupp, kelle suhtes on otsus tehtud, ka vastavalt ennetusotsustele käitub.

Otsingute korraldamist suurandmete alusel põhjendatakse vajadusega teostada teenuse kvaliteedi tõstmist, kuritarvitamiste ja pettuste avastamist, uuringuandmete analüüsi, personali kontrolli, võimaliku kriminaalse tegevuse avastamist ning terrorismi ennetustegevusega.[311] Terrorismi ennetustegevusega seonduvalt võimaldab selline otsingute teostamine viia läbi

[309] B. Schneier, lk 24.
[310] M. Hu 2014, lk 796.
[311] D. J. Steinbock. lk 15.

laiapõhjalist analüüsi tuvastamaks potentsiaalseid terroriste või identifitseerimaks võimalikke terrorismiga seotud isikuid seni „tundmatute“ isikute hulgast. Olemasolevate süsteemide kaudu analüüsitakse läbi suurel hulgal isikuid, et leida vasteid, kes võiksid sobituda loodud näidisprofiiliga. Süsteemid võimaldavad automaatselt, kas siis kirjeldavat või ennustavat mudelit kasutades, tuvastada võimalikke uusi seoseid inimeste, kohtade või omavaheliste suhete kaudu.[312] Andmete seostamine erineb otsingutest selle poolest, et erinevate struktuuride alusel on võimalik teatud omaduste ja käitumiste tuvastamist ning seda kasutatakse sageli ennetavate otsuste tegemisel. Otsingute käigus kohaldatakse andmebaasi läbi statistilise analüüsi ja modelleerimise, luues leitud varjatud struktuuride ja seoste vahel andmetes reeglid, mis võimaldavad tulevikus välja pakkuda sarnaseid tulemeid.

Suurandmete põhiseid analüüsi tulemeid kasutatakse igapäevaselt julgeoleku- ja politseiasutuste poolt nii taustakontrollide läbiviimisel, kui ka kriminaalmenetluse algfaasis olemasolevate faktide kinnitamiseks või ümberlükkamiseks. Menetlustoimingute planeerimisel ning kohtult jälitusloa saamise põhjendamisel kasutavad julgeoleku- ja politseiasutused nende infosüsteemides säilitatud isikutega seonduvat informatsiooni. Kui karistusregistri kanded kustutatakse peale aegumistähtaegade saabumist, siis julgeoleku- ja politseiasutuste infosüsteemides säilitatakse neid ka peale karistusandmete kustutamist karistusregistrist. Näiteks on õigusruumis sätestatud tingimused kriminaalkorras karistatud isiku karistusandmete säilitamise ja nende registrist kustutamise osas. EV-s on KarS § 81 kehtestatud, et kedagi ei tohi kuriteos süüdi mõista ega karistada, kui kuriteo lõpule viimisest kuni selle kohta tehtud kohtuotsuse jõustumiseni on möödunud kümme aastat I astme ja viis aastat II astme kuriteo korral. Karistatud isiku ja tema karistatuse kohta olevad andmed on registreeritud karistusregistri infosüsteemis. Registri eesmärk on tagada usaldusväärse teabe olemasolu karistusalase teabe kohta. Karistusregistri seaduse[313] § 24 lg 1 p 8 ja 9 alusel kustutatakse karistusandmed registrist kui:

- alla viie aastase vangistuse ära kandmisest on möödunud 5 aastat;
- 5-20 aastase vangistuse ära kandmisest on möödunud 10 aastast;
- üle 20 aastase vangistuse ära kandmisest on möödunud 15 aastat.

[312] D. J. Steinbock, lk 16.
[313] Karistusregistri seadus. – RT I, 21.03.2011, 3 … RT I, 30.12.2015, 17. Arvutivõrgus: https://www.riigiteataja.ee/akt/130122015017 (22.03.2017).

Võimaliku kuriteokahtluse korral kontrollitakse julgeoleku- ja politseiasutuste infosüsteemidest isikuga seonduvat informatsiooni. Juhul kui tuvastatakse vaste, et isik on eelnevalt kriminaalkorras karistatud või on infosüsteemides temaga seonduvat informatsiooni, siis on see aluseks otsuste vastuvõtmisel ja ametniku siseveendumuse kujunemisel. Olemasolevat informatsiooni kasutatakse ning selle alusel põhjendatakse isiku suhtes planeeritavaid toiminguid.

Indiviidide õiguste kaitseks ja andmete põhjalt kujundatud otsuste tuvastamiseks on kehtestatud andmekaitse regulatsioon. Andmekaitse regulatsiooni eesmärgiks on isikute privaatsuse tagamine ning valitsusasutuste ja erasektori poolt teostatavate andmete kogumise seaduslikkuse kontroll. See annab ka isikule võimaluse kontrollida tema kohta loodud andmete õigsust. Andmekaitse efektiivsust saab mõõta mahus, milles suudetakse jälgimist kontrollida ja sellega kaasnevat negatiivset mõju vähendada.[314]

EL tasandil on indiviidi õiguste kaitseks vastu võetud EL andmekaitsedirektiiv, kus on sätestatud õigus olla unustatud. Indiviidil on võimalik enda osas olemasolevaid elektroonilisi andmeid kontrollida, nagu näiteks otsingumootori kaudu tema isikuga seonduvat informatsiooni. Selle tuvastamisel on isikul võimalus taotleda väärinformatsiooni eemaldamist. EL Kohus on otsuses C-131/12[315] rõhutanud, et otsingumootori poolt avaldatud andmete kustutamise eelduseks ei ole tingimus, et andmete avaldamine tekitaks isikutele kahju, vaid andmete kustutamise kohustus on kohtu arvates piiratud üksnes olukordades, kus andmed on ebaõiged. Kohtu hinnangul võib andmete töötlemise vastuolu direktiiviga tuleneda sellest, et andmed ei ole piisavad või asjakohased või ületavad otstarbe piire, mille tarvis neid töödeldakse. Samuti, et neid andmeid ei ajakohastata või säilitatakse pikema aja jooksul, kui see on vajalik, välja arvatud juhul kui neid säilitatakse ajaloo, statistika või teadusega seonduvalt. Seega saab Euroopa Kohtu arvates järeldada, et andmete töötlemine on direktiiviga vastuolus ka siis, kui andmed on nende töötlemise kunagisi eesmärke ja möödunud aega arvestades ülemäärased ning ei ole isiku poolt kontrollimise hetkel enam asjakohased.[316]

---

[314] D. H. Flaherty, lk 11.

[315] EKo C-131/12, *Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González.* Arvutivõrgus: http://eur-lex.europa.eu/legal-content/ET/TXT/HTML/?uri=CELEX:62012CJ0131&from=EN (01.04.2017).

[316] A. Värv. Euroopa Kohtu Google'i otsus ja isiku õigus olla unustatud. Tallinn: Riigikogu Kantselei, õigus- ja analüüsiosakond 2014. Arvutivõrgus: https://www.riigikogu.ee/wpcms/wp-content/uploads/2015/01/Teemaleht_20_2014.pdf (03.03.2017).

Harta artikkel 7 tagab õiguse eraelu puutumatusele ning artikkel 8 sätestab õiguse isikuandmete kaitsele. Isiku kohta otsingumootori abil tehtud päringute abil kaaluvad need põhiõigused Euroopa Kohtu hinnangul üldjuhul üles nii otsingumootori haldaja majandushuvi kui ka üldsuse huvi teabe saamiseks. Erandina võib üldsuse huvi teabe saamiseks olla isiku põhiõigustest kaalukam, juhul kui see teave puudutab avaliku elu tegelast. Eeltoodust tulenevalt on otsingumootori haldajal kohutus igal üksikjuhtumil kaaluda, kas otsingutulemuste eemaldamine on konkreetse taotluse puhul õigustatud. [317]

Isikute suhtumine ja hoiakud on loodud õiguslikus kontekstis olulised, sest see loob hoiakute raamistiku, kus üksikindiviidil on võimalik oma käitumist ja õiguste kaitset tagada ning vajadusel ka õiguslikke meetmeid enda kaitseks rakendada. Elektroonilisel viisil andmete säilitamine ja töötlemine erineb oluliselt füüsilisel kujul andmete säilitamisest, mistõttu peab õigussüsteem seda arvestama ning tagama reeglid isikute andmete kaitseks.[318]

Suurandmete kasutamine on kaasa toonud selle, et isikute hindamine toimub andmeid kogudes ning nende andmete kontekst seotakse sarnaste teiste juba tuvastatud käitumismustrite alusel. Ehk siis suurandmetest filtreeritakse välja indiviidide selektsiooni võimaldavad käitumismustrid ning konkreetsete inimgruppide klassifitseerimist võimaldavad parameetrid. Sellise info olemasolu võimaldab teostatavaid otsuseid automatiseerida ning vähem kasutada inimeste poolt teostatavat analüüsi. Sellega seonduvalt ei pruugi analüüsi käigus saadavad tulemid olla usaldusväärsed võtmaks vastu toimingute läbiviimisega seotud otsuseid. Selliste ennatlike otsuste teostamine võib endaga kaasa tuua süütuse presumptsiooni riive ning suurendada ka info valdaja võimupositsiooni otsuste vastuvõtmiseks. Mida suurem on olemasolevate andmete maht, seda tõepärasem võib tunduda nende pinnalt tehtud järeldusotsuste tulem. Suurandmete kasutajad ja nende pinnalt analüüside teostajad peaksid suutma andmete pikemaks säilitamiseks põhjendada andmete potentsiaalseid kasutusviise ja saadavat kasu isegi siis, kui konkreetsed üksikasjad on seoses info võimaliku kasutamisvõimalustega seonduvalt veel kujundamata.

[317] A. Värv 2014.

[318] K. N. Metcalf. Uuring: Privaatsusõigus inimõigusena ja igapäevatehnoloogiad. Privaatõiguse ja andmekaitse õiguslikud aspektid. Tartu Ülikool 2014, lk 82. Arvutivõrgus: http://www.humanrightsestonia.ee/wp/wp-content/uploads/2014/11/EST-Uuringu-V-osa-Privaat%C3%B5iguse-ja-andmekaitse-%C3%B5iguslikud-aspektid.pdf (23.03.2017).

Suurandmete alusel kujundatud teadmise osas tuleb tagada piisav sõltumatu asutuse poolne kontroll ehk nii teabehanke kui ka jälitustoimingute teostamiseks lubade saamisel peab kohus veenduma, et kasutatavad andmed isiku osas, kelle suhtes toiminguid planeeritakse läbi viia, oleksid kontrollitud ja objektiivselt hinnatud. Kohus peaks kontrollima, kas metoodika ja tulemid, mida kohtule toimingute läbiviimiseks esitatakse on saadud usaldusväärsetest allikatest ning ega nende pinnalt ei oleks tehtud ennatlikke otsuseid. Seega oleks autori arvates soovitatav, et õigusmõistmisega seotud isikud oleksid teadlikud andmete alusel sisustatavate tõendite kujunemisest ning täiendaksid valdkonna põhiselt sellest lähtuvalt ka enda teadmisi.

# KOKKUVÕTE

Magistritöös uuris autor suurandmete kasutamisega kaasnevat võimalikku süütuse presumptsiooni riivet. Töö käigus leidis osaliselt kinnitust püstitatud hüpotees, et suurandmete analüüsi käigus kujunevate teadmiste pinnalt teostatavad järeldusotsused võivad olla ennatlikud ning kontekstiga mitte kokku sobituvad. Suurandmete pinnalt järeldusotsuste teostamine võib kaasa tuua süütuse presumptsiooni riive, kuna isiku suhtes kogutud andmete alusel põhjendatakse ning viiakse läbi esmaseid toiminguid teabehanke ja jälitustoimingute näol.

Seoses eelpooltooduga tuleb andmete kogumisel ja säilitamisel tagada põhimõte, et need oleksid kasutatavad vaid põhjendatud kahtluse olemasolul. Kohtul tuleb julgeoleku- ja politseiasutuste poolt teabehanke ning jälitustegevuse lubade taotlemise käigus kontrollida, et kasutatavate andmete analüüs oleks kvaliteetne ja nende põhjalt järeldusotsuste teostamine oleks läbi viidud õigetel alustel ning kohtule esitatud kujul ka konteksti sobituv. Nimelt tuleb loa andmisel tuvastada info kontekst olemasoleva kahtluse mõistes, millega seonduvalt soovitakse konkreetse isiku suhtes toiminguid läbi viia.

Magistritöös jõudis autor järeldusele, et EV julgeoleku- ja politseiasutused kõikide andmete kogumist käesoleval hetkel ei teosta, seda tehakse vaid osaliselt sideandmete kontekstis. Lisaks sideandmetele võimaldavad suurandmete alusel otsuseid kujundada ka anonümiseeritud avaandmed ning veebiliikluse analüüsitarkvara kasutamine.

Magistritöö esimeses peatükis käsitles autor suurandmete mõistet, nende kujunemist ja väärtust ühiskonna arengu kontekstist lähtuvalt, kus järjepidevalt suurenev andmemaht moodustab järgmise põlvkonna andmeressursid. Autor tuvastas, et suurandmete suurimaks väärtuseks saab lugeda nende töötlemisel saadud tulemit, kus töötlemata andmetest kujunevad läbi analüüsi otsuste kujundamise alused. Informatsiooni töödeldakse selliselt, et selle põhjal oleks võimalik küsimusi formuleerida ning võimalike hüpoteeside tekkimiseks liigutatakse olemasolev küsimus info juurde. Läbi andmete analüüsi tuvastavad käitumismustrid võimaldavad ennustuste teostamist isiku võimaliku tulevikus aset leidva käitumise osas. Ennustusotsused võivad aga olla ennatlikud ning põhineda andmeanalüütiku ekslikel seostel ja oletustel.

Magistritöö teises peatükis käsitles autor suurandmete kasutusalasid USA, EL-i ja EV kontekstis ning sideandmete kogumise raamistikku ja nende kogumisega seonduvat probleemistikku. Suurandmete ajastuga on muutunud info kogumise põhimõtted, mis võimaldavad teostada analüüse nii indiviidi kui ka riiklikul tasandil. Suurandmete kasutusalad on kriminaalmenetluse eelses faasis seotud peamiselt teabehanke ja jälitustoimingute läbiviimisega, mis on ka demokraatlikus ühiskonnas vajalikud. Tagada tuleb tõhus kontroll selle üle, kes ja mis otstarbel ning kuidas teabehanget ja jälitustoiminguid läbi viib. Oluline on siinjuures, et jälitustoimingute läbiviimisega võidakse riivata isikute põhiõiguseid, sest suurandmete ajastul võib igaüks, kes elektroonilisi kanaleid kasutab, olla info kogumise subjektiks. Andmete kogumisel kasutatavad meetmed peavad seega saavutatava eesmärgi osas olema vajalikud, proportsionaalsed ja täpsed. Teine peatükk käsitles ka EL-i poolt kehtestatud sideandmete kogumise reeglistiku, mis on EV õigusesse üle võetud ja mis käesoleval hetkel võimaldab üldiselt vahet tegemata säilitada kõikide klientide ning registreeritud kasutajate liiklus- ja asukohaandmeid. Autor toetab EV õiguskantsleri seisukohti, et eeltoodud võimalus tuleb õiguskaitseorganite poolt läbi viidava ennetustegevuse teostamiseks ka edaspidiselt säilitada ning seda vajadust tuleb EL-i tasandil Euroopa Kohtu otsuste mõju arvestades selgitada.

Magistritöö kolmas peatükk käsitles süütuse presumptsiooni mõistet, ajaloolist tausta ning sisustamist suurandmete ajastul. Kehtiv õigus peab vastama tingimustele, kus kogutud informatsiooni kasutatakse vaid ettenähtud korra kohaselt, võimalikult lühikese ajaperioodi jooksul ning vaid kuriteoga seotud isikute osas. Peatükk selgitab, et süütuse presumptsiooni eesmärgiks on tagada üksikisikutele kaitse riigi omavoli eest, ehk süütuse presumptsioon on kaalukas õiguslik tugisammas individuaalsete õiguste tagamiseks kriminaalmenetluses. Oluline on sealjuures järgida, et kriminaalmenetluse normid peavad andma võimaluse teha kindlaks süüdistatava süü ning aitama rakendada riiklikku karistusnõuet. Autori arvates kinnitab peatükk arusaama, et tänases suurandmete kasutamisega seonduvas ühiskonnas on süütuse presumptsiooni tagamiseks vajalik leida tasakaal riikliku julgeoleku ja kuritegude ennetamise õiguslikus raamistikus, et meetmete kasutamisega kaasnevad riived oleksid kasutatavad proportsionaalselt võimaliku olemasoleva ohu suhtes.

Neljandas peatükis käsitles autor suurandmete põhjal tõendite kujunemist ja hindamist ning nende alusel kujundatud otsuste usaldusväärsust. Peatükk tõi välja, et tõendite kujunemine ja hindamine tuleneb andmete analüüsist, mis võimaldab teostada ennustusotsustusi. See ei kaota

aga ära vajadust saadud otsuseid analüütikute poolt täiendavalt üle kontrollida. Kontrollimine on vajalik, kuna suurandmed võimaldavad saavutada tulemeid ka näiliselt tähtsusetust informatsioonist. Vältimaks valedel alustel kujundatud otsuseid, peavad analüütikud hindama analüüsi pinnalt tehtud otsuste tõepärasust. Neljandas peatükis leidis käsitlust, et EV-s viiakse suurandmete alusel teabehanke- ja jälitustoiminguid läbi põhjendatud kahtluse olemasolul, mis on konkreetsete tuvastatud indiviidide põhine. Kogu andmete kogumine ja nende kasutamine on teostatav sideandmete ning anonümiseeritud andmete kontekstis. Eeltoodust tulenevalt on autor arvamusel, et teabehanke ja jälitustoimingute läbiviimisel ei tohiks tugineda vaid suurandmete analüüsist saadud tulemitele. Toiminguteks vajaliku loa saamiseks on vaja ka konkreetse kahtlusega seonduvaid muid kinnitavaid tõendeid – elektroonne info versus inimallikate info.

Internet on muutnud isikute vahelist suhtlust, kaotades ära erinevad barjäärid, mis olid senini seotud nii distantsi, ajaliste, finants jms võimalustega. Küberruumis toimuv suhtlus ja tegevus jätab maha jälgi, mis võimaldab tuvastada nende teostajaid. Tekkivaid andmeid saab analüüsida ning transformeerida teadmisteks, mis omakorda võimaldavad isikuid profileerida, tuues kaasa võimaliku isikute privaatsusega seonduva riive. Isikud, kelle osas informatsiooni kogutakse, ei pruugi teada, kus ja millises kontekstis kogutud andmeid võidakse kasutada. Andmete kogumisel moodustuvad isikupõhised personaalsed andmekogumid ning seega peab kehtiv õigusruum tagama, et isikute õigused oleksid kaitstud ja et isikud oleksid teadlikud võimalustest, kuidas enda osas andmete kogumist piirata. Nimelt võimaldab suurandmete analüüs teostada erinevaid ennetusotsuseid ning hinnata isikute gruppe nende käitumismustrite alusel.

EL-is kehtiva õiguse kohaselt tuleb isikuandmete töötlemisel järgida kindlaks määratud eesmärke, teostades seda andmesubjekti nõusolekul ja õigusruumis kehtestatud reeglite alusel. Siseriiklikult on õigus kehtestada eelpool nimetatud reegleid riigi julgeoleku ning kriminaalõiguse valdkonnaga seonduvalt, mis ei tohi olla vastuolus inimõiguste ja põhivabaduste kaitse Euroopa konventsiooniga. See tähendab, et andmete kogumist ja juurdepääsu tuleb piirata üksnes seoses raske kuritegevusega seonduvas võitlusega. Selleks peab loodav õiguslik raamistik ette nägema andmetele juurdepääsu eeltingimusena kohtu või sõltumatu haldusasutuse eelneva kontrolli.

Süütuse presumptsioon koosneb erinevatest tehnikatest ja doktriinidest, mis loovad kriminaalmenetluses mehhanismi vähendamaks võimalikku eksimise riski menetluse käigus kellegi ennatlikuks süüdi mõistmiseks. Tegemist on õiglase menetluse aluspõhimõttega, mille eesmärgiks on tagada, et riiklikku karistusõigust ei kuritarvitataks ning isiku süüdimõistmiseks oleks kehtestatud kindlad reeglid. Läbi olemasoleva informatsiooni moodustuvad suurandmetest teadmised, mille puhul peab arvestama võimalike puuduste esinemisega nende kasutamisel. Kujundatud otsused võivad kaasa tuua süütuse presumptsiooni riive, kuna nende alusel tõendite kujundamisel võidakse neid valedel alustel tõlgendada.

Digitaalselt kogutud andmeid kasutatakse aina enam julgeoleku- ja korrakaitseasutuste töös. Nende puhul on vajalik tagada tõhus kontroll info kogumise aluseks oleva kuriteo kahtluse ja kasutavate meetodite vajalikkuse ning proportsionaalsuse osas. Suurandmete põhjal järeldusotsuste läbiviimisel on vajalik kogenud analüütiku olemasolu, kes suudab olemasolevaid andmeid vajaliku kontekstiga sisustada ega teostaks nende pinnalt ennatlikke otsuseid. Arvestada tuleb, et suurandmete hulgas võib esineda teadlikult kujundatud või küberrünnete käigus tekkinud väärinformatsiooni, mis võib kaasa tuua selle, et olemasolevatest andmetest kujuneb süüstavate järelmite kogum.

Olemasolevad andmed loovad menetluses otsuseid kujundava analüütiku jaoks raamistiku, millest otsuste kujundamisel lähtutakse. Loodud raamistikku kasutatakse konkreetse isiku suhtes menetluslike otsuste vastuvõtmisel ning kui tema osas on juba mingis andmebaasis info olemas, siis otsuseid kujundav isik ehk analüütik peab nendega arvestama. See võib vaatluse all oleva isiku suhtes tuua kaasa negatiivse mõjuga otsused, kuna otsuseid kujundav analüütik ei pruugi hinnata kogu olemasolevat informatsiooni kogumise konteksti ning kujundab otsused olemasolevate andmete pinnalt nende konteksti süvenemata.

Kokkuvõtvalt toob töö välja, et tänapäeva suurandmete ajastul levib Internetis palju vääriformatsiooni ja -tõlgendamist. Internetis olevad andmed säilivad pikaajaliselt ning on sageli kasutajast mitte sõltuvalt viidatavad ja kasutatavad, mistõttu on isikud kaotamas kontrolli nendega seonduvate andmete kasutamise üle. Kogutud andmeid saab kasutada ka kriminaalmenetluse kontekstis isikute suhtes tõendite kujundamisel, mis võib kaasa tuua ennatlikud otsused ja sellega kaasneva süütuse presumptsiooni riive. Tagamaks indiviidide põhiõiguste kaitset luuakse järjest enam õiguslikke vahendeid, mis võimaldavad tõhusamat kaitset andmete kasutamise, kogumise, parandamise ja kustutamise osas.

Käesoleva magistritööga loodab autor anda panuse suurandmete kasutamisega seonduvate mõjude teadvustamisse, andes töös teoreetilise ülevaate nii suurandmete olemusest, nende kogumisest ja nende pinnalt tõendite kujunemisest ning juhtides tähelepanu sellele, et suurandmete analüüsi pinnalt võidakse kujundada vääraid otsuseid, mis võivad kaasa tuua süütuse presumptsiooni riiveid. Autori arvates on magistritöös käsitletud teemad leidnud, töös käsitletud kontekstis, EV-s vähest käsitlemist, mistõttu annab töö hea ülevaate suurandmete nii positiivsetest kui ka negatiivsetest kasutamise võimalustest ja mõjust otsuste kujundamisel.

# SUMMARY

In this Master's thesis "Presumption of Innocence in the era of Big Data" the author studied possible infringement of presumption of innocence accompanying the use of big data. In course of the work, the set hypothesis found partial confirmation that the conclusive decisions effected on the knowledge that is formed in course of analysis of big data may be premature and may not fit in context. Performing conclusive decisions on the ground of big data may bring along infringement of presumption of innocence as on the basis of data collected in relation to the person, initial procedural activities are justified and carried out in form of request for intelligence and surveillance activities.

In connection with the above-said, by collecting and maintaining of data it is required to secure the principle that these could be used in case of justified suspicion. The court must control in course of the proceeding of requests for intelligence and surveillance permits submitted by the security and the police authorities that analysis of the data being used is of high quality and that performing of conclusive decisions on this ground would be conducted on correct basis and in form submitted to court – also fitting to context. Namely, by granting permissions it is necessary to establish the context of information in the sense of existing information, relating to what it is wished to perform the procedural activities in relation to the definite person.

In Master's thesis, the author reached to the conclusion that at the moment the security and police authorities of the Republic of Estonia do not conduct collecting of all data, this is done only partially in context of communication data. In addition to communication data, also anonymised open data and use of analysis software of web traffic enable to form decisions on the basis of big data.

In the first chapter of the Master's thesis the author handles the term of big data, their forming and value proceeding from context of development of society where consistently increasing data volume constitutes data resources of the next generation. The author establishes that the biggest value of big data can be considered the result received by their processing where knowledge is formed from unprocessed data by agency of analysis. Information is processed this way that questions could be formed on its basis and the existing question is moved to the information for emerging possible hypotheses. Behavioural patterns established via analysis of

data enable to carry out forecasts in relation to possible behaviour of the person in the future. But the forecasting decisions may be premature and to found on data analyst's erroneous connections and conclusions.

In the second chapter of the Master's thesis, the author disserts the field of use of big data in context of the United States of America, the European Union and of the Republic of Estonia and framework of collecting communication data and problematics related to collecting of those. With era of big data, there have changed the principles of data collecting that enable carry out analyses at personal as well as at national level. Areas of application of big data in the phase before criminal procedure are related mainly to intelligence retrieval and surveillance activities that are also necessary in the democratic society. It is required to secure efficient control of who and for which purposes and how is conducting these. It is necessary hereby that by conducting surveillance activities fundamental freedoms of persons may be infringed as in era of big data everyone who is using electronic channels may be the subject of data collecting. The measures used by data collecting must thus be necessary, proportional and exact in part of the objective to be achieved.

The second chapter handles also the ruleset of collecting communication data enforced by the European Union that has been transposed to the law of the Republic of Estonia and enables to maintain at the present moment all traffic and location data of all clients and registered users without making distinctions. The author supports standpoints of the Chancellor of Justice of the Republic of Estonia that the above-mentioned possibility must be preserved for conducting prevention activities also in the future and this necessity must be explained, if necessary, at the level of the European Union considering influence of the judgments of the European Court.

The third part of the Master's thesis handles the term of presumption of innocence, historical background and furnishing in the era of big data. The valid rule of law must respond to the conditions, where collected information is used only pursuant to foreseen order, in course of possibly short period and solely in connection with persons related to the criminal offence. The chapter explains that the objective of the presumption of innocence is to secure protection of individuals from arbitrary action of the state, or presumption of innocence is a cogent legal mainstay for securing individual rights in criminal procedure. Therewith it is important to follow that the norms of criminal procedure must provide possibility to establish the guilt of the accused and to help to apply the national penal claim. From the author's point of view, the

chapter confirms understanding that in today's society that is associated with use of big data, in order to secure presumption of innocence, it is necessary to find balance in legal framework of national security and prevention of crimes, that infringements accompanying use of measures would be usable proportionally in relation to potentially existing danger.

In the fourth chapter, the author handles evolution and assessment of evidence on the ground of big data and credibility of decisions formed on the basis of these. The chapter brought forth that forming and assessment of evidence is proceeding from analysis of data that enables to effect foretold decisions. But this does not abolish the need to re-check received decisions by analysts additionally. Checking is necessary as big data enable to receive outcome also from apparently unimportant information. In order to avoid decisions formed on wrong bases, the analysts must assess veracity of the decisions made on the ground of analysis. In the fourth chapter there is handled that in the Republic of Estonia, intelligence retrievals and surveillance activities are conducted on the basis of big data in case of existence of justified suspicion that is based on certain established individuals. All data collecting and use of these is performable in context of communication data and anonymised data. Proceeding from the above-said, the author is of the opinion that by conducting intelligence retrieval and surveillance activities it cannot be relied merely on results received from analysis of big data. In order to receive the permit necessary for procedural activities, also other confirming evidence relating to definite suspicion is necessary – electronical information versus information of human sources.

Internet has changed interpersonal communication, by abolishing different barriers that had been connected so far with the distance, time-related, financial, etc. possibilities. Communication and activities conducted in cyber-space leave their traces that enable to identify their performers. The emerging data can be analysed and to transform into knowledge that enable in turn to profile the persons, by bringing along possible infringement of privacy of the persons. Persons in relation to whom information is collected may not know where and in which context the collected data could be used. By collecting data, there will be formed person-based data collections and hence, the valid legal space must secure that rights of the persons would be protected and the persons would be aware of the possibilities on how to restrict collecting data in relation to them. Namely, analysis of big data enables to provide different decisive decisions and to assess the groups of persons on the basis of their behavioural patterns.

Pursuant to law valid in the European Union, it is required to follow predetermined objectives by processing personal data, by doing this with the agreement of the data subject and on the basis of rules stipulated in the legal space. It is entitled to enact nationally the above-mentioned rules in connection with the security of state and field of criminal law that must not be at variance with the European Convention for the Protection of Human Rights and Fundamental Freedoms. It means that collection of data and access to data must be restricted only in connection with fight against serious crime. To this end, the legal framework must foresee prior control of the court of independent administrative authority as prerequisite for access to data.

Presumption of innocence consists of different technics and doctrines that create a mechanism in criminal procedure for decreasing possible risk of making mistakes in course of the procedure for premature conviction of anyone. It is dealt with basic principle of fair proceeding the aim of which is to secure that national penal law would not be abused and that there would be established certain rules. By agency of the existing information, knowledge is formed from the big data in case of which existence of possible errors must be considered by using these. Formed decisions may bring along infringement of presumption of innocence as these may be interpreted falsely by forming evidence on the basis of these.

Digitally collected data are used in work of security and law enforcement authorities ever more. In case of these it is necessary to secure efficient control over necessity and proportionality of methods to be used in relation to suspicion of crime that is basis for collecting information. By carrying out conclusive decisions on the basis of big data, there is required existence of the experienced analyst who is able to furnish the existing data with necessary context nor would make premature conclusions on the basis of these. It must be taken into account that among the big data there may be consciously formed or false information emerged in course cyber-attacks that may bring along that the set of convicting implications.

The existing data creates for the analyst who is forming decisions the framework that is proceeded from by shaping decisions. The created framework is used by taking procedural decisions in relation to definite persons and if information exists about this person previously, then the person taking the decision or analyst must take these into account. This may bring along decisions of negative influence in relation to persons subject to examination as the analyst forming decisions may not assess the context of all information collecting and forms decisions on the basis of existing data without delving deeply into their context.

As a summary, the work brings forth that in nowadays era of big data, a lot of false information and false interpretation are spreading out in internet. Data existing in internet preserve for a long time and can be often referred to and used independent from users for what reason the persons are about to lose control over the use of data related to them. Collected data can be also used in context of criminal procedure that may bring along premature decisions and accompanying it infringement of presumption of innocence. In order to secure protection of fundamental freedoms of persons, there are created ever more legal instruments that enable more efficient protection in part of use, collecting, amending and deleting of data.

By this Master's thesis the author is hoping to contribute to raising awareness of influences related to use of big data by providing in his work an overview about the essence of big data, collecting of these and forming evidence on the basis of these as well as drawing attention to circumstance that on the basis of big data, false decisions may be formed that may bring along infringements of presumption of innocence. In the author's opinion, the issues handled in the Master's thesis have been handled scarcely in the Republic of Estonia, for what reason the work provides a good overview of positive as well as negative possibilities of use of big data and their influence by forming decisions.

# KASUTATUD KIRJANDUS


1. Aas, N. Riigi peaprokuröri ülevaade Riigikogu põhiseaduskomisjonile seadusega prokuratuurile pandud ülesannete täitmise kohta 2010. aastal. Tallinn 2011.
2. Akhgar, B., jt. Application of big data for national security: a practitioner´s guide to emerging technologies. 1 Ed. Amsterdam: Elsevier/Butterworth-Heinemann 2015.
3. Andmebaas. Kuidas vahet teha andmetel ja informatsioonil. Arvutivõrgus: http://andmebaas.ee/andmed-ja-informatsioon/ (25.04.2017).
4. Andmekaitse Inspektsioon. Metaandmed ja privaatsus: Juhis organisatsioonidele ja kodukasutajatele seaduse rakendamisel. 28. oktoober 2015. Arvutivõrgus: http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/Juhised/Metaandmed.pdf (25.11.2016).
5. Andmekaitse inspektsioon. Suurandmed ja privaatsus. Juhendmaterjal organisatsioonidele. 19. jaanuar 2017. Arvutivõrgus: http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/suurandmed_ja_privaatsus.pdf (15.03.2017)
6. Batini, C., Scannapieco, M. Data Quality: Concepts, Methodologies and Techniques (Data-Centric Systems and Applications). Springer-Verlag Berlin Heidelberg 2006.
7. Беккариа, Ч. О Преступлениях и наказаниях. Москва 2009.
8. Bennet, C. J. Regulating Privacy. Data Protection and Public Policy in Europe and the United States. Ithaca: Cornell University Press 1992.
9. Berman, J. J. Principles of Big Data: Preparing, Sharing, and Analyzing Complex Information. Elsevier Inc., 2013.
10. Big Data, Crime and Security. Houses of Parliament. July 2014, No 470. Arvutivõrgus: http://www.google.ee/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=0ahUKEwj8vdKdxOrKAhVDG5oKHeU-CboQFgggMAE&url=http%3A%2F%2Fresearchbriefings.files.parliament.uk%2Fdocuments%2FPOST-PN-470%2FPOST-PN-470.pdf&usg=AFQjCNEJdsdCcBFCr6tEtx7yyDS_hDAcNA (22.02.2016).
11. Birkinshaw, P. Freedom of Information: The Law, the Practice and the Ideal. 3. Ed. UK: Hobbs the Printers Ltd 2001.

12. BNS. Politsei võtab patrullsõidukites kasutusele uue e-politsei lahenduse. Postimees 26. juuni 2016.
Arvutivõrgus: http://www.postimees.ee/3743991/politsei-votab-patrullsoidukites-kasutusele-uue-e-politsei-lahenduse (12.03.2017).
13. Brenner, S. W. Cyberthreats and the Decline of the National-State. New York: Routledge 2014.
14. Brown, I. Communications Data Retention in an Evolving Internet. International Journal of Law and Information Technology, Vol. 19. Oxford University Press 2010, No 2.
15. Burns, M. Alleged CIA leak re-demonstrates the dangers of smart TVs. March 7, 2017. Arvutivõrgus: https://techcrunch.com/2017/03/07/recent-cia-leak-demonstrates-again-the-dangers-of-smart-tvs/ (17.03.2017).
16. Carrett, B. Big Data Is Changing Your World…More than You Know. United States, California: Columbia University Press, August 2013.
17. Civil Rights, Big Data and Our Algorithmic Future: A September 2014 report on social justice and technology. 2014.
Arvutivõrgus: https://bigdata.fairness.io/predictive-policing/ (22.02.2016).
18. Clough, J. Principles of Cybercrime. Cambridge: Cambridge University Press 2010.
19. Craig, T., Ludloff, M. E. Privacy and Big Data. O'Reilly 2011.
20. Corcos, C. Prosecutors, prejudices and justice: Observations on Presuming Innocence in Popular Culture and Law. University of Toledo law review. Louisiana State University Law Centre, Vol. 34, 2003.
21. Deflem, M. Sociology of Law. Cambridge: Cambridge University Press 2008.
22. Donohue, L. K. Section 702 and the Collection of International Telephone and Internet Content. Harvard Journal of Law & Public Policy, Vol 38, Winter 2015, Issue 1.
23. Dumbill, E. Big Data Now: 2012 Edition. 1 Ed. USA: O'Reilly Media, Inc., 2012.
24. Dumbill, E. Understanding the Data Value Chain: Adopt a different wiew of data as a raw mateerial for the data lifecycle bussiness resource. IBM Big Data & Analytics Hub, November 10, 2014.
Arvutivõrgus: http://www.ibmbigdatahub.com/blog/understanding-data-value-chain (18.03.2017)
25. E-teenused kui infosüsteem. Kokkuvõte: E-teenusele esitatavad nõuded.
Arvutivõrgus: http://e-teenus.weebly.com/kokkuvotildete.html (26.04.2017).

26. Eylandt, O. Eesti juurtega IT-geenius: ühes asjas Orwell eksis. Eesti Päevaleht, 7. jaanuar 2017.
Arvutivõrgus: http://m.epl.delfi.ee/article.php?id=76787520 (07.01.2017).
27. Fairfieldt, J. A. T., Luna, E. Digital Innocence. Cornell Law Review,Vol. 99, Issue 5.
28. Ferguson, A. G. Big Data and Predictive Reasonable Suspicion. University of Pennsylvania Law Review, Vol. 163, January 2015, No 2.
29. Flaherty, D. H. Protecting Privacy in Surveillance Societies. USA: The University of North Carolina Press 1989.
30. Frank, D. Privacy, Due Process and the Computational Turn: The philosophy of law meets the philosophy of technology. Routledge 2013.
31. Fung, B. The House just voted to wipe away the FCC´s landmark Internet privacy protections. The Washington Post, March 28, 2017.
Arvutivõrgus: https://www.washingtonpost.com/news/the-switch/wp/2017/03/28/the-house-just-voted-to-wipe-out-the-fccs-landmark-internet-privacy-protections/?utm_term=.0ed450ff7031 (30.03.2017).
32. Galetta, A. The changing nature of the presumption of innocence in today's surveillance societies: rewrite human rights or regulate the use of surveillance technologies? European Journal of Law and Technology, Vol. 4, 2013, No 2.
Arvutivõrgus: http://ejlt.org/article/view/221/377 (11.02.2017).
33. Gotev, G. Commission: Russian propaganda has deeply penetrated EU countries. Euroactiv, July 14, 2016.
Arvutivõrgus: https://www.euractiv.com/section/global-europe/news/thurs-commission-official-russian-propaganda-has-deeply-penetrated-eu-countries/ (26.02.2017).
34. Greenwald, G. Rand Paul Is Right: NSA Routinely Monitors Americans' Communications Without Warrants. The Intercept, March 13, 2017.
Arvutivõrgus: https://theintercept.com/2017/03/13/rand-paul-is-right-nsa-routinely-monitors-americans-communications-without-warrants/ (22.03.2017).
35. Gurin, J. Big data and open data: what's what and why does it matter? The Guardian, April 15, 2014.
Arvutivõrgus: https://www.theguardian.com/public-leaders-network/2014/apr/15/big-data-open-data-transform-government (16.03.2017).

36. Halilov, I. Propagandisliku narratiivi muutmine konfliktisituatsioonis: Ukraina kriisi näitel. Tartu Ülikool. Sotsiaal- ja haridusteaduskond. Riigiteaduste instituut. Magistritöö. 2015.
Arvutvõrgus: https://dspace.ut.ee/bitstream/handle/10062/47120/halilov_indrek_ma_2015.pdf? (23.03.2017).
37. Heater, B. Can your smart home be used against you in court? TechCrunch, March 12, 2017.
Arvutivõrgus: https://techcrunch.com/2017/03/12/alexa-privacy/ (17.03.2017).
38. Heldna, E. Julgeolekuasutuste kogutud informatsiooni kasutamine kriminaalmenetluses ja jagamine uurimisasutustega. Juridica 2016/X.
39. Hildebrandt, M. Criminal Law and Technology in A Data-Driven Society. The Oxford Handbook of Criminal Law. Oxford: Oxford University Press 2014.
40. Hildebrandt, M. Smart Tehnologies and the End(s) of Law: Novel Entanglements of Law and Technology. USA: Edward Elgar Publishing Inc., 2015.
41. Hu, M. Small Data Surveillance v. Big Data Cybersurveillance. Pepperdine Law Review, Vol. 42, 2014.
42. Hu, M. Taxonomy of the Snowden Disclosures. Washington and Lee Law Review, Vol. 72, Issue 4, September 1, 2015.
43. Internet Usage Statistics: The Internet Big Picture. Internet World Stats.
Arvutivõrgus: www.internetworldstats.com/stats.htm (22.02.2016).
44. Jackson, J. D., Summers, S. J. The Internationalisation of Criminal Evidence Beyond the Common Law and Civil Law Traditions. UK: Cambridge University Press 2012.
45. Jõesaar, T. Rootsi trollivabriku salapäraseid rahaasju aetakse Eestist. Eesti Päevaleht, 27. veebruar 2017.
Arvutivõrgus: http://epl.delfi.ee/news/eesti/rootsi-trollivabriku-salaparaseid-rahaasju-aetakse-eestist?id=77360858 (27.02.2017).
46. Kamm, L. Privaatsust säilitav andmeanalüüs. Sirp, 08. mai 2015.
Arvutivõrgus: http://www.sirp.ee/s1-artiklid/c21-teadus/privaatsust-sailitav-andmeanaluus/ (28.02.2017).
47. Kergandberg, E. Kriminaalmenetlus kui kullakaevandus. Juridica 2016/II.
48. Kergandberg, E. Natuke privaatsusest ja mõnevõrra enam selle jälitustegevuslikust riivest isikuandmeid töötleva Eesti avaliku võimu poolt. Juridica 2005/VIII.

49. Kergandberg, E., Pikamäe, P. Kriminaalmenetluse seadustik. Kommenteeritud väljaanne. Tallinn: Juura 2012.
50. Kergandberg, E., Sillaots, M. Kriminaalmenetlus. Tallinn: Juura 2006.
51. Kerr, I, Earle, J. How Big Data Threatens Big Picture Privacy. 66 Stan. L. Rev. Online 65, September 3, 2013.
52. Kert, E. Kuidas Big Data aitab teha paremaid krediidiotsuseid? Arvutivõrgus: https://web.creditinfo.ee/erki-kert-big-data.pdf (22.02.2016).
53. Kodar, E. Küberründed jõu kasutamise õiguse ja humanitaarõiguse raames – millised on mängureeglid? Diplomaatia nr 85, September 2010. Arvutivõrgus: http://www.diplomaatia.ee/artikkel/kuberrunded-jou-kasutamise-oiguse-ja-humanitaaroiguse-raames-millised-on-mangureeglid/ (22.02.2016).
54. Kogu riigi infosüsteem ühes autos. Riigi infosüsteemi teejuht: Eesti IT-edulood. Riigi Infosüsteemide Amet 2010. Arvutivõrgus: https://www.ria.ee/teejuht/eesti-it-edulood/kogu-riigi-infosusteem-uhes-autos (12.03.2017).
55. Komisjoni ettepanek võtta elektroonilise side valdkonnas vastu kõrgetasemelised eraelu kaitse normid ja ajakohastada EL-i institutsioonide andmekaitsenorme. Euroopa Komisjon – Pressiteade. Brüssel, 10. jaanuar 2017. Arvutivõrgus: www.europa.eu/rapid/press-release_IP-17-16_et.pdf (14.01.2017).
56. Kruusamäe, M., Reinthal, T. Kohtupraktika analüüs: Jälitustegevuse kohtulik eelkontroll Eestis. Tartu, 2013. Arvutivõrgus: http://www.riigikohus.ee/vfs/1503/6_Lisa%205_Jalitustegevuse%20analuus.pdf (20.06.2016).
57. Kwapien, A. How Big Data Helps To Fight Crime? Datapine, May 10, 2016. Arvutivõrgus: http://www.datapine.com/blog/big-data-helps-to-fight-crime/ (19.03.2017)
58. Laaneoks, E. Sissejuhatus võrgutehnoloogiasse. Tartu Ülikool: Matemaatika-informaatikateaduskond, arvutiteaduse instituut 2010. Arvutivõrgus: file:///C:/Users/kasutaja/Downloads/Sissejuhatus_vorgutehnoloogiasse.pdf (20.03.2017).
59. Lardinois, F. Google Home brings Google´s smarts to your living room. TechCrunch, November 3, 2016.

Arvutivõrgus: https://techcrunch.com/about/#about-tc (17.03.2017).

60. Ларин, А. М. Презумпции Невиновности. Москва: Наука, 1982.
61. Ларин, А. М., Темнов, Е. И. Латинские Юридические Изречения. Москва: Юрист, 1996.
62. Laugen, L. Rootsi on kübersõja kuningas, kes jälgib suurt osa Venemaa suhtlusest Läänemere kaabli kaudu. Delfi, 18. jaanuar 2017.
Arvutivõrgus: http://www.delfi.ee/news/paevauudised/valismaa/usa-valjaanne-rootsi-on-kubersoja-kuningas-kes-jalgib-suurt-osa-venemaa-suhtlusest-laanemere-kaabli-kaudu?id=76942876 (20.01.2017).
63. Li, X. Cybercrime and Deterrence: Networking Legal Systems in the Networked Information Society. Turku: Turun Yliopiston oikeustieellisen tiedekunnan julkaisuja. Yliopistollinen väitöskirja. 2008.
64. Liiv, I. Andmetest poliitika kujundamiseni: Uuring suurandmete ja teiste uuenduslike andmepõhiste meetodite võimalustest kujundada tõendustele tuginevat poliitikat. 2016. Arvutivõrgus: https://e-estonia.com/wp-content/uploads/2014/02/Data4policy_Raport_est_final.pdf (08.01.2017).
65. Linask, K., jt (tõlkijad). Aja jälg. Kui õiglane on õigus. Tallinn: Juura 2007.
66. Liu, E.C., Doyle, C. Goverment Collection of Privarte Information: Background and Issues Related to the USA PATRIOT Act Reauthorization in Brief. Congressional Research Service, May 19, 2015.
Arvutivõrgus: https://fas.org/sgp/crs/intel/R44042.pdf (22.03.2017).
67. Локшина, С. М. Краткий словарь иностранных слов. 6-е изд. Москва 1978.
68. Lõhmus, U. Elektroonilise side andmete säilitamise lõpetamata saaga. Juridica 2015/X.
69. Lõhmus, U. Elektroonilise side andmete säilitamise saaga sai lahenduse, Eestis siiski veel mitte. Juridica 2016/X.
70. Lõhmus, U. Põhiõigustest kriminaalmenetluses. Tallinn: Juura 2012.
71. Lõhmus, U. Põhiõigused kriminaalmenetluses. 2. tr. Tallinn: Juura 2014.
72. Lõhmus, U. Veel kord õigusest sõnumite saladusele ehk kuidas 20. sajandi tehnoloogia mõjutab põhiseaduse tõlgendusi. Juridica 2016/III.
73. Lõpparuanne: Uuring „Lingitud Eesti“. Tallinn 2014.
Arvutivõrgus: https://riigikantselei.ee/sites/default/files/content-editors/TOF/TOF_uuringud/lingitud_eesti_lopparuanne_2.0.pdf (04.01.2017).
74. Lyon, D. Surveillance, Snowden, and Big Data: Capacities, consequences, critique. Big Data & Society, July–December 2014.

75. Madise, Ü., jt. Eesti Vabariigi Põhiseadus: kommenteeritud väljaanne. Tallinn: Juura 2012.

76. Madise, Ü. Õiguskantsleri seisukoha edastamine. Tallinn: Õiguskantsleri Kantselei, 2015.
Arvutivõrgus: http://oiguskantsler.ee/sites/default/files/field_document2/6iguskantsleri_seisukoht_vastuolu_mittetuvastamise_kohta_elektroonilise_side_andmete_kogumine_sideettevotte_poolt.pdf (22.02.2016).

77. Magness, J. FISA Section 702: Is warrantless surveillance national security or a hitt o privacy? McClatchy DC BUREAU, March 1, 2017.
Arvutivõrgus: http://www.mcclatchydc.com/news/politics-government/congress/article135841918.html (22.03.2017).

78. Maruste, R. Konstitutsionalism ning põhiõiguste ja –vabaduste kaitse. Tallinn: Juura 2004.

79. McAfee, A., Brynjolfsson, E,. Big Data: The Management Revolution. Harvard Business Review, October 2012.
Arvutivõrgus: http://www.rosebt.com/uploads/8/1/8/1/8181762/big_data_the_management_revolution.pdf (16.03.2016).

80. Mcgarvey, S. The 2006 EC Data Retention Directive: A Systematic Failure. Hibernian Law Journal, Vol. 10, 2011.
Arvutivõrgus: http://www.heinonline.org.ezproxy.members.marshallcenter.org/HOL/Page?handle=hein.journals/hiblj10&div=9&start_page=119&collection=journals&set_as_cursor=0&men_tab=srchresults (31.08.2016).

81. Metcalf, K. N. Uuring: Privaatsusõigus inimõigusena ja igapäevatehnoloogiad. Privaatõiguse ja andmekaitse õiguslikud aspektid. Tartu Ülikool 2014.
Arvutivõrgus: http://www.humanrightsestonia.ee/wp/wp-content/uploads/2014/11/EST-Uuringu-V-osa-Privaat%C3%B5iguse-ja-andmekaitse-%C3%B5iguslikud-aspektid.pdf (23.03.2017).

82. Michaels, C. W. No Greater Threat: America After September 11 and the Rise of a National Security State. New York: Algora Publishing 2002.

83. Mozer, M. Big Data and You. New York: The Rosen Publishing Group, Inc., 2015.

84. Mueller, P., Yadegari, B. Report: The Stuxnet Worm. The University of Arizona: Arizona Computer Sciance 2012.
Arvutivõrgus: https://www2.cs.arizona.edu/~collberg/Teaching/466-566/2012/Resources/presentations/2012/topic9-final/report.pdf (27.02.2017).
85. Männiko, M. Õigus privaatsusele ja andmekaitse. Tallinn: Juura 2011.
86. NIST Big Data Interoperability Framework: Volume 1, Definitions. National Institute of Standards and Technology U.S Department of Commerce.
Arvutivõrgus: http://bigdatawg.nist.gov/_uploadfiles/NIST.SP.1500-1.pdf (22.02.2016).
87. NIST Big Data Interoperability Framework: Volume 3, Definitions. Use Cases and General Requirements. National Institute of Standards and Technology U.S Department of Commerce.
Arvutivõrgus: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1500-3.pdf (15.03.2017).
88. Nix, A. The Power of Big Data and Psychograohics. Concordia Summit 2016. Presentation.
Arvutivõrgus: https://www.youtube.com/watch?v=n8Dd5aVXLCc (10.03.2017).
89. Normet, M. Jälgimisühiskond ja mobiiltelefon. Akadeemia 2005/5.
90. Ollila, R. Freedom of Speech and Protection of Privacy in Convergence of Electronic Communications. Rovaniemi: Acta Universitatis Lapponiensis 41 2001.
91. Петрушевский, Д. М. Великая хартия вольностей и конституционная борьба в английском обществе во второй половине XIII века. Москва: Сабашниковы, 1915.
92. Polonetsky, J, Tene, O. Privacy and Big Data: Making ends meet. 66 Stan. L. Rev. 25, September 3, 2013.
93. Poom, R. Brexit ja Trump on omavahel seotud, neid ühendab varju hoidev ajupesumiljardär. Eesti Päevaleht 28. veebruar 2017.
Arvutivõrgus: http://epl.delfi.ee/news/valismaa/brexit-ja-trump-on-omavahel-seotud-neid-uhendab-varju-hoidev-ajupesumiljardar?id=77371654 (28.02.2017).
94. Privaatsus ja anonüümsus veebis. Tartu Ülikool. Arvutiteaduse Instituut.
Arvutivõrgus: https://courses.cs.ut.ee/2015/infsec/Et/Loeng-Anon%C3%BC%C3%BCmsusVeebis (01.03.2016).
95. Privacy International, UK. Big Data: Industrial Raw Material. An introduction to Data Protection. The European Digital Rights papers 2013, No 6.
96. Raska, E. Olemise õigus. Tallinn: Sisekaitseakadeemia 2010.

97. Raska, E. Õiguse apoloogia: sissejuhatus regulatsiooni sotsioloogiasse. Tartu: Fontese Kirjastus 2004.
98. Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies. Liberty and Security in a Changing World. December 12, 2013.
99. Roberts, P., Zuckerman, A. Criminal Evidence. Oxford: Oxford University Press 2004.
100. Roheline Raamat – Süütuse presumptsioon. Euroopa Komisjon. Brüssel, 26. aprill 2006. Arvutivõrgus: http://eur-lex.europa.eu/legal-content/ET/TXT/HTML/?uri=CELEX:52006DC0174&from=EN (12.02.2017).
101. Rondel, M. Informatsioonilise enesemääramise õigus ja jälitustegevus: isiku õigus teada saada tema suhtes tehtud jälitustoimingutest. Juridica 2016/X, lk 709-717.
102. Rudder, C. The Real Stuff White People Like. September 8, 2010. Arvutivõrgus: http://blog.okcupid.com/index.php/the-real-stuff-white-people-like/ (21.03.2016).
103. Saar, J. Õiguskultuur ja kuritegevuse kontroll. Juridica 2013/I.
104. Schneier, B. Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. W.W. Norton & Company, 2015.
105. Семигин, Г. Ю. Антология мировой политической мысли. Том 1. Москва: Мысль, 1999.
106. Siibak, A., Suder, S. Ülemus kui „suur vend". Arvutivõrgus: https://www.etis.ee/File/DownloadPublic/6fadddc4-cec1-45d5-b3a3-dcc7ccd85c6c?name=Fail_Siibak%26Suder.pdf&type=application%2Fpdf. (01.03.2016).
107. Sillaots, M. Kaitsja võimalikust rollist ja seisundist Eesti tulevases kriminaalmenetluses. Juridica 2000/II.
108. Sootak, J. Karistusõigus: üldosa. Tallinn: Juura 2010.
109. Sootak, J. Sanktsiooniõigus: karistusõiguslikud regulatsioonid ja nende kohaldamine. Tallinn: Juura 2007.
110. Steinbock, D. J. Data matching, data mining, and due process. Georgia Law Review. University of Toledo - College of Law, Vol. 40, Fall 2005, No 1.
111. Zbytniewska, K. Former RT presenter: Russian disinformation is a weapon. Euroactiv, Detsember 22, 2016. Arvutivõrgus: http://www.euractiv.com/section/global-europe/interview/former-rt-presenter-russian-disinformation-is-a-weapon/ (26.02.2017).

112. Zittrain, J. The Future of the Internet And How To Stop It. Yale University Press New Haven and London 2008.
113. Tammelo, I. Õiglus ja Hool. Tartu: Ilmamaa 2006.
114. The Secret Surveillance Catalogue. The Intercept.
Arvutivõrgus: https://theintercept.com/surveillance-catalogue/ (22.02.2016).
115. Toivonen, M. Big Data Quality Challenges in the Context of Business Analytics. University of Helsinki. Department of Computer Science. 2015.
Arvutivõrgus: http://hdl.handle.net/10138/156666 (04.02.2017)
116. Томсинов, В. А. Хрестоматия по истории государства и права зарубежных стран (Древность и Средние века). Москва: Зерцало, 1999.
117. Truuväli, E.-J., jt. Eesti Vabariigi põhiseadus: kommenteeritud väljaanne. 2. tr. Tallinn: Juura 2008.
118. Turvaline veebiliiklus: HTTPS. Miks internetiliiklust saab pealt kuulata ja jälgida. Tartu Ülikool: Loodus- ja täppisteaduste valdkond, arvutiteaduse instituut.
Arvutivõrgus: https://courses.cs.ut.ee/2015/infsec/Et/HTTPS (20.03.2017).
119. Черниловский, З. М. Всеобщая история государства и права.
Arvutivõrgus: http://www.gumer.info/bibliotek_Buks/Pravo/Chernil/ (10.01.2017).
120. Uibopuu, H. J. Inimõiguste rahvusvaheline kaitse – käsiraamat ja õpik ülikoolidele. Tallinn; Salzburg: Juura 2000.
121. Ушакова, Д. Н. Толковый словарь русского языка. Том 3. Москва 1994.
122. Verizon forced to hand over telephone data – full court ruling. The Guardian, June 6, 2013.
Arvutivõrgus: https://www.theguardian.com/world/interactive/2013/jun/06/verizon-telephone-data-court-order (23.03.2017).
123. Värv, A. Euroopa Kohtu Google'i otsus ja isiku õigus olla unustatud. Tallinn: Riigikogu Kantselei, õigus- ja analüüsiosakond 2014.
Arvutivõrgus: https://www.riigikogu.ee/wpcms/wp-content/uploads/2015/01/Teemaleht_20_2014.pdf (03.03.2017).
124. Wall, D. S. Cyberspace Crime. England: Dartmouth Publishing Company Ashgate Publishing Limited, 2003.
125. Wedde, P. jt. Digitalisierung Der Grundrechte? Zur Verfassungsvertraglichkeit der Informations- und Kommunikationstechnik. Westdeutcher Verlag GmbH, 1990.
126. Wyllie, D. How „Big Data" is helping law enforcement. August 20, 2013.

Arvutivõrgus: https://www.policeone.com/police-products/software/Data-Information-Sharing-Software/articles/6396543-How-Big-Data-is-helping-law-enforcement/ (22.02.2016).

# KASUTATUD ÕIGUSAKTID


127. Eesti Vabariigi põhiseadus. – RT 1992, 26, 349 … RT I, 15.05.2015, 2.
128. Elektroonilise side seadus. – RT I 2004, 87, 593 … RT I, 23.03.2017, 5.
129. Euroopa Liidu Põhiõiguste Harta. – 2012/C 326/02.
130. Euroopa Parlamendi resolutsioon 2013/2188(INI), 12. märts 2014, USA Riikliku Julgeolekuagentuuri jälgimisprogrammi ja EL-i liikmesriikide jälgimisasutuste ning nende mõju kohta EL-i kodanike põhiõigustele ja Atlandi-ülesele koostööle justiits- ja siseküsimustes.
131. Euroopa Parlamendi resolutsioon 2015/2612(RSP), 10. märts 2016, eduka andmepõhise majanduse suunas liikumise kohta.
132. Euroopa Parlamendi ja Nõukogu direktiiv 95/46/EÜ, 24. oktoober 1995, üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta – ELT L 281.
133. Euroopa Parlamendi ja Nõukogu direktiiv 2002/58/EÜ, 12. juuli 2002, isikuandmete töötlemist ja eraelu puutumatuse kaitset elektroonilise side sektoris (eraelu puutumatust ja elektroonilist sidet käsitlev direktiiv). – ELT L 201, lk 37-47 (eestikeelne eriväljaanne: ptk 13, kd 029, lk 514-524).
134. Euroopa Parlamendi ja Nõukogu direktiiv 2006/24/EÜ, 15. märts 2006, üldkasutatavate elektrooniliste sideteenuste või üldkasutatavate sidevõrkude pakkujate tegevusega kaasnevate või nende töödeldud andmete säilitamist, millega muudetakse direktiivi 2002/58/EÜ – ELT L 105/54.
135. Euroopa Parlamendi ja Nõukogu direktiiv 2011/0023 (COD), 02. veebruar 2011, mis käsitleb broneeringuinfo kasutamist terroriaktide ja raskete kuritegude ennetamiseks, avastamiseks, uurimiseks ja nende eest vastutusele võtmiseks.
136. Euroopa Parlamendi ja Nõukogu määrus (EL) nr 2016/679, 27. aprill 2016, millega kehtestatakse füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus). – ELT L 119.
137. Inimeste ja kodanikuõiguste deklaratsioon 1789.
Arvutivõrgus: http://www.concourt.am/hr/rus/un/6_5.htm (10.01.2017).
138. Inimõiguste ja põhivabaduste kaitse konventsioon. – RT II 2000, 11, 57.
139. Isikuandmete kaitse seadus. – RT I 2007, 24, 127 … RT I, 06.01.2016, 10.

140. Julgeolekuasutuste seadus. – RT I 2001, 7, 17 … RT I, 17.12.2015, 39.
141. Kaitsepolitseiameti poolt teabe varjatud kogumisel kasutatavad meetodid ja vahendid ning teabetoimiku pidamise ja säilitamise kord. – RTL 2001, 70, 945 … RT I, 07.02.2013, 9.
142. Kaitsepolitseiameti põhimäärus. – RT I, 15.02.2017, 6.
143. Karistusseadustik. – RT I 2001, 61, 364 … RT I, 31.12.2016, 14.
144. Karistusregistri seadus. – RT I, 21.03.2011, 3 … RT I, 30.12.2015, 17.
145. Kriminaalmenetluse seadustik. – RT I 2003, 27, 166 … RT I, 31.12.2016, 46.
146. Riigipiiri seadus. – RT I 1994, 54, 902 … RT I, 06.04.2016, 11.
147. Vabariigi Valitsuse korraldus „Valitsusasutustele ja valitsusasutuste hallatavatele riigiasutustele 2015. Aastaks määratud tööjõu- ja majandamiskulude jaotus, investeeringute ja investeeringutoetuste objektiline liigendus ning ministeeriumide ja nende valitsemisala riigiasutuste 2015. aasta tegevuskavad“ Lisa 3. Arvutivõrgus: https://www.riigiteataja.ee/aktilisa/3311/2201/4001/581klisa3.pdf (20.01.2017).

# KASUTATUD KOHTUPRAKTIKA


148. EIKo 30562/04 ja 30566/04, *S. ja Marper v. Ühendkuningriik*.
149. EIKo 4378/02, *Bykov v. Russia*.
150. EIKo 5029/71, *Klass and others v. Germany*.
151. EKo C-131/12, *Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González.*
152. EKo C-203/15 ja C-698/15, *Tele2 Sverige AB v. Post-och telestyrelsen and Secretary of State for the Home Department v. Tom Watson and others*.
153. EKo C-293/12 ja C-594/12, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*.
154. RKKKo 3-1-1-22-10.
155. RKKKo 3-1-1-70-11.
156. RKKKo 3-1-1-136-13.
157. RKKKo 3-1-1-51-14.
158. RKKKo 3-1-1-94-14e.
159. RKKKo 3-1-1-93-15.
160. RKKKo 3-1-1-64-16.
161. RKKKo 3-1-1-79-16.

# LÜHENDID

| | |
|---|---|
| CIA | Ameerika Ühendriikide Luure Keskagentuur |
| EIK | Euroopa Inimõiguste Kohus |
| EIÕK | Euroopa inimõiguste ja põhivabaduste kaitse konventsioon (ka Euroopa inimõiguste konventsioon) |
| EL | Euroopa Liit |
| ESS | Elektroonilise side seadus |
| EV | Eesti Vabariik |
| FISA | The Foreign Itelligence Act |
| FBI | Föderaalne Juurdlusbüroo |
| FRA | Rootsi riigikaitse raadioasutus Försvarets Radioanstalt |
| IKT | Info- ja kommunikatsioonitehnoloogia |
| JAS | Julgeolekuasutuste seadus |
| KAPO | Kaitsepolitseiamet |
| KarS | Karistusseadustik |
| KrMS | Kriminaalmenetluse seadustik |
| NSA | Rahvuslik Julgeolekuagentuur |
| PPA | Politsei- ja Piirivalveamet |
| PS | Põhiseadus |
| RKKK | Riigikohtu kriminaalkolleegium |
| RT | Russia Today |
| USA | Ameerika Ühendriigid |
| USA PATRIOT ACT | Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 |
| VF | Vene Föderatsioon |

# LISA 1. NSA ANDMETE KOGUMISEGA SEONDUVAD PROGRAMMID

a. Metaandmete[319] kogumise programm – NSA kogus miljonite USA telefonioperaatorite klientide suhtlusandmeid (nt mõlema helistajapoole andmed, helistaja asukohaandmed, kõne kestvus, unikaalsed identifitseerimisandmed). Andmeid koguti täismahus olenemata sellest, kas isikuid kahtlustati millegi toimepanemises või mitte.

b. PRISM – programm, mille kaudu kogutakse veebilehtede unikaalseid aadresse ja elektroonilisi andmeid, mis on seotud suuremate teenusepakkujatega nagu *Gmail*, *Outlook*, *Facebook* jne. Kogutud materjali jagatakse järjepidevalt USA-s nii FBI kui ka CIA-ga.

c. UPSTREAM – fiiberoptilise infoedastuse jälgimise programm, mille abil kogutakse nii metaandmeid kui ka kommunikatsiooni sisu, mis liiguvad läbi fiiberoptiliste kaablite. Tegemist on ühe infoallikaga, mille põhjal koostatakse näiteks USA-s igapäevaselt presidendile julgeolekuküsimuste päevaülevaateid.

d. SHELL TRUMPET – programm, mis alustas kui reaalajas toimiv metaandmete analüsaator. Viie aastase tegevuse käigus kujunes sellest aga välja mitmeid töötlusvõimalusi ja kontrollivõimekusi omav süsteem, mis suudab muuhulgas edastada näiteks e-posti teel otseteavitusi. 31. detsembriks 2012 oli süsteemi abil töödelnud üle triljoni metaandme kirje.

e. SNACKS – sotsiaalvõrgustiku analüüsi programm, mis suudab välja pakkuda organisatsioonide personali hierarhia konkreetse struktuuri. Ehk siis olemasolevate andmete põhjal mudeldada ettevõtte juhtimisstruktuuri.

f. XKEYSCORE – programm, mis kogub, analüüsib ja võimaldab teha otsinguid olemasolevatest andmetest. Lisaks võimaldab süsteem analüütikutel vaadelda kõike, mida tavaline internetikasutaja teeb ehk e-posti sisu, milliseid lehekülgi kasutaja külastab ja milliseid otsinguid teostab.

[319] Metaandmed on andmed, mis sisaldavad teavet muude andmete kohta. See on teave, mis tekib siis, kui kasutatakse erinevaid infotehnilisi lahendusi ja süsteeme ning mis annab teada, kes, mida, kus, millal ja kuidas tegi. (IP-aadress ja privaatsus: Juhis organisatsioonidele ja kodukasutajatele seaduse rakendamisel. Andmekaitse Inspektsioon.) Arvutivõrgus: http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/Juhised/Metaandmed.pdf (25.11.2016)).

# LISA 2. NSA RÜNNAKUPROGRAMMID

a. QUANTUMHAND – on sotsiaalvõrgustiku lehekülgedele paigutatud varjatud pahavara. See võimaldab varjatult teeseldes mõnda *Facebook*-i lehekülge, mida jälgitav isik kasutab ning selle abil tungida jälgitava isiku arvutisse ja vaadelda tema arvuti kõvakettal olevad andmed.

b. QUANTUMSKY ja QUANTUMCOPPER – programmid, mille abil on võimalik blokeerida võimalikke sihtmärke ehk sulgeda juurdepääsu teatatud veebilehekülgedele. Programmid võimaldavad tõkestada ka failide allalaadimist.

c. SECONDDATE ja FOXACID – veebilehitsejate ümbersuunamise pahavarad. SECONDDATE suudab mõjutada reaalajas toimuvat kommunikatsiooni kliendi ja serveri vahel ning suunata veebilehitseja NSA pahavara serverisse nimega FOXACID.

d. TURBINE – programm, mille tehnoloogia võimaldab pahavara sisendeid suunates mõjutada kümneid miljoneid arvuteid maailmas. Tegemist on automatiseeritud arvutitesse tungimise ja jälgimise tehnoloogiaga, mis võimaldab NSA-l tungida väljavalitud rünnatavatesse arvutitesse ning luurata välismaa internetiliiklust ja arvutivõrke.

**Lihtlitsents lõputöö reprodutseerimiseks ja lõputöö üldsusele kättesaadavaks tegemiseks**

Mina **OLGERT RÕÕM**

(sünnikuupäev: 29. oktoober 1977)

1. annan Tartu Ülikoolile tasuta loa (lihtlitsentsi) enda loodud teose

**SÜÜTUSE PRESUPMOTSIOON SUURANDMETE AJASTUL**

mille juhendajad on *J.S.D* Helen Eenmaa-Dimitrieva, *LL.M* Kaspar Kala, *mag. iur.* Andres Parmas

1.1. reprodutseerimiseks säilitamise ja üldsusele kättesaadavaks tegemise eesmärgil, sealhulgas digitaalarhiivi DSpace-is lisamise eesmärgil kuni autoriõiguse kehtivuse tähtaja lõppemiseni;

1.2. üldsusele kättesaadavaks tegemiseks Tartu Ülikooli veebikeskkonna kaudu, sealhulgas digitaalarhiivi DSpace´i kaudu kuni autoriõiguse kehtivuse tähtaja lõppemiseni.

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

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

Tartus, 28. aprill 2017