TARTU ÜLIKOOL
SOTSIAALTEADUSTE VALDKOND
ÕIGUSTEADUSKOND
Avaliku õiguse osakond

Marion Kallakas

Õiguslik alus eriliigiliste biomeetriliste andmete töötlemiseks eraõiguslikes suhetes

Magistritöö

Juhendajad
MA Kärt Salumaa-Lepik
Dr. Helen Eenmaa-Dimitrieva

Tartu

2019

Sisukord

Sissejuhatus

Biomeetriliste tehnoloogiate levik viimastel aastatel ei ole tõenäoliselt kellelgi märkamata jäänud. Näo- või häältuvastustehnoloogiad ja sõrmejälje lugerid on kasutusel lugematutes tarbeseadmetes isiklikest mobiiltelefonidest kuni kontori ukselukuni. Biomeetrilised tuvastustehnoloogiad on Eestis viimasel ajal palju tähelepanu saanud ka *startup* maailmas. Näiteks seisneb ühe hetkel Eesti edukama iduettevõtte Veriffi teenus pankadele näotuvastustehnoloogia pakkumises, et pangad saaksid tuvastada klientide isikusamasust.[1] Samuti näeb üha rohkem tarkvaraettevõtteid spetsialiseerumas biomeetriliste tehnoloogiate arendamisele. Ühe näitena avas tarkvaraettevõte Helmes oma töötajatele biomeetrilise raamatukogu, kust saab näotuvastuse abil raamatuid laenutada.[2] Maailma perspektiivis on biomeetriliste tehnoloogiate valdkond üks kiiremini kasvavaid infotehnoloogia suundi, mida demonstreerib ka asjaolu, et enim investeeringuid kaasavad just biomeetria iduettevõtted.[3] Biomeetriliste tehnoloogiatega puutub kokku nii asjade internetis, riiklikes ID-süsteemides, piirikontrollis, makseteenustes, interneti analüütika tööriistades ja veel paljudes muudes valdkondades. Samal ajal on kõik need arengud alles võrdlemisi uued ja seetõttu vajab vastav õiguslik regulatsioon täpsustamist.

Eelneva valguses toodi andmekaitse reformi paketi raames Euroopa andmekaitse maastikule ka uus isikuandmete liik: biomeetrilised andmed. Biomeetrilised isikuandmed lisati nii 2018. mais jõustunud Euroopa Parlamendi ja Nõukogu määrusesse (EL) 2016/679 füüsiliste isikute kaitse kohta isikuandmete töötlemisel[4] (edaspidi Määrus) kui ka politseikoostöö ja õigusalase koostöö Direktiivi (EL) 2016/680[5] (edaspidi politseikoostöö ja õigusalase koostöö Direktiiv). Kuni andmekaitse reformi paketi vastuvõtmiseni käsitlesid Euroopa tasandil biomeetrilisi isikuandmeid ainult avaliku sektori õigusaktid, nagu sõrmejälgede kogumine kriminaalõiguses

[1] R. Liive. Eestlaste idufirma Veriff lubab maailma kõige turvalisemat isikutuvastamise teenust. – Digigeenius 28.06.2016. Kättesaadav arvutivõrgus: https://digi.geenius.ee/rubriik/uudis/eestlaste-idufirma-veriff-lubab-maailma-koige-turvalisemat-isikutuvastamise-teenust/.

[2] I. Kald. Helmes käivitas näotuvastusega raamatulaenutuse. Äripäev. ITuudised 23.11.2018. Kättesaadav arvutivõrgus: https://www.ituudised.ee/uudised/2018/11/23/helmes-kaivitas-naotuvastusega-raamatulaenutuse.

[3] A. Janofsky. Facial Recognition, Robotic Process Automation Companies Among Most-Funded AI Startups. 14.02.2019. Kättesaadav arvutivõrgus: https://www.wsj.com/articles/facial-recognition-robotic-process-automation-companies-among-most-funded-ai-startups-11550138401.

[4] Euroopa Parlamendi ja Nõukogu määrus (EL) 2016/679, 27. aprill 2016, füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiiv 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus). – ELT L119, 04.05.2016, lk 1-88. Edaspidi Määrus.

[5] Euroopa Parlamendi ja nõukogu direktiiv (EL) 2016/680, 27. aprill 2016, mis käsitleb füüsiliste isikute kaitset seoses pädevates asutustes isikuandmete töötlemisega süütegude tõkestamise, uurimise, avastamise ja nende eest vastutusele võtmise või kriminaalkaristuste täitmisele pööramise eesmärgil ning selliste andmete vaba liikumist ning millega tunnistatakse kehtetuks nõukogu raamotsus 2008/977/JSK. – ELT L 119, 04.05.2016, lk 89–131, art 3 p 14. Kättesaadav arvutivõrgus: https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=celex%3A32016L0680.

või piirikontrollis biomeetriliste isikuandmete töötlemine.[6] Rahvusvahelistes instrumentides puudusid selged sätted biomeetriliste isikuandmete kontseptsiooni kohta erasektoris ja reeglid, mis reguleeriks nende töötlemist. See selgitab varasemat ühtse arusaama puudumist biomeetrilistest isikuandmetest. Näiteks olid biomeetrilised isikuandmed mõnes riigis, sh Eestis, delikaatsete isikuandmete nimekirjas,[7] kuid mitmes teises Euroopa Liidu (edaspidi EL) liikmesriigis vastav õigusakt neid isegi ei nimetanud.

Samas on mitmed EL liikmesriikide andmekaitse järelevalveasutused avaldanud arvamusi või soovitusi biomeetriliste isikuandmete töötlemiseks nii enne Määrust kui Määruse tõlgendamiseks.[8] Määrus lisas biomeetrilised isikuandmed *expressis verbis* eriliigiliste isikuandmete nimekirja. Erinevalt teistest eriliigilistest isikuandmetest Määruse artiklis 9 lg 1, ei ole biomeetrilised andmed seal nimekirjas absoluutsel kujul, vaid artikkel 9 ütleb: „Keelatud on töödelda /---/ füüsilise isiku kordumatuks tuvastamiseks kasutatavaid biomeetrilisi andmeid /---/.“[9] Seega jääb esmapilgul mulje, et eriliigilisteks isikuandmeteks klassifitseerumise piirmäär biomeetrilistele andmetele on nende kasutamise viis. Määrus aga ei selgita, mida tähendab niivõrd oluline „kordumatu tuvastamise“ funktsioon, millest sõltub kas biomeetriliste andmete töötlemine on keelatud või mitte. Määruse artikkel 4 p 14 annab biomeetriliste isikuandmete definitsiooni, mis on järgnev: „konkreetse tehnilise töötlemise abil saadavad isikuandmed isiku füüsiliste, füsioloogiliste ja käitumuslike omaduste kohta, mis võimaldavad kõnealust füüsilist isikut kordumatult tuvastada või kinnitavad selle füüsilise isiku tuvastamist, näiteks näokujutis ja sõrmejälgede andmed.“[10] Definitsioon sisaldab endas kahte andmete tüüpi, mida võiks lugeda biomeetrilisteks isikuandmeteks. Esimene tüüp on seotud inimese keha tunnustega ehk füüsilised või füsioloogilised tunnused. See andmete tüüp on suhteliselt otseselt arusaadav ja kooskõlas sellega, mida inimesed üldiselt biomeetriliste andmete all mõistavad, näiteks sõrmejäljed ja silmaiirisekujutis. Teine andmete tüüp on seotud

[6]Euroopa Parlamendi ja nõukogu määrus (EÜ) nr 1987/2006, 20. detsember 2006 , mis käsitleb teise põlvkonna Schengeni infosüsteemi (SIS II) loomist, toimimist ja kasutamist. - ELT L 381, 28.12.2006, lk 4-23, art 1, lg 2. https://eur-lex.europa.eu/legal-content/ET/ALL/?uri=CELEX:32006R1987; Euroopa Parlamendi ja nõukogu määrus (EÜ) nr 444/2009, 28. mai 2009 , millega muudetakse nõukogu määrust (EÜ) nr 2252/2004 liikmesriikide väljastatud passide ja reisidokumentide turvaelementide ja biomeetria standardite kohta. – ELT L 142, 6.6.2009, p. 1–4.

[7] Isikuandmete kaitse seadus, RT I 2007, 24, 127. Edaspidi IKS.

[8] Commission Nationale de l'informatique et des Libertés. Les dispositifs biométriques pour l'accès aux cantines scolaires. 23. 11.2015. Kättesaadav arvutivõrgus: https://www.cnil.fr/fr/les-dispositifs-biometriques-pour-lacces-aux-cantines-scolaires; Commission Nationale de l'informatique et des Libertés. Le contrôle d’accès biométrique sur les lieux de travail. 28.03.2019. – Kättesaadav arvutivõrgus: https://www.cnil.fr/fr/le-controle-dacces-biometrique-sur-les-lieux-de-travail.

[9] Määrus art 9 lg 1.

[10] Määrus art 4 p 14.

informatsiooniga inimese käitumisest ja on seetõttu laiem. Selle järgi peaks inimese iga käitumuslik tunnus, mis võimaldab teda teistest inimestest eristada, olema biomeetrilised isikuandmed.

Alates Määruse vastuvõtmisest on õiguskirjanduses oldud valdavalt seisukohal, et Määrus ei lahenda probleemi biomeetriliste andmete kasutamisega ja liikmesriikidelt on vaja sinna juurde juhendeid või eriregulatsioone siseriiklikes õigusaktides.[11] Näiteks tekitab vastuolulisi arvamusi artikli 4 definitsioon.[12] Teiseks on Määrus püüdnud artiklitega 4 ja 9 jagada biomeetrilised andmed nn tavalisteks ja eriliigilisteks isikuandmeteks. Siin jällegi esineb eriarvamusi, millised biomeetrilised andmed on eriliiglised isikuandmed.[13] Kogu vastutus isikuandmete olemuse määratlemise ja õige klassifitseerimise eest lasub aga ainuüksi vastutaval töötlejal.

Vahe tegemine, kas biomeetriliste andmete puhul on tegemist nn tavaliste või eriliigiliste isikuandmetega, on oluline vastutavale töötlejale töötlemiseks õigusliku aluse valikul. Probleemiks füüsilistele, füsioloogilistele ja käitumuslikele tunnustele vastavate isikuandmete töötlemisel saab asjaolu, et on ebaselge, millisel ajahetkel muutuvad nn tavalised isikuandmed biomeetrilisteks andmeteks ja sealt edasi eriliigilisteks biomeetrilisteks andmeteks. Eriliigiliste biomeetriliste andmete töötlemine on lubatud vaid artikkel 9 lg 2 toodud erandite alusel. Enamasti on aga biomeetriliste andmete töötlemine hall ala, kus õigusliku aluse valik sõltub igal üksikul juhul kasutatavast tehnoloogiast ja töötlemise eesmärgist. Kui vastutav töötleja ei liigita biomeetrilisi andmeid korrektselt ega vali õiget õiguslikku alust, siis töötleb ta isikuandmeid ilma õigusliku aluseta ehk ebaseaduslikult.

Eelnevast tulenevalt käesolev magistritöö uurib, kuidas vastutav töötleja peaks valima sobiva õigusliku aluse eriliigiliste biomeetriliste andmete töötlemiseks erasektoris. Täpsemalt keskendutakse õigusliku aluse valikule olukorras, kus vastutav töötleja soovib vabatahtlikult pakkuda või kasutada biomeetrilist tuvastamist. Seega on fookuses õigusliku alusena eelkõige andmesubjekti selgesõnaline nõusolek biomeetriliste teenuste kasutamisele kui üldine

[11] E. J. Kindt. Having yes, using no? About the new legal regime for biometric data. - Computer Law & Security Review. 2018/6, Vol 34, No 3, lk 523-538. Edaspidi Kindt 2018; C. Jasserand. Legal Nature of Biometric Data: From Generic Personal Data to Sensitive Data. - European Data Protection Law Review 2016/2. Edaspidi Jasserand; P. de Hert, V. Papakonstantinou. The new General Data Protection Regulation: Still a sound system for the protection of individuals? - Computer Law & Security Review 2016, Vol 32, No 2. Edaspidi P. de Hert, V. Papakonstantinou.

[12] Kindt 2018; Jasserand; A. Krausova. Online Behavior Recognition: Can We Consider It Biometric Data under GDPR. - Masaryk University Journal of Law and Technology 2018, Vol 12. Edaspidi Krausova.

[13] P. de Hert, V. Papakonstantinou; Krausova; Kindt 2018.

eriliigiliste isikuandmete töötlemise alus Määruse artiklist 9 lg 2 p a. Sellegipoolest ei ole andmesubjekti nõusolek igas olukorras kõige sobivam alus ja seetõttu võrreldakse eri olukordades konkureerivaid õiguslikke aluseid. Kuna Määruse artikkel 9 klassifitseerib biomeetrilised andmed eriliigilisteks vaid nende kasutuse eesmärgist lähtuvalt, siis keskendub magistritöö analüüs ka eriliigiliste biomeetriliste andmete tuvastamisele olukordades, kus töötlemisel on mitu eesmärki. Magistritöö hüpotees on, et Eesti õiguses on vaja sätestada Määrusest täpsem regulatsioon eriliigiliste biomeetriliste isikuandmete töötlemiseks. Magistriöös vastatakse järgmistele küsimustele:

1. Mis on biomeetrilised isikuandmed Määruse mõistes?
2. Millal on biomeetriliste isikuandmete puhul tegemist eriliigiliste isikuandmetega ja millal mitte?
3. Milline õiguslik alus on vastutavale töötlejale potentsiaalselt kõige sobivam eriliigiliste biomeetriliste andmete töötlemiseks erinevate valdkondade lõikes?
4. Millistele tingimustele peab vastama andmesubjekti selgesõnaline nõusolek eriliigiliste biomeetriliste andmete töötlemiseks?
5. Kas ja kuidas oleks vaja täiustada Eesti õigust biomeetriliste isikuandmete töötlemise seisukohalt?

Uurimisküsimustest tulenevalt on magistritöö jaotatud kolmeks osaks.

Esimese osa eesmärk on analüüsida uut biomeetriliste andmete definitsiooni Määruses ja tuvastada konkreetsed probleemkohad nii biomeetriliste andmete määratlemises kui õigusliku aluse valikus. Selleks analüüsitakse Määruse artiklis 4 p 14 toodud biomeetriliste andmete definitsiooni elemente. Autor võrdleb definitsiooni elemente senise Euroopa Kohtu (edaspidi EK) ja Euroopa Inimõiguste Kohtu (edaspidi EIK) praktikaga biomeetriliste isikuandmete vallas ja praktikas kasutatavate isikuandmete töötlemisviisidega. Sealjuures antakse ülevaade üldistest biomeetriliste andmete tunnustest, mida kasutatakse magistritöö teistes osades erinevate töötlemisviiside hindamiseks. Viimaseks võrdleb autor Määruse biomeetriliste andmete definitsiooni artiklis 9 lg 1 toodud eriliigiliste isikuandmete klassifikatsiooniga ja esimeses osas vastatakse küsimusele, kuidas erinevad eriliigilised biomeetrilised andmed nn tavalistest biomeetrilistest andmetest.

Teine osa keskendub biomeetriliste tehnoloogiate kasutamisele eesmärgiga füüsiline isik kordumatult tuvastada. Sellisel eesmärgil biomeetriliste isikuandmete kasutamisel on kõige tõenäolisem, et vastutav töötleja töötleb eriliigilisi biomeetrilisi andmeid. Tuvastamaks,

millised on vastutava töötleja valikud õigusliku aluse valimisel, võrreldakse biomeetrilise tuvastustehnoloogia kasutamist andmesubjekti osalusel ja ilma andmesubjekti enda osaluseta, näiteks internetist kättesaadava info põhjal. Õiguslike aluste analüüsiks uuritakse biomeetriliste isikuandmete töötlemist finantssektoris, kui valdkonda, kus uutel biomeetrilistel tehnoloogiatel arvatakse olevat kõige suurem mõju.[14] Uuritakse ka õiguslikke aluseid töökohas biomeetrilise tuvastustehnoloogia kasutamiseks, sest töösuhted on valdkond, kus tööandjal on võimupositsioonist tulenevalt raske tugineda isikuandmete töötlemisel töötaja nõusolekule.[15] Käesolevast magistritööst jäetakse välja isikuandmete töötlemine ajakirjanduses, näiteks fotod ajalehtedes, sest ajakirjandusele lubatavad õiguslikud alused väljuvad magistritöö teema püstitusest. Analüüsi tulemusena leitakse, millal on andmesubjekti selgesõnaline nõusolek kõige sobivam õiguslik alus vastutava töötleja jaoks ja millal on see kohustuslik. Viimaseks leitakse, millistele kriteeriumitele peab vastama andmesubjekti selgesõnaline nõusolek biomeetriliste tuvastusteenuste kasutamiseks.

Kolmandas osas uuritakse biomeetriliste tehnoloogiate kasutamise nö halli ala, kus töötlemise eesmärgiks ei ole otseselt isikut tuvastada ja esmapilgul ei ole selge, kas tegemist on eriliigiliste või nn tavaliste biomeetriliste andmete töötlemisega. Eelkõige keskendutakse analüüsis asjade internetile, internetis kasutajate käitumist analüüsivatele tööriistadele ja profiilianalüüsi eristamisele biomeetrilisest tuvastamisest. Osa eesmärk on tuvastada juhud, millal muutuvad tavalised inimese füüsilised või käitumuslikud tunnused teatud tehnoloogiates kasutades Määruse järgi biomeetrilisteks andmeteks. Teisisõnu leitakse millal peab vastutav töötleja arvestama, et õiguslik alus isikuandmete töötlemise käigus muutub ja mis juhtudel peab vastutav töötleja juba töötlemist planeerides eeldama, et töötlemine viib biomeetriliste või eriliigiliste biomeetriliste andmete töötlemiseni. Osa lõpetuseks teeb autor ettepanekud õiguslikult reguleerida eriliigiliste biomeetriliste isikuandmete töötlemist Eestis.

Püstitatud uurimisküsimustele vastamiseks kasutab autor hermeneutilist-argumentatiivset meetodit. Selline meetod on sobivaim, kui peamiseks uurimisobjektiks on dokument ja selle tõlgendamine.[16] Seega kasutatakse hermeneutilist-argumentatiivset meetodit Määruse analüüsiks, sest peamine uurimisobjekt on Määruse artiklite 4 ja 9 tekstid ja nende tõlgendamine. Meetod on ühtlasi argumentatiivne, sest vastuseid leitakse konkreetsetele

[14] A. Goode. Biometrics for banking: best practices and barriers to adoption. - Biometric Technology Today. Vol 2018, No 10, lk 5-7. Edaspidi Goode.
[15] Määrus, preambul p 155; Artikkel 29 Töörühm. Guidelines on consent under Regulation 2016/679. Lk 7.
[16] M. V. Hoecke (koost). Methodologies of Legal Research. Which Kind of Method for What Kind of Discipline? Oxford ja Portland, Oregon: Hart Publishing 2011, lk 4.

küsimustele[17] ja Määruse tõlgendamiseks kasutatakse suures osas teaduskirjandust, milles esitatud seisukohti kinnitatakse või seatakse kahtluse alla. Teiseks kasutab autor analüütilist meetodit kuivõrd analüüsitakse EIK ja EK tehtud otsuseid biomeetriliste andmete vallas ja antakse hinnang Määruse kooskõlale senise kohtupraktikaga. Neid otsuseid on väga vähe ja ainus Euroopa-ülene erasektoris biomeetriliste andmete kasutamist reguleeriv normatiivne allikas on Määrus, mistõttu ei saa kogu töö tugineda analüütilisele meetodile. Eelnevatega kombineeritult kasutatakse võrdlevat analüüsi. Võrdleva analüüsi jaoks kasutatakse EL liikmesriikide andmekaitse järelevalveasutuste arvamusi ja otsuseid, et tuvastada ühtsete mustrite olemasolu biomeetriliste isikuandmete valdkonnas.

Magistritöö argumentatsiooni toetavad peamiselt isikuandmete kaitse direktiivi 95/46/EÜ[18] (edaspidi Direktiiv 95/46/EÜ) artikkel 29 alusel loodud Artikkel 29 Andmekaitse Töörühma[19] (edaspidi Artikkel 29 Töörühm) ja Euroopa andmekaitseinspektori avaldatud arvamused. Nende arvamused kajastavad üldist praktikat või konsensust Euroopa Liidus. Direktiivis 95/46/EÜ otsesõnu küll biomeetrilisi isikuandmeid nimetatud ei olnud, küll aga on Artikkel 29 Töörühm alates 2003. aastast avaldanud arvamusi biomeetrilistest andmetest ja lugenud need Direktiivi 95/46/EÜ mõistes isikuandmeteks.[20] Mõned kasutatavad arvamused on lugenud kehtivaks ka Määruse alusel loodud uus nõuandev organ Andmekaitsenõukogu. Kuigi ülejäänud Artikkel 29 Töörühma arvamused ei ole siduvad, annavad nad siiski ülevaate arutelust ja suurematest probleemkohtades biomeetriliste andmete kasutuse levikul Euroopas. Kuna tegemist on ka niivõrd uue tehnoloogiaga erasektoris, siis kõik EK ja EIK lahendid käsitlevad vaid biomeetriliste isikuandmete töötlemist avalikus sektoris. Sellest hoolimata neid lahendeid kasutatakse käesolevas magistritöös ulatuses, milles autori hinnangul biomeetriliste isikuandmete töötlemine peaks olema ühesugune nii avalikus kui erasektoris. Kasutatud on ka Euroopas biomeetriliste isikuandmete valdkonna ekspertide artikleid ja raamatuid, eelkõige E. J. Kindt, P. de Hert, C. Jasserand ja R. Yampolskiy. Magistritöös on nende seisukohti võrreldud ja antud autoripoolne hinnang õigusliku aluse valikust lähtuvalt. Magistritöid eriliigiliste isikuandmete õiguslike aluste kohta Määruse järgi on küll juba avaldatud Eestis mitmeid,

[17] *Ibid*.
[18] Euroopa Parlamendi ja nõukogu direktiiv 95/46/EÜ, 24. oktoober 1995, üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta. ELT L 281, 23.11.1995. Edaspidi Direktiiv 95/46/EÜ.
[19] Direktiiv 95/46/EÜ alusel loodi töörühm, kes koosnes liikmesriikide andmekaitse järelevalveasutuste esindajatest, Euroopa andmekaitseinspektorist ja Euroopa Komisjoni esindajaist. Töörühmal oli nõuandev roll Direktiivi rakendamise ja tõlgendamise osas. Alates 2018. aastast asendati töörühm Määruse alusel loodud Andmekaitsenõukoguga.
[20] Artikkel 29 Andmekaitse Töörühm. Working Document on biometrics. 12168/02/NE, WP80, 01.08.2003, lk 4.

näiteks S. Velbri[21] ja M.-L. Piiskop[22] 2018. aastal, kuid need magistritööd on liiga üldised biomeetriliste andmete töötlemiseks sobiva õigusliku aluse hindamiseks. Biomeetrilisi isikuandmeid on põhjalikumalt käsitlenud 2015. aastal magistritöös J. Antonova, kuid seda kriminaalmenetluse kontekstis.[23]

Lisaks eelnevale on käesolevas magistritöös kasutatud ka Suurbritannia, Iirimaa, Prantsusmaa, Saksamaa, Poola ja Belgia andmekaitse järelevalveasutuste juhiseid. Neist enim on kasutatud Prantsusmaa *Commission Nationale de l'informatique et des Libertés* (edaspidi CNIL) arvamusi ja otsuseid, sest Prantsusmaal on Euroopas kõige põhjalikum ja pikaaegsem erasektoris biomeetriliste isikuandmete kasutuse regulatsioon. Suurbritannias on aga pikk ajalugu avalikus sektoris biomeetriliste andmebaasidega. Suurbritannias on ametis ka eraldi biomeetria järelevalve organ, kelle ülesandeks on jälgida biomeetriliste isikuandmete töötlemist avalikus sektoris. Teistes viidatud riikides on andmekaitse järelevalveasutused teinud otsuseid või avaldanud arvamusi vaid üksikutel konkreetsetel biomeetriliste isikuandmete töötlemise teemadel. Kuivõrd liikmesriikide andmekaitse järelevalveasutuste seisukohad näitavad ainult ühe riigi hoiakut teatud teema suhtes, siis ei ole neil suurt õiguslikku kaalu Eesti kohtute või Andmekaitse Inspektsiooni jaoks. Sellegipoolest peegeldavad nad teatud biomeetriliste isikuandmete töötlemise standardit olukorras, kus puuduvad Euroopa-ülesed biomeetriliste isikuandmete töötlemise juhised. Vastutav töötleja peab ka arvestama erinevate riikide praktikaga, kui soovib isikuandmeid töödelda rahvusvaheliselt. Kasutatud on ka erinevaid nii erasektori kui avaliku sektori poolt koostatud analüüse isikuandmete töötlemiseks uue Määruse järgi.

Märksõnad: andmekaitse, isikuandmed, privaatsus, biomeetriline tuvastamine.

[21] S. Velbri. Isikuandmete kaitse üldmäärusest tulenev nõusoleku vajadus ja selle tingimused isikuandmete töötlemisel äriühingute poolt. Tartu Ülikool. Magistritöö. Tallinn 2018.
[22] M.-L. Piiskop. Andmesubjekti isikuandmete töötlemine nõusoleku alusel. Tartu Ülikool. Magistritöö. Tallinn 2018.
[23] J. Antonova. Isikuandmete kaitse kohtueelses kriminaalmenetluses Eestis. Tartu Ülikool. Magistritöö. Tartu 2015.

1. Biomeetrilised andmed Määruses

Andmekaitse reformi paketi raames lisati biomeetrilised isikuandmed *expressis verbis* eriliigiliste isikuandmete nimekirja nii Määruses kui ka politseikoostöö ja õigusalase koostöö Direktiivis.[24] Varasemalt oli õiguskirjanduses ja ka Artikkel 29 Töörühma poolt avaldatud vaid arvamust, et kuivõrd biomeetrilised andmed võimaldavad ligipääsu eriliigilistele isikuandmetele, siis peaksid need olema reguleeritud nagu eriliigilised isikuandmed.[25] Eriliigiliste isikuandmete nimekirja kandmine tõi biomeetriliste isikuandmete töötlemisele juurde kitsamad õiguslikud alused Määruse artiklist 9 lg 2. Mõistmaks, mida on mõeldud eriliigiliste biomeetriliste isikuandmetena Määruse artiklis 9 lg 1, tuleb vaadata artiklis 4 p 14 antud biomeetriliste andmete definitsiooni, mis on järgnev: „konkreetse tehnilise töötlemise abil saadavad isikuandmed isiku füüsiliste, füsioloogiliste ja käitumuslike omaduste kohta, mis võimaldavad kõnealust füüsilist isikut kordumatult tuvastada või kinnitavad selle füüsilise isiku tuvastamist, näiteks näokujutis ja sõrmejälgede andmed.“[26] Praeguse tehnoloogia arenguga on võimalik lugematutel viisidel inimeste käitumist jälgida ja analüüsida, näiteks kas või *online* keskkonnas analüütika tööriistadega inimese internetis käitumist uurides on võimalik tuvastada konkreetseid mustreid ja seega ka füüsilist isikut ennast tuvastada.[27] Internetis kasutajate käitumist analüüsivaid tööriistu kasutavad aga enamus veebilehtede operaatoreid, aga samal ajal ei saa öelda, et nad kõik töötleks seetõttu eriliigilisi isikuandmeid, mis on võrdsed tervise, etnilise päritolu või seksuaalse orientatsiooni andmete töötlemisega. Seetõttu tuleb järgnevalt vaadata lähemalt nii Määruse artikkel 4 p 14 definitsiooni elemente kui ka artiklit 9 lg 1. Nimelt ei ole biomeetrilised isikuandmed veel eriliigilised isikuandmed puhtalt artikkel 4 alla sobitudes, vaid artikkel 9 annab juurde ühe lisatingimuse: „Keelatud on töödelda /---/ füüsilise isiku kordumatuks tuvastamiseks kasutatavaid biomeetrilisi andmeid /---/.“[28] „Kordumatu tuvastamise“ kriteeriumit Määrus ei selgita ja seetõttu tuleb käesolevas magistritöö esimeses osas ka vastata küsimusele, millal on biomeetrilised andmed tavalised

[24] Politsei ja õigusalase koostöö direktiiv art 3 p 14.
[25] E. J. Kindt. Privacy and Data protection Issues of Biometric Applications. A Comparative Legal Analysis. Leuven: Springer 2013, lk 160. Edaspidi Kindt 2013; Artikkel 29 Andmekaitse Töörühm. Working Document on biometrics. 12168/02/NE. WP80. 01.08.2003, lk 4. Kättesaadav arvutivõrgus: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp80_en.pdf. Edaspidi Artikkel 29 Töörühm. Working Document on biometrics.
[26] Määrus art 4 p 14.
[27] Käitumuslikku biomeetriat kasutab näiteks *The Royal Bank of Scotland* pettuste avastamiseks. Vt S. Cowley. Banks and Retailers Are Tracking How You Type, Swipe and Tap. – The New York Times 13.08.2018. Kättesaadav arvutivõrgus: https://www.nytimes.com/2018/08/13/business/behavioral-biometrics-banks-security.html.
[28] Määrus art 9 lg 1.

isikuandmed ja millal eriliigilised. Sobiva õigusliku aluse valiku eest vastutab vastutav töötleja, mistõttu on väga oluline igale inimese füüsiliste või käitumuslike tunnustega kokkupuutuvale vastutavale töötlejale teada, millisest Määruse artiklist õigusliku aluse valikul lähtuda.

Väljaspool Määruse konteksti on inimese bioloogilised, füsioloogilised ja käitumuslikud andmed mõistetud koondnimega biomeetrilised andmed tegemata vahet eriliigilistel ja nn tavalistel isikuandmetel. Seega selguse huvides nimetatakse käesolevas magistritöös läbivalt kõiki selliseid andmeid biomeetrilisteks tunnusteks ja Määruse artikkel 4 p 14 definitsioonis kirjeldatud isikuandmetele viidatakse kui biomeetrilistele andmetele. Magistritöös tähendavad biomeetrilised tunnused otsest inimese füüsilist, füsioloogilist või käitumuslikku tunnust, nagu nägu või silmaiiris ilma edasise töötlemiseta ehk nö toored andmed (inglise k *raw data*).

Magistritöö esimese osa eesmärk on leida, mida mõistetakse biomeetriliste andmetena Määruses ja millal muutuvad nn tavalised biomeetrilised andmed eriliigilisteks. Esiteks antakse kontekstiks ülevaade biomeetriliste tunnuste üldlevinud omadustest. Seejärel võrdleb autor iga definitsiooni elementi senise Euroopa Kohtu ja Euroopa Inimõiguste Kohtu praktikaga või varasemate Artikkel 29 Töörühma arvamustega ja praktikas kasutatavate isikuandmete töötlemisviisidega. Uuritakse kuidas erinevad biomeetrilised andmed teistest isikuandmetest ja kuidas see definitsioon on kooskõlas üldiste biomeetriliste andmete tunnustega. Seejärel võrdleb autor Määruse biomeetriliste andmete definitsiooni artiklis 9 lg 1 toodud eriliigiliste isikuandmete klassifikatsiooniga ja töös vastatakse küsimusele, kuidas erinevad eriliigilised biomeetrilised andmed nn tavalistest biomeetrilistest andmetest. Eelnevast tulenevalt kaardistab autor Määruse probleemkohad biomeetriliste andmete töötlemisele õigusliku aluse valikul, mida magistritöö järgnevates osades uurida.

1.1. Biomeetriliste andmete tunnused

Biomeetriliste andmete tunnusteks on universaalsus, püsivus ja unikaalsus. Mõned neist andmetest on epigeneetilised[29] ja seega ühesugused identsete kaksikute puhul. Need tunnused ongi biomeetriliste tehnoloogiate riskide põhjuseks, mistõttu on biomeetrilised andmed leidnud koha eriliigiliste isikuandmete nimekirjas.

Universaalsus tähendab, et printsiibis on biomeetrilised andmed igal inimesel. See eeldus välistab spetsiifiliste tunnuste kasutamise, nagu sünnimärgid ja armid, mida võidakse kasutada

[29] Epigeneetiline tähendab, et andmed on saadud ilma geneetilise täpsustuseta ehk ilma DNA-ga sidumiseta.

isikute tuvastamiseks näiteks õnnetuste stsenaariumis. Kuigi eeldatakse, et andmed on universaalsed, ei tähenda see, et need peaksid olema igal inimesel. Inimesed võivad ka olla kaotanud teatud biomeetrilise tunnuse õnnetuse või muude asjaolude tõttu. Ka etniline päritolu või nahavärv võivad olla määravad biomeetrilise süsteemi kasutuses. Arvestada tuleb ühe tunnuse liigi mitmekesisusega, mistõttu süsteem tuleb üles ehitada mitte diskrimineerivalt. Näiteks on näotuvastustehnoloogia kasutamisel raskusi inimestel, kes on õnnetustes viga saanud või programm ei suuda arvestada nahavärvi erisustega. Suurbritannias viidi näiteks läbi passides biomeetrilise tuvastamise uuring, millest selgus, et süsteem andis rohkem veateateid teatud etnilise päritoluga inimeste puhul.[30]

Biomeetrilised andmed peavad isiku tuvastamiseks olema püsivad ehk ei muutu ajas. Sellised andmed on näiteks silmaiirised ja sõrmejäljed. Eeldatakse, et andmesubjekt ei saa neid tunnuseid muuta. Mõned tunnused on siiski rohkem muutuvad kui teised. Näiteks inimese nägu võib olla abiks tuvastamisel, kuid aja möödudes võib tuvastamisel tekkida raskusi tahtlike välimuse muudatustega, nagu prillid, habe või iluoperatsioonid. Samuti mittetahtlikud muutused nagu vigastus, vananemine, kaalus juurde- või allavõtmine. Lastel võib muutuda ka käe või sõrmede geomeetria.[31] Seega kasutatakse püsivuse asemel ka terminit stabiilsus. Stabiilsuse kriteerium määrab vältimatult ära kasutatava tehnoloogia turvalisuse ja usaldusväärsuse taseme. Biomeetriliste andmete muutuvus väljendub tehnilise süsteemi vigades ja seega tuleks sellega arvestada biomeetriliste tehnoloogiate valikus vastavaks ülesandeks.

Biomeetrilised andmed peavad biomeetrilistes süsteemides kasutamiseks olema ka unikaalsed või vähemalt eristatavad. See on biomeetriliste tehnoloogiate tuum, et tehnoloogiad peavad võimaldama tuvastada või autentida füüsilisi isikuid. Sõrmejälge loetakse üldiselt unikaalseks. Silmaiirist loetakse epigeneetiliseks tunnuseks ja on samuti unikaalne. Isegi käsitsi kirjutatud allkirja loetakse unikaalseks.[32] Kuigi unikaalsus on oluline, ei tuvasta tehnoloogia biomeetrilise jäljendi unikaalsust, vaid tõenäosust, et kaks esitatud näidist tulenevad samast isikust. Sarnast lähenemist kasutatakse kriminalistikas, kus keskne küsimus on kahtlustatava või ohvri

[30] E. J. Kindt. The Processing of Biometric Data. A Comparative Legal Analysis with a focus on the Proportionality Principle and recommendations for a legal framework. Doctoral thesis. Leuven: Katholieke Universiteit 2012, lk 280. Edaspidi Kindt 2012.
[31] Kindt 2013, lk 33.
[32] Artikkel 29 Töörühm. Opinion 3/2012 on developments in biometric technologies. 00720/12/EN. WP193. 27.04.2012, lk 4. Kättsaadav arvutivõrgus: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf. Edaspidi Artikkel 29 Töörühm Opinion 3/2012 on developments in biometric technologies.

tuvastamine ning võrreldakse andmenäidiseid kuriteopaigalt ja kahtlustatavalt. Need näidised on küll unikaalsed, aga mitte identsed. Neid saab kasutada tõendamiseks näitamaks, et mõlemad andmenäidised tulenevad samast allikast. Kõik kasutatavad andmed ei ole aga unikaalsed, vaid on lihtsalt eristatavad. Näiteks käe geomeetriat ei loeta unikaalseks tunnuseks, vaid pigem grupist eristatavaks tunnuseks.[33] Eristatavust vaadatakse ka siis kui biomeetrilist tehnoloogiat kasutatakse käitumuslike tunnuste analüüsiks.[34]

Eristatakse bioloogilisi ja käitumise põhiseid andmeid või tunnuseid. Konkreetse biomeetrilise tehnoloogia valikut ja süsteemi arhitektuuri mõjutab selleks kasutatavate biomeetriliste tunnuste valik ja nende tunnuste kasutamise aktsepteerimine andmesubjektide poolt. Seega peab vastutav töötleja hindama enda poolt kogutavaid isikuandmeid eeltoodud kriteeriumitest lähtuvalt. Määruse definitsioon biomeetrilistest andmetest on küllalt lai, millega justkui teadvustatakse, et biomeetrilised tehnoloogiad on alles uued ja jätkuvalt arenevad. Seega on autori hinnangul Määruse definitsioon sobiv võrreldes üldiste biomeetriliste andmete tunnustega ja hõlmab endas isikuandmete tüüpe, mis võivad tekkida tulevikus tehnoloogia arenedes.

1.2.Biomeetriliste andmete mõiste Määruses

Biomeetriliste andmete kvalifikatsioonist Määruses parema ülevaate saamiseks tuleb esiteks analüüsida artikkel 4 p 14 definitsiooni elemente. Järgnevalt analüüsitakse nelja elementi:

a. isikuandmed;
b. konkreetse tehnilise töötlemise abil saadavad isikuandmed;
c. füüsilise isiku füüsilised, füsioloogilised ja käitumuslikud omadused;
d. isikuandmed, mis võimaldavad kõnealust füüsilist isikut kordumatult tuvastada või kinnitavad selle füüsilise isiku tuvastamist.

Biomeetrilised andmed on definitsiooni kohaselt esiteks tavalised isikuandmed. Seega enne, kui biomeetrilised andmed kvalifitseeruvad eriliigiliste isikuandmete alla, peavad nad vastama üldisele isikuandmete mõistele. Isikuandmed Määruse järgi on „igasugune teave tuvastatud või tuvastatava füüsilise isiku („andmesubjekti“) kohta; tuvastatav füüsiline isik on isik, keda saab otseselt või kaudselt tuvastada, eelkõige sellise identifitseerimistunnuse põhjal nagu nimi,

[33] Kindt 2013, lk 28.
[34] Krausova lk 168.

isikukood, asukohateave, võrguidentifikaator või selle füüsilise isiku ühe või mitme füüsilise, füsioloogilise, geneetilise, vaimse, majandusliku, kultuurilise või sotsiaalse tunnuse põhjal."[35] Tuvastatavust ei ole Määruses ega Direktiivis defineeritud. Küll aga on identifitseeritavuse piir madal. Isik ei pea olema identifitseeritud, vaid ainult identifitseeritav. Artikkel 29 Töörühm on oma arvamuses isikuandmete kontseptsiooni kohta tõlgendanud mõistet „identifitseeritud" kui väljavalitud või eristatud inimeste grupist.[36] Seega isikuandmete kaitse kontekstis ei vaja identifitseerimine kellegi identiteedi kindlaks tegemist. Piisab „identifitseeritavusest," mis tähendab, et isiku identiteet ei ole veel teada, kuid teda on võimalik identifitseerida, kui siduda isikuga muud informatsiooni. Test sisaldab endas palju faktoreid, mis on loetletud Määruse preambuli punktis 26, mille järgi isiku tuvastatavuse kindlaks tegemisel tuleb arvestada kõiki vahendeid, mida mõistliku tõenäosusega võib kasutada isiku identiteedi kindlakstegemiseks. See sisaldab nii andmete töötlemise ajal kättesaadavat tehnoloogiat kui ka tehnoloogilisi arenguid.[37] Tehnoloogia arengu arvestamine on eriti oluline biomeetria kontekstis, kuivõrd biomeetria on suhteliselt uus, kuid kiirelt kasvav valdkond ja biomeetrilisi andmeid artikkel 4 definitsiooni kohaselt töödeldakse läbi tehniliste vahendite. Biomeetrilised andmed oma olemuselt on igal inimesel ja need on elu jooksul suhteliselt püsivad. Samal ajal jätavad sellised andmed jälgi, nagu sõrmejäljed klaasil, või on kergelt kättesaadavad fotode kujul internetis, mistõttu isiku tuvastatavuse tõenäosus pea igas biomeetrilises tehnoloogias on äärmiselt kõrge.

Teine biomeetriliste andmete definitsiooni element „konkreetse tehnilise töötlemise abil saadavad isikuandmed" on üks ebaselgemaid definitsiooni osasid. Määrus ei täpsusta, mida mõeldakse biomeetriliste andmete definitsioonis konkreetse tehnilise töötlemise all kui ainult, et selle eesmärk on isik tuvastada. Selgusetu on ka millisel hetkel muutub lihtsalt tehniline töötlemine konkreetseks tehniliseks töötlemiseks, näiteks analoog fotod *versus* digitaalfotod. Määruse preambuli punkt 51 ütleb, et fotode töötlemine on hõlmatud biomeetriliste andmete määratlusega, kui neid töödeldakse konkreetsete tehniliste vahenditega. Siin tekib ka küsimus, kas see hõlmab fotosid kõikidest biomeetrilistest tunnustest. Huvitav on ka fakt, et Määruse ja politseikoostöö ja õigusalase koostöö Direktiivi definitsioonid biomeetrilistest andmetest on samad, küll aga puudub politseikoostöö ja õigusalase koostöö Direktiivist Määruse preambuli punktiga 51 sarnane täpsustus. Konkreetse tehnilise töötlemise kriteeriumi vajalikkust

[35] Määrus art 4 p 1.
[36] Artikkel 29 Töörühm. Opinion 4/2007 on the concept of personal data. 01248/07/NE. WP 136. 20.06.2007, lk 12. Kättesaadav arvutivõrgus: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf. Edaspidi Artikkel 29 Töörühm. Opinion 4/2007 on the concept of personal data.
[37] Määrus preambul, p 26.

Määruses nähti põhjusel, et kui lähtuda ainult biomeetriliste tunnuste olemusest, siis paljudel juhtudel on tegemist nn tavalise isikuandmete töötlemisega, mida ei peaks piirama. Näitena võib tuua eraisiku poolt fotode või videode avalikult üles panekut või ajalehe väljaannetes fotode kasutamist. Samuti ei ole biomeetrilised andmed sellised inimese füüsilised või käitumuslikud tunnused, mida ei olegi tehniliselt töödeldud, näiteks vereproovid, ehk nö toored andmed. Seetõttu otsustasid Määruse autorid, et ülimuslik on isikuandmete kasutamise viis, mitte isikuandmed ise.[38]

Mõistmaks artiklis 4 p 14 mõeldut, tuleb lähemalt vaadata biomeetrilise töötlemise eripärasid. Biomeetriliste andmete töötlemisel tuvastustehnoloogiates on väga spetsiifilised etapid ja seega on mõned autorid arvamusel, et konkreetne tehniline töötlemine tähendab, et arvestada tuleb erinevaid andmete töötlemise etappe.[39] Nendeks etappideks on andmete kogumise faas, näiteks inimene asetab sõrme sensorile. Teiseks etapiks on tuvastamiseks vajaliku info eraldamine esitatud andmetest ja biomeetrilise jäljendi loomine. Kolmanda etapina on biomeetrilise tunnuse, nagu sõrmeots, võrdlemine süsteemis talletatud matemaatilise jäljendiga.[40] Need etapid vastavad mitmele Määruse isikuandmete töötlemise definitsioonis toodud tegevusele nagu kogumine, kohandamine, säilitamine, päringute tegemine ja kasutamine.[41] Arvamusega konkreetsetest töötlemise etappidest on raske nõustuda, sest füsioloogilisi või käitumuslikke andmeid töötlevad tehnoloogiad võivad lihtsalt koostoimes teiste andmetüüpidega juba tuvastada isiku ilma süsteemi talletatud jäljendi võrdlemiseta.[42] Konkreetsete etappide kriteerium eeldaks, et Määrus mõistab biomeetriliste tehnoloogiatena vaid konkreetselt identiteedi tuvastamise eesmärgil biomeetriliste andmete töötlemist, nagu näokujutisega mobiiltelefoni avamine või sõrmejäljega rahaülekande tegemine. Artikkel 4 definitsioon ütleb aga, et tehnoloogia peab vaid „võimaldama kordumatut tuvastamist." E. J. Kindt on arvamusel, et nii Määrus kui politseikoostöö ja õigusalase koostöö Direktiiv mõistavad konkreetse tehnilise töötlemise all biomeetriliste tunnuste kasutamist biomeetrilisel võrdlemisel. See tähendab, et tunnuste kujutised valmistatakse ette biomeetriliseks võrdluseks, näiteks piltide täiustamine neist asjakohase info eraldamiseks või biomeetriliste jäljendite

[38] *Ibid.*
[39] C. Jasserand on arvamusel, et konkreetne tehniline töötlemine tähendab biomeetriliste andmete töötlemise etappide läbimist. Vt Jasserand lk 303.
[40] Artikkel 29 Töörühm. Opinion 3/2012 on developments in biometric technologies, lk 5.
[41] Määrus art 4 p 2.
[42] Tegemist on nn sensorite segunemise fenomeniga (inglise k *sensor fusion*), kus erinevatest sensoritest saadud või tuletatud andmed kombineeritakse selliselt, et tulemuseks on täpsem informatsioon kui siis kui neist sensoritest koguda andmeid isoleeritult.

töötlemine. Selliselt töödeldud isikuandmed muutuvad E. J. Kindti arvates biomeetrilisteks andmeteks.[43] Samas esimene etapp, millest biomeetriline võrdlus saaks alata, on esialgne biomeetriliste tunnuste andmebaas. Kuid jääb mulje, et Määrus ega politseikoostöö ja õigusalase koostöö Direktiiv ei loe sellist andmebaasi biomeetrilisteks andmeteks. Samuti tundub kummaline biomeetriliste andmete definitsioonist välja jätta olukord, kus vastutav töötleja loob andmebaasi biomeetrilistest tunnustest, kuid ei kasuta seda kellegi tuvastamiseks. Sellisel juhul jääksid biomeetriliste andmete töötlemise kaitsealast välja näiteks fotode ja sõrmejälgede andmebaasid. Sellised andmebaasid võimaldavad aga teiste andmetüüpidega kombineeritult mõistliku vaevaga isikut tuvastada.

Eelnevat arvesse võttes ei ole käeoleva töö autor nõus E. J. Kindti arvamusega, et konkreetne tehniline töötlemine tähendab biomeeriliste tunnuste ettevalmistamist biomeetriliseks võrdluseks, ehk jäljendi loomist. Selline lähenemine ignoreerib juba eelnevalt väljatoodud andmebaaside probleemi. Arvesse tuleb võtta biomeetriliste tehnoloogiate omadusi ja kiiret arengut, mistõttu ei saa kasutusviisi nii kitsalt piiritleda. Google tegevjuht E. Schmidt teadvustas avalikult juba 2010. aastal piltide kogumise ja tehnoloogia kaugele ulatuvaid tagajärgi, mistõttu Google loobus oma liidetud inimkonna (inglise k. *augmented humanity)* plaanis näotuvastustehnoloogiatest.[44] EIKi praktikas on rõhutatud, et kõigest biomeetriliste andmebaaside loomine kujutab juba endast olulist ohtu eraelu puutumatusele. Kohus leidis *S. and Marper* lahendis, et arvestades kiiret tehnoloogia arengut võivad tulevikus eraelu huvid ühendatuna geneetilise informatsiooniga viia eraelu mõjutamiseni viisil, mida ei saa praegu ette näha piisava täpsusega, mistõttu sõrmejälgede, DNA profiilide ja rakunäidiste hoidmine kujutab endast eraelu puutumatuse rikkumist.[45] Euroopa Nõukogu on samuti oma kohtupraktika ülevaates rõhutanud, et tulevikus kujutavad privaatsusele rohkem probleeme andmebaasid nagu Viisainfosüsteem, Schengeni infosüsteem ja EURODAC, mis kõik sisaldavad biomeetrilisi isikuandmeid.[46] Biomeetrilised andmed on väga erinevad teistest isikuandmetest põhjusel, et nende klassifikatsioon sõltub puhtalt töötlemise viisist ja kasutatavatest tehnilistest vahenditest. Eelnevast tulenevalt on käesoleva töö autor seisukohal, et Määruse kriteeriumiga konkreetsest tehnilisest töötlemisest on eelkõige peetud silmas

[43] Kindt 2018.
[44] L. Gannes, Eric Schmidt: Welcome to "Age of Augmented Humanity." 07.09.2010. http://gigaom.com/2010/09/07/eric-schmidt-welcome-to-the-age-of-augmented-humanity/.
[45] EIKo. 04.12.2008, 30562/04 ja 30566/04, *S and Marper v United Kingdom*, p 69, 86. Edaspidi *S. and Marper.*
[46] Research Division. Internet: case-law of the European Court of Human Rights. *Sine loco*, European Court of Human Rights 2015, lk 13. Kättesaadav arvutivõrgus: https://www.echr.coe.int/Documents/Research_report_internet_ENG.pdf.

välistada biomeetriliste andmete definitsioonist tavaline ja väikesemahulise töötlemine. Tavaline töötlemine autori hinnangul tähendab näiteks ajalehe väljaannetes inimeste fotode avaldamist või olukorda, kus tööandja kogub uue töötaja otsingul kandidaatide CV-d ühte kausta arvutis ja CV-d sisaldavad enamasti ka kandidaadi pilti. Teisisõnu biomeetriliste tunnuste töötlemine on kaasnev tagajärg ja ilma edasise tehnilise töötlemiseta üksinda kedagi ei tuvastaks.

Teiseks tuleb uurida tehnilise töötlemise mõju biomeetrilistele tunnustele võrreldes nn tavalise töötlemisega. Tehnilise töötlemise nõue jaotab pealtnäha samad isikuandmete tüübid eri tüüpi isikuandmeteks. Näiteks kui panga „tunne oma klienti“ (inglise k. *Know Your Customer*) protsessis klienditugi tuvastab klientide identiteete fotosid vaadeldes ja seejuures kasutatakse ainult inimressurssi, siis ei saaks Määruse järgi tegemist olla biomeetriliste andmete töötlemisega. Kui samu fotosid analüüsib aga seade, mis suudab kiirelt eristada ühe isiku teisest, siis sellised fotod kvalifitseeruvad Määruse järgi biomeetrilisteks andmeteks. Samas teised eriliigilised isikuandmed, nagu geneetiliste andmete või terviseandmete definitsioonid artiklis 4 ei sisalda konkreetse tehnilise töötlemise nõuet.[47] E. J. Kindt on arvamusel, et biomeetriline tehnoloogia oluliselt muudab isikute vahel võimusuhet. Inimesed enamjaolt kontrollivad automatiseerimata identifitseerimist andes ise identifitseerivat infot ja teades, kellele see info kättesaadav on. Automatiseeritud biomeetriline tuvastustehnoloogia loob aga olukorra, kus igaühel on võimalus väga palju infot isiku kohta hankida pelgalt näo või muu nähtava biomeetrilise tunnuse järgi ilma, et andmesubjekti ennast sellest informeeritaks.[48] Autor on nõus eelneva arvamusega biomeetrilise tehnoloogia erinevusest tavalistest identifitseerimisviisidest. Samuti võib väita, et biomeetriliste tunnuste kasutamise riskid tulenevad sellest, et enamasti ei saa inimene neid tunnuseid enda juures kunagi muuta, aga samal ajal kasutab ta sama muutumatut füsioloogilist tunnust erinevates rakendustes. Näiteks võib inimene ühe päeva jooksul kasutada sõrmejälge mobiiltelefoni avamiseks, rahaülekandeks ja kontoriuksest sisenemiseks. Seega tuleneb tehnilise töötlemise nõue biomeetriliste andmete puhul asjaolust, et töötlemise riskid on kergemini avalduvad tehnilisel töötlemisel. Tuvastustehnoloogiaga kaamerad või internetis kasutajate käitumisest mustreid loovad analüütika tööriistad viivad riskideni nagu jälitamine, tuvastamine poliitilistel või religioossetel üritustel, diskrimineerimine, stigmatiseerimine või kahtlusalusena kohtlemine ja üldine

[47] Määrus art 4 pp 13, 15.
[48] Kindt 2018.

jälitusühiskonna teke.[49] Andmesubjektile tekkiv kahju biomeetrilistest tehnoloogiatest on paljudel juhtudel suurem, kui muude tehnoloogiate puhul. Arvestades biomeetriliste andmete püsivust ja universaalsust võib isikuandmete leke kiirelt viia näiteks identiteedivarguseni ja sellisel juhul on keeruline midagi ette võtta, sest näiteks oma sõrmejälge inimene muuta ei saa sama lihtsalt nagu PIN-i. Seega eelnevast tulenevalt tuleb autori hinnangul lugeda Määruse biomeetriliste andmete konkreetse tehnilise töötlemise kriteerium täidetuks, kui töödeldakse inimese füüsilisi ja käitumuslikke tunnuseid tehniliste vahenditega viisil, kus luuakse biomeetrilistest tunnustest andmekogusid, mis mõistliku vaevaga võimaldavad isikut grupist eraldada ja millel on oht tekitada andmesubjektile olulist kahju.[50]

Kolmas definitsiooni element „isikuandmed füüsilise isiku füüsiliste, füsioloogiliste ja käitumuslike omaduste kohta“ on lai valik mõõdetavatest inimese tunnustest. See katab nii füüsilised ja füsioloogilised tunnused, nagu sõrmejälg ja silmaiiris, kui ka käitumuslikud tunnused, nagu hääl, allkiri, rüht või ka tegevuste sooritamise strateegia. Üks olulisemaid käitumuslike biomeetriliste andmete tunnuseid on aja dimensioon ehk mõõdetaval käitumisel on algus, kestvus ja lõpp.[51] Vahe füsioloogiliste ja füüsiliste omaduste vahel on siiski ebaselge. Õiguskirjanduses nimetatakse biomeetriliste andmetena vaid kahte andmete tüüpi: füüsilised või käitumuslikud andmed.[52] Artikkel 29 Töörühm on nimetanud biomeetrilisteks isikuandmeteks nii bioloogilisi, käitumuslikke, füsioloogilisi kui ka psühholoogilisi tunnuseid, kuid jaotab nad ikkagi laias laastus kaheks grupiks: füüsilised või füsioloogilised ja käitumuslikud tunnused.[53] Seega käesolevas magistritöös kasutatakse inimese füüsilisi ja füsioloogilisi tunnuseid sünonüümidena.

[49] M. Hildebrandt, S. Gutwirth (koost). Profiling the European Citizen. Cross-Disciplinary Perspectives. Dordrecht: Springer 2008, lk 144. Edaspidi M. Hildebrandt, S. Gutwirth; Artikkel 29 Andmekaitse Töörühm. Opinion 8/2014 on the on Recent Developments on the Internet of Things. 14/NE. WP223. 16.09.2014, lk 8. Kättesaadav arvutivõrgust: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf. Edaspidi Artikkel 29 Töörühm. Opinion 8/2014 on the on Recent Developments on the Internet of Things; Kindt 2018. .

[50] Määruse preambul p 75 loetleb kahjudena: “/---/ füüsiline, materiaalne või mittemateriaalne kahju, eelkõige juhtudel, kui töötlemine võib põhjustada diskrimineerimist, identiteedivargust või -pettust, rahalist kahju, maine kahjustamist, ametisaladusega kaitstud isikuandmete konfidentsiaalsuse kadu, pseudonümiseerimise loata tühistamist või mõnda muud tõsist majanduslikku või sotsiaalset kahju /---/.“

[51] L. Wang, X. Geng (koost). Behavioral Biometrics for Human Identification: Intelligent Applications. New York: Medical Information Science Reference 2009, lk 2. Edaspidi L. Wang, X. Geng.

[52] Jasserand, lk 304; L. Wang, X. Geng, lk xviii.

[53] Artikkel 29 Töörühm. Opinion 3/2012 on developments in biometric technologies, lk 4.

1.3.Kordumatu tuvastamise kriteerium

Määruse artikkel 4 definitsiooni osa „isikuandmed, mis võimaldavad kõnealust füüsilist isikut kordumatult tuvastada või kinnitavad selle füüsilise isiku tuvastamist“ on võtmekriteerium biomeetriliste andmete eriliigilisteks isikuandmeteks kvalifitseerimisel. Kordumatu tuvastamise kriteerium esineb nii artiklis 4 kui ka 9, mistõttu analüüsitakse selle tähendust artikkel 4 definitsioonist eraldi. Määruse artikkel 9 sätestab: „Keelatud on töödelda /---/ füüsilise isiku kordumatuks tuvastamiseks kasutatavaid biomeetrilisi andmeid /---/.“[54] Seega artikkel 4 annab eelduse, et biomeetrilisi andmeid peab olema võimalik selliselt kasutada.

Esiteks kirjeldab füüsilise isiku tuvastamine biomeetriliste tunnuste kasutamise eesmärki ja teiseks seab see biomeetrilistele andmetele kohalduva identifitseerimise piirmäära. Piir tõmmatakse biomeetrilise identifitseerimise ja üldise isikuandmete abil identifitseerimise vahele. Identiteet biomeetrilises kontekstis ei vaja juriidilise või füüsilise identiteedi kindlaks tegemist, vaid kindlaks tehakse, et biomeetrilise tunnuse näidis ja varasemalt salvestatud matemaatiline biomeetriline jäljend tulenevad samast isikust. Identiteet on kindlaks tehtud, kui biomeetriline tunnus klapib biomeetrilise jäljendiga.

Termin „kordumatult tuvastada“ tõstatab mitmeid küsimusi. On teadmata, kas see seab piirmäära identifitseerimisele biomeetrilise identifitseerimise kontekstis või viitab see biomeetriliste andmete funktsioonile ehk kedagi unikaalselt eristada. Määruse preambuli punkt 51 lisab, et fotode töötlemine on hõlmatud biomeetriliste andmete määratlusega, kui töötlemine võimaldab füüsilist isikut kordumatult tuvastada või autentida. Seega võib „kordumatu tuvastamine“ tähendada, et tehniliste vahenditega töötlemine peab olema nii täpne, et võimaldab kordumatut identifitseerimist. Näiteks sotsiaalmeedia pildialbumis inimeste nägudest piltide üles panek ei ole veel biomeetriliste andmete töötlemine. Küll aga on biomeetriliste andmete töötlemine näost või silmaiirisest matemaatilise jäljendi tegemine, mis võimaldab igal üksikul juhul sama inimest tehniliste vahenditega kiiresti tuvastada.

Nagu eelnevalt selgitatud, siis identifitseerimise piir Määruses on madal, sest isik peab olema kõigest identifitseeritav. Aga see piir on palju kõrgemal biomeetriliste andmete jaoks. Terminit „kordumatu tuvastamine“ kasutatakse Määruses ainult kolmes kohas: Artiklites 4 p 14 ja 9 lg 1 ja preambuli punktis 51. Semantiliselt võib „kordumatu tuvastamine“ viidata kellegi tuvastamisele kui üks ja ainus. Samas termin „kordumatut“ võib viidata ka biomeetriliste

[54] Määrus art 9 lg 1.

andmete omadusele seostada isikut tema kehaga. Kumbki neist ei oleks aga päris õige, sest teaduslikult ei saa öelda, et biomeetrilised andmed on unikaalsed igale inimesele ja võimaldavad isiku kordumatut tuvastamist. Mitte kunagi ei ole teaduslikult tõestatud, et kahel inimesel ei saa olla sama sõrmejälge. Biomeetriline tuvastamine põhineb sarnasuste tõenäosusel. On teada, et biomeetrilise võrdlemise käigus saadavad tulemused võivad olla vigased või viia vale identifitseerimiseni.[55] Seega ei saa biomeetrilised andmed olla sama kordumatud kui unikaalne isikukood. Euroopa andmekaitseinspektor on samuti oma arvamuses soovitanud mitte kasutada biomeetrilisi andmeid kordumatute identifitseerijatena nende tehnoloogiate tõenäosusliku olemuse tõttu, sest see viib andmete kvaliteedi põhimõtte rikkumiseni.[56] Kuigi biomeetriliste andmete sobilikkus turvaliste identifitseerijatena on vaieldav, kasutatakse neid just turvalise tuvastamise ja autentimise eesmärgil väga laialdaselt nii avalikus kui erasektoris. Artikkel 29 Töögrupi arvamuse järgi on aga kordumatu tuvastamise mõiste suhteline sõltudes erinevatest faktoritest, sealhulgas andmebaasi suurusest ja kasutatavate biomeetriliste andmete tüübist.[57] Eelnevast tulenevalt võib autori hinnangul väita, et biomeetriliselt süsteemilt eeldatakse isiku eristamist grupist tema biomeetriliste tunnuste põhjal ja seda eristusvõimet hinnatakse kontekstis.

Teisest küljest nagu eelnevalt välja toodud, ei suuda ükski biomeetriline süsteem garanteerida alati kordumatut tuvastamist ja seega tekib küsimus milline tõenäosuse määr oleks piisav, et lugeda kasutatav tehnoloogia Määruse mõistes biomeetriliste andmete töötlemiseks. Sellisel juhul tuleb ka mõelda, kas usaldusväärsust hinnatakse individuaalselt igal konkreetsel juhul eraldi või peaks eelistama mõnda kindlat veamäära. Määruse preambul ütleb, et füüsiliste isikute kaitse peaks olema tehnoloogiliselt neutraalne ega tohiks sõltuda kasutatud meetoditest.[58] Seega ei tohiks erinevaid biomeetrilisi süsteeme diskrimineerida sõltuvalt nende sooritusest. A. Krausova näiteks on arvamusel, et tehnoloogia veamäära asemel peaks arvestama konkreetse tehnoloogia mõjuga. Kordumatu tuvastamise nõude tõttu ei peaks välistama biomeetriliste andmete definitsioonist vähem usaldusväärseid süsteeme, nagu inimese käitumise analüüsil põhinevad biomeetrilised süsteemid.[59] Eelnevast tulenevalt on käesoleva töö autor arvamusel, et biomeetrilisteks andmeteks Määruse mõistes liigituvad

[55] Jasserand, lk 306.
[56] Euroopa andmekaitseinspektor. Comments on the Communication of the Commission on interoperability of European databases. 10.03.2006, lk 4. Kättesaadav arvutivõrgus: https://edps.europa.eu/sites/edp/files/publication/06-03-10_interoperability_en.pdf.
[57] Artikkel 29 Töörühm. Working document on biometrics. lk 2.
[58] Määrus, preambul p 15.
[59] Krausova, lk 165.

andmed, mis võimaldavad piisavalt täpselt ja igakordselt füüsilist isikut tuvastada välistamata ennetavalt ühtegi konkreetset tehnoloogiat. Sealjuures tuleks autori hinnangul arvestada ka, et biomeetrilised tunnused kannavad teatud vahelüli rolli isiku identiteedi ja teiste andmebaaside vahel. Näiteks interneti analüütika tööriista andmebaas anonüümsete kasutajate käitumismustritest veebilehel kombineerituna panga käitumispõhise tuvastussüsteemiga või tudengiorganisatsiooni andmebaas suurest hulgast liikmete fotodest kombineeritult õiguskaitseorganite tuvastussüsteemidega. Teisisõnu hinnata tuleks kui tõenäoline on kasutatava tehnoloogia olemust arvestades, et biomeetriliste andmete põhjal saab isikut tulevikus tuvastada kombineerituna muu informatsiooniga, mis iseseisvalt kedagi automaatselt ei tuvastaks.

Lisaks sõnale „kordumatu“ tekitab biomeetria kontekstis segadust ka sõna „tuvastamine.“ Määrus nimetab artiklites 4 ja 9 vaid „tuvastamist“ kuigi biomeetria valdkonnas on tuvastamisel väga kitsas tähendus. Biomeetrilistel tehnoloogiatel on laias laastus kaks funktsiooni: tuvastamine ja autentimine. Biomeetriliste süsteemide mõistmiseks on oluline neil funktsioonidel vahet teha. Esiteks erineb viis, kuidas sisestatavaid andmeid andmebaasiga võrreldakse. Autentimisel võrdleb süsteem sisestatud biomeetrilisi andmeid ainult ühe biomeetrilise tunnusega andmebaasis, nn üks ühele võrdlemine, mis peaks andma tulemuse, kas tunnus kuulub ühele ja samale inimesele.[60] Autentimise tehnoloogiat kasutatakse näiteks mobiiltelefoni avamiseks või rahaülekandeid tehes.[61] Tuvastamisel aga võrreldakse sisestatud tunnust kõigi andmebaasis olemasolevate biomeetriliste tunnustega, nn üksikult üldisele võrdlemine.[62] Tuvastamist kasutatakse palju avalikus sektoris, näiteks EL-i immigratsioonikontrollis võrreldakse andmebaasis inimeste fotosid ja sõrmejälgi.[63] Tuvastamine kujutab endast isiku privaatsusele palju suuremat ohtu ja võimaldab isiku andmeid süsteemi sisestada ka andmesubjekti teadmata.[64] E. J. Kindt on samuti kritiseerinud Määrust selle poolest, et juriidilised definitsioonid ei peegelda tehnoloogiat praktikas, kuigi tehniliselt korrektse terminoloogia kasutamine on oluline.[65] Määruse preambul nimetab

[60] Artikkel 29 Töörühm. Opinion 3/2012 on developments in biometric technologies. Lk 6.
[61] Pangad, kes kasutavad eri vormides biomeetrilist tuvastamist oma teenustele ligipääsuks on näiteks *Lloyds Banking Group plc, Citi Group Inc., Wells Fargo, Commonwealth Bank of Australia, Royal Bank of Scotland Group plc, Deutsche Bank, Mastercard* jpt.
[62] Artikkel 29 Töörühm. Opinion 3/2012 on developments in biometric technologies. Lk 5.
[63] Nõukogu otsus 2007/533/JSK, 12.06.2007, mis käsitleb teise põlvkonna Schengeni infosüsteemi (SIS II) loomist, toimimist ja kasutamist. – ELT L 205, 7.8.2007, art 20 lg 2 pp. e, f. Kättesaadav arvutivõrgus: https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=uriserv:OJ.L_.2007.205.01.0063.01.EST&toc=OJ:L:2007:205:FULL.
[64] Artikkel 29 Töörühm. Opinion 3/2012 on developments in biometric technologies. Lk 8, 23.
[65] Kindt 2013, lk 42.

biomeetriliste andmete definitsiooni osana nii tuvastamist kui autentimist,[66] kuid artikkel 4 p 14 definitsioon nii selge ei ole. „Võimaldavad füüsilist isikut kordumatult tuvastada või kinnitavad selle füüsilise isiku tuvastamist“ tundub viitavat autentimise ja tuvastamise funktsionaalsuse erinevustele. Seega tõlgendab käesoleva magistritöö autor, et biomeetriliste andmete definitsioon artiklis 4 p 14 hõlmab nii tuvastamist kui autentimist või ei sõltu midagi Määruse rakendamises nende kahe mõiste eristamisest.

1.4. Biomeetrilised andmed eriliigiliste isikuandmetena

Järgnevalt analüüsitakse, kuidas sobivad Määruse artikkel 4 p 14 definitsiooni järgi biomeetrilised andmed eriliigiliste isikuandmete gruppi. Eriliigilised isikuandmed on isikuandmete grupp, mis vajab kõrgemat kaitset tagajärgede tõttu, mida nende väärkasutamine võib endaga kaasa tuua. Need on sellist laadi isikuandmed, mis on oma olemuselt põhiõiguste ja -vabaduste seisukohast eriti tundlikud ja väärivad erilist kaitset, sest nende töötlemise kontekst võib põhiõigusi ja -vabadusi olulisel määral ohustada.[67] Neid tagajärgi loetakse nii rasketeks, et printsiibis on eriliigiliste isikuandmete töötlemine keelatud. Määruse artiklis 9 on toodud kinnine loetelu eriliigilistest isikuandmetest.[68] Biomeetrilised andmed teeb seal nimekirjas eriliseks asjaolu, et keelatud on töödelda „füüsilise isiku kordumatuks tuvastamiseks kasutatatavaid biomeetrilisi andmeid.“[69] Selline sõnastus toob lisakriteeriumi biomeetriliste andmete eriliigilisteks isikuandmeteks klassifitseerimisele. See tähendab, et kõigile Määruse kohalduvusalasse kuuluvatele isikutele, nii riigiasutustele kui eraorganisatsioonidele, on printsiibis keelatud biomeetriliste andmete töötlemine kordumatuks tuvastamiseks.

Biomeetriliste andmete puhul oli andmekaitse reformi paketi koostamisel probleemiks, et mitmeid aastaid oli kestnud debatt teemal, kas biomeetrilised andmed on ise eriliigilised isikuandmed või nad paljastavad teisi eriliigilisi isikuandmeid. Tähelepanu all on siin olnud eelkõige rassile ja etnilisele päritolule viitamine.[70] Samuti on hiljutised teadusuuringud näidanud, et sõrmejälg paljastab mitmeid terviseandmeid. Sõrmejälg moodustub koos loote arenguga ja näitab näiteks *Downi* sündroomi olemasolu.[71] Samamoodi on häältuvastamisel

[66] Määrus, preambul p 51.
[67] Määrus, preambul p 51.
[68] Määrus, art 9 lg 1.
[69] Määrus, art 9 lg 1.
[70] Artikkel 29 Töörühm. Opinion 3/2012 on developments in biometric technologies. Lk 15; Kindt 2012, lk 93.
[71] Kindt 2012, lk 241.

võimalik inimese häälest aru saada, kui tal on Parkinsoni tõbi või ta on kuulmispuudega.[72] Hoolimata sellest, et biomeetrilised andmed sisaldavad teisi eriliigilisi isikuandmeid, ei lisatud biomeetrilisi andmeid Määrusesse siiski eriliigiliste isikuandmetena absoluutsel kujul, vaid piiri paneb ette kasutamise eesmärk. Seega nagu eelpool analüüsitud, on biomeetrilised andmed Määruse järgi eriliigilised isikuandmed vaid siis, kui neid kasutatakse konkreetsete tehniliste vahenditega füüsilise isiku kordumatuks tuvastamiseks.

Teisisõnu teeb Määrus vahet biomeetriliste andmete omamisel ja kasutamisel. Omamisest kasutamiseni on väike samm ja on risk, et andmesubjekt võib kergelt kaotada kontrolli oma isikuandmete edaspidise kasutamise üle. Biomeetriliste andmete kasutamise eesmärgi rõhutamine eriliigiliste isikuandmete nimekirjas tõstatab mitmeid küsimusi, nagu kas piisab kui vastutav töötleja kogub biomeetrilisi andmeid andmebaasi teades, et andmete hoidmine tulevikus võimaldab identifitseerimist. Samuti on ebaselge, kuidas liigitub isikuandmete kogumine juhul, kui vastutaval töötlejal on plaanis andmeid kasutada identifitseerimiseks alles kauges tulevikus või selline plaan on mõnel kolmandal isikul. EIK lahendis *S. and Marper* oli kohus seisukohal, et ainuüksi sõrmejälgede hoidmine struktureeritud kujul on iseenesest eraelu puutumatuse rikkumine ja siinkohal ei ole oluline andmete edasine kasutamine.[73] Teises EIKi lahendis *M.K. v. France* kinnitas kohus seda seisukohta öeldes, et inimeste nimede ja sõrmejälgede piiramatu kogumise ja hoidmisega andmebaasis kaasneb stigmatiseerimise risk ja tegemist on ebaproportsionaalse eraellu sekkumisega.[74] Need lahendid näitavad, kui ohtlikuks eraelu puutumatusele loeb EIK biomeetrilisi andmebaase olenemata nende võimalikest kasutusviisidest. Sellega peaks arvestama vastutav töötleja, kui kaalub kas tema töödeldavad biomeetrilised andmed käivad artikkel 9 eriliigiliste isikuandmete nimekirja või mitte. Ei saa eirata asjaolu, et Määruse teksti autorid on püüdnud eristada artikleid 4 ja 9. Seega kui artikkel 4 biomeetriliste andmete määratlus võib hõlmata laia valikut biomeetrilisi andmebaase, siis artikli 9 kohaldamiseks tuleks vastutaval töötlejal leida piir, kus andmebaaside loomise eesmärk ja kasutamise viis rikuvad oluliselt andmesubjekti eraelu puutumatust. Näiteks lahendis *M.K. v. France* oli üheks põhiprobleemiks andmete säilitamine 25 aastat, mis andmesubjekti jaoks on hoomamatu ajaperiood ja on võimatu ennustada andmebaasi kasutamise viise nii pika aja peale. Eelnevast tulenevalt on oluline nii andmete hoidmise konkreetne kontekst, kuid sama oluline on, kui andmed oma kogumise viisilt

[72] Kindt 2012, lk 243.
[73] *S. and Marper*, pp 67, 124.
[74] EIKo. 18.04.2013, no.19522/09, *M.K. v. France*, pp 33, 37, 43. Edaspidi *M.K. v. France*.

võimaldavad tuvastamist ja on sobivad biomeetriliseks võrdlemiseks teiste juba olemasolevate biomeetriliste andmebaasidega.

Eriliigiliste isikuandmete töötlemine on lubatud vaid artikkel 9 teises lõikes toodud erandjuhtudel. Vahe tegemine, kas biomeetriliste andmete puhul on tegemist tavaliste või eriliigiliste isikuandmetega, on oluline vastutavale töötlejale töötlemiseks õigusliku aluse valikul. Vastutav töötleja peab igal üksikul juhul analüüsima, kas tema kasutatav tehnoloogia sisaldab endas esiteks andmeid isiku füüsiliste, füsioloogiliste ja käitumuslike omaduste kohta ja teiseks, kas need andmed tuvastavad isiku kordumatult. Kui vastus mõlemale küsimusele on jaatav, peab vastutav töötleja vaatama Määruse artikkel 9 lõiget 2, kus on loetletud õiguslikud alused eriliigiliste isikuandmete töötlemiseks. Nende hulgas on selgesõnaline nõusolek, mis erineb nõusolekust, mida võib küsida tavaliste isikuandmete töötlemiseks. Kui vastutav töötleja leiab, et ta ei töötle artikkel 9 kohaselt biomeetrilisi andmeid, siis võib ta valida õigusliku aluse Määruse artiklist 6. Kui vastutav töötleja otsustab kasutada anonümiseerimist, siis peab ta arvestama, et õiguskirjanduses arvatakse, et biomeetrilisi andmeid ei saa anonüümselt töödelda, sest biomeetriline informatsioon ei ole kunagi absoluutselt anonüümne.[75] Sellest hoolimata biomeetrilisi tunnuseid kasutatakse suures osas tehnoloogiates, mis andmete töötlemisel kasutavad tehisintellekti, masinõpet ja suurandmete analüütikat, kus läheb kaotsi andmete töötlemise läbipaistvus ja töötlemine võib viia ettearvamatute tulemusteni.[76] Seega võib vastutav töötleja kergesti leida end olukorras, kus ta on töödelnud eriliigilisi isikuandmeid ilma kehtiva õigusliku aluseta. Eelnevast tulenevalt on igal vastutaval töötlejal oluline teada, kuidas tema poolt kogutavad andmed võivad klassifitseeruda.

1.5.Õiguslikud alused biomeetriliste andmete töötlemisel

Euroopas on andmekaitse põhiõigus *sui generis* Euroopa Liidu põhiõiguste harta artikkel 8 lg 1 kohaselt.[77] Harta artikkel 8 kohaselt peab isikuandmete töötlemiseks olema õiguslik alus.[78] Võimalikke õiguslikke aluseid biomeetriliste isikuandmete töötlemiseks leiab Määrusest

[75] Y. Liu. Identifying Legal Concerns in the Biometric Context. - Journal of International Commercial Law and Technology 2008, Vol 3, No 1, lk 48; R. Sanchez-Reillo jt. How to implement EU data protection regulation for R&D in biometrics. - Computer Standards & Interfaces 2019, Vol 61, lk 91.
[76] Information Commissioner's Office. Big data, artificial intelligence, machine learning and data protection. *Sine loco* 2017, lk 10. Kättesaadav arvutivõrgus: https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf. Edaspidi Information Commissioner's Office. Big data, artificial intelligence, machine learning and data protection.
[77] Euroopa Liidu põhiõiguste harta. - ELT C 326, 26.10.2012. Edaspidi Harta.
[78] Harta art 8 lg 2.

hulganisti. Probleemiks füüsilistele, füsioloogilistele ja käitumuslikele tunnustele vastavate isikuandmete töötlemisel saab asjaolu, et artikkel 4 definitsioon on nii lai, et neid andmeid võib paigutada mitme Määruse sätte alla. Eelnevast analüüsist on selge, et biomeetrilised andmed jaotuvad kahte kategooriasse: tavalised ja eriliigilised isikuandmed. Millisesse kategooriasse töödeldavad isikuandmed kuuluvad, sõltub suuresti biomeetriliste andmete kasutusest.

Esiteks tavaliste isikuandmetena klassifitseerides võib vastutav töötleja valida Määruse artiklist 6 õigusliku aluse.[79] Erasektoris biomeetrilise teenuse pakkumisel peab vastutav töötleja tõenäoliselt valima nõusoleku, lepingu või enda või kolmanda isiku õigustatud huvi vahel. Eelnevast analüüsist tulenevalt saab artiklist 6 õigusliku alusel valida, kui biomeetriliste andmete töötlemise eesmärk ei ole füüsiliste isikute kordumatu tuvastamine ega biomeetriliste andmete töötlemine ei ohusta oluliselt andmesubjekti eraelu puutumatust. Selline töötlemine on näiteks klientide kõnesalvestuste logi pidamine vastutava töötleja klienditeeninduse parendamiseks või töötajate koolitamiseks.

Ettevõtted töötlevad tihti isikuandmeid paralleelselt mitmel eesmärgil ja töötlemise aluseks on rohkem kui üks õiguslik alus, näiteks osa kliendi isikuandmete töötlemisest toimub lepingu, osa nõusoleku ja osa juriidilise kohustuse alusel. Artikkel 29 Töörühm on oma arvamuses kehtiva nõusoleku kohta öelnud, et vastutavad töötlejad peavad algusest peale olema selged selles osas, milline töötlemise eesmärk käib millise isikuandmete tüübi kohta ja millisele õiguslikule alusele toetutakse.[80] Läbipaistvuse printsiibi ja Määruse artiklite 13 ja 14 informatsiooni kohustuste kohaselt tuleb igast töötlemise õigusliku aluse muutusest andmesubjekti teavitada. Artikkel 29 Töörühm on seisukohal, et inimeste suhtes oleks fundamentaalselt ebaõiglane, kui vastutav töötleja annab mõista, et töötlemiseks õiguslik alus on nõusolek samal ajal, kui tegelikult toetutakse hoopis teisele alusele.[81] Kuigi vastutav töötleja peab juba piisavalt vaeva nägema Määruse artiklist 6 õigusliku aluse valimisega, muutub olukord keerulisemaks, kui vastutav töötleja ei tee kindlaks, kas ta töötleb biomeetrilises tehnoloogias eriliigilisi isikuandmeid või tavalisi isikuandmeid. Samal ajal tuleneb eelnevast analüüsist, et on ebaselge, millisel ajahetkel muutuvad vastutava töötleja poolt kogutud tavalised isikuandmed biomeetrilisteks andmeteks ja sealt edasi eriliigilisteks biomeetrilisteks

[79] Määrus art 6 lg 1 pp a – f.
[80] Artikkel 29 Andmekaitse Töörühm. Guidelines on consent under Regulation 2016/679. 17/NE. WP259 rev.01. 10.04.2018, lk 22. Kättesaadav arvutivõrgus: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051. Edaspidi Artikkel 29 Töörühm. Guidelines on consent under Regulation 2016/679.
[81] Artikkel 29 Töörühm. Guidelines on consent under Regulation 2016/679. Lk 23.

andmeteks. Ebaselge on ka millised biomeetrilised andmed on tavalised isikuandmed, näiteks fotod nägudest *versus* fotod sõrmejälgedest. Selline mitmetasandiline ebaselgus muudab Määrusega antava kaitse vaid teoreetiliseks ja seetõttu on ELi liikmesriikidelt oodata lahknevaid regulatsioone.

Kui vastutaval töötlejal on kahtlus, et ta töötleb eriliigilisi isikuandmeid, peab ta analüüsima Määruse artiklit 9. Õiguslik alus tuleb leida artikkel 9 lõike 2 valiku seast: selgesõnaline nõusolek; töötlemine on vajalik seoses vastutava töötleja või andmesubjekti tööõigusest ning sotsiaalkindlustuse ja sotsiaalkaitse valdkonna õigusest tulenevate kohustuste ja eriõigustega; töötlemine on vajalik selleks, et kaitsta andmesubjekti või teise füüsilise isiku elulisi huve; isikuandmeid töödeldakse poliitilise, filosoofilise, religioosse või ametiühingulise suunitlusega sihtasutuse, ühenduse või muu mittetulundusühingu õiguspärase tegevuse raames; töödeldakse isikuandmeid, mille andmesubjekt on ilmselgelt avalikustanud; töötlemine on vajalik õigusnõude koostamiseks, esitamiseks või kaitsmiseks; vajalikkus olulise avaliku huviga seotud põhjustel liidu või liikmesriigi õiguse alusel ning on proportsionaalne saavutatava eesmärgiga; vajalikkus ennetava meditsiini või töömeditsiiniga seotud põhjustel, töötaja töövõime hindamiseks, meditsiinilise diagnoosi panemiseks, tervishoiuteenuste või sotsiaalhoolekande või ravi võimaldamiseks või tervishoiu- või sotsiaalhoolekandesüsteemi ja -teenuste korraldamiseks; vajalikkus avalikes huvides toimuva arhiveerimise, teadus- või ajaloouuringute või statistilisel eesmärgil.[82] Kuna käesoleva magistritöö eesmärk on uurida vastutava töötleja vabatahtlikku soovi biomeetrilisi isikuandmeid töödelda, siis tulenevalt biomeetriliste andmete omadustest keskendub autor artikli 9 lg 2 õiguslike aluste analüüsil selgesõnalisele nõusolekule ja isikuandmete töötlemisele, mida andmesubjekt on ilmselgelt avalikustanud. Sellegipoolest hinnatakse nende õiguslike aluste sobivust erinevates olukordades võrreldes teiste artikkel 9 lg 2 õiguslike alustega.

Lisades artikli 9 analüüsi vastutava töötleja kohustuste hulka, võib vastutaval töötlejal olenevalt isikuandmete tüübist tekkida küsimus, millised biomeetrilised isikuandmed on andmesubjekt ise avalikustanud. Määruses puudub seletus, mida tähendab „ilmselgelt ise avalikustanud." Kas vastutav töötleja võib sel alusel füüsilise isiku kordumatuks tuvastamiseks kasutada näiteks andmesubjekti poolt sotsiaalmeediasse üles laetud fotosid? Määruse tekstist jääb mulje nagu võiks näotuvastustehnoloogiaid kasutada ilma andmesubjekti selgesõnalise nõusoleku või olulise avaliku huvita. Seega vajab magistritöö järgmises osas edasist uurimist

[82] Määrus art 9 lg 2 (a) – (j).

andmesubjekti poolt avalikustatud isikuandmete töötlemise aluse eristamine selgesõnalisest nõusolekust.

Teine võimalik töötlemise alus artiklis 9 lg 2 on selgesõnaline nõusolek. Nõusolek on „vabatahtlik, konkreetne, teadlik ja ühemõtteline tahteavaldus, millega andmesubjekt kas avalduse vormis või selge nõusolekut väljendava tegevusega nõustub tema kohta käivate isikuandmete töötlemisega.“[83] Biomeetriliste tehnoloogiate puhul tekib probleem juba esimese nõusoleku tingimusega: vabatahtlikkus. Vabatahtlikkuse kriteerium viitab andmesubjektide reaalsele valikuvõimalusele ja kontrollile.[84] Biomeetrilisi tehnoloogiaid kasutatakse aga palju tarbijaseadmetes, nn asjade internetis, koos masinõppe ja tehisintellektiga. Paljudel juhtudel puudub sellistel seadmetel mobiiltelefoni ekraaniga sarnane graafiline kasutajaliides, vaid seadmed on tihti diskreetsed. Selliste seadmetega puutub kokku määramata isikute ring, kui tegelikkuses selgesõnalist nõusolekut küsiti vaid seadme omanikult. Näiteks võib koduukse kohal olev turvakaamera tuvastada külalisi või sõiduauto tuvastada kaassõitjaid. Kehtiva nõusoleku olemasolu peab aga tõendama vastutav töötleja.[85] Seega vajab käesolevas töös edasist uurimist, kuidas vastutav töötleja tagab kehtiva nõusoleku olemasolu biomeetriliste tehnoloogiate kasutamiseks.

Lisaks artiklitele 6 ja 9 on Määruses veel üks oluline säte õigusliku aluse leidmiseks. Kui vastutava töötleja tegevus viitab profileerimisele, siis tuleb õiguslik alus võtta artiklist 22 lg 2. Töötlemise alused profiilianalüüsile on järgnevad: andmesubjekti ja vastutava töötleja vahelise lepingu sõlmimiseks või täitmiseks; lubatud vastutava töötleja suhtes kohaldatava liidu või liikmesriigi õigusega; põhineb andmesubjekti selgesõnalisel nõusolekul. Sama artikli lõige 4 aga sätestab, et profiilianalüüsil põhinevaid otsuseid ei või teha eriliiki isikuandmete töötlemisel, välja arvatud kui selleks on andmesubjekti selgesõnaline nõusolek või õiguslikuks aluseks on avalik huvi. Profiilianalüüse luuakse inimeste käitumismustrite alusel. Käitumuslikud andmed on biomeetriliste andmete liik ja kasutusel nii tuvastustehnoloogiates, asjade internetis kui ka *online* analüütika tööriistades. Enamasti on need seotud ka suurandmete töötlusega. Suurandmete töötluse mõte on koguda ja analüüsida kõiki kättesaadavaid andmeid. Kuigi puudub üks kindel suurandmete definitsioon, siis oma olemuselt on need andmed, mida erinevate ja muutuvate omaduste tõttu on raske traditsioonilisel viisil analüüsida. Seetõttu on suurandmetega lähedalt seotud tehisintellekt. Tehisintellekti põhiline omadus on, et

[83] Määrus art 2 p 11.
[84] Artikkel 29 Töörühm. Guidelines on consent under Regulation 2016/679. Lk 5.
[85] Määrus art 7 lg 1.

tehisintellekti programmid ei analüüsi andmeid lineaarselt sellisel viisil nagu esialgu neid oli programmeeritud, vaid nad õpivad ise ette antud andmetest ja vastavalt kohandavad ise analüüsi tulemusi. Teisisõnu tehisintellektil on omadus olla inimlikult intelligentne.[86] Seega tekib siin jällegi muutuva õigusliku aluse probleem, kus vastutav töötleja peab ette nägema kuidas tema kasutatavad algoritmid võivad muuta biomeetrilisi andmeid tavalistest eriliigilisteks või kuidas profiilianalüüs muutub biomeetriliseks tuvastamiseks. See on aga ääretult keeruline, kui analüütika tööriist põhineb masinõppel ja tehisintellektil.

1.6. Peatüki kokkuvõte

Biomeetrilised andmed on inimese füüsilised, füsioloogilised või käitumuslikud tunnused, mis on printsiibis igal inimesel, elu jooksul suhteliselt muutumatud ja võimaldavad konkreetset inimest teistest eristada ehk universaalsed, püsivad ja unikaalsed. 2018. kevadel jõustunud Määrus püüab reguleerida uue isikuandmete tüübina biomeetrilisi andmeid. Määrus jaotab biomeetrilised andmed kaheks: tavalised isikuandmed ja eriliigilised isikuandmed. Samal ajal on jäetud kahe isikuandmete klassifikatsiooni erinevus mitmeti mõistetavaks ja lõplik vastutus õige liigitamise üle lasub vastutaval töötlejal. Määruse artiklis 4 toodud biomeetriliste andmete definitsiooni järgi on isikuandmed biomeetrilised andmed, kui nad on seotud isiku füüsiliste, füsioloogiliste või käitumuslike omadustega, mis on saadud konkreetse tehnilise töötlemise abil ja võimaldavad füüsilist isikut kordumatult tuvastada. Autori hinnangul tuleb lugeda konkreetse tehnilise töötlemise kriteerium täidetuks, kui isikuandmeid töödeldakse tehniliste vahenditega viisil, mis loob biomeetrilistest tunnustest andmekogusid ja sellised andekogud võimaldavad mõistliku vaevaga isikut grupist eraldada.

Võtmekriteerium biomeetriliste andmete liigitamisel on kordumatu tuvastamise nõue. Esiteks on isikuandmed biomeetrilised andmed, kui nad võimaldavad kordumatut tuvastamist ja teiseks on tegemist Määruse artikkel 9 lg 1 järgi eriliigiliste isikuandmetega, kui neid kasutatakse kordumatuks tuvastamiseks. Käesoleva osa analüüsist tulenevalt leiti, et biomeetrilisteks andmeteks Määruse mõistes liigituvad andmed, mis võimaldavad piisavalt täpselt ja igakordselt füüsilist isikut tuvastada ja iga kord tuleb sellest vaatenurgast biomeetrilist tehnoloogiat ka hinnata. Tehnoloogia neutraalsuse põhimõttest lähtuvalt ei saa

[86] Information Commissioner's Office. Big data, artificial intelligence, machine learning and data protection, lk 7

ennetavalt välistada teatud veamääraga tehnoloogiaid. Sealjuures tuleks arvestada ka et biomeetrilised tunnused kannavad teatud vahelüli rolli isiku identiteedi ja teiste andmebaaside vahel. Teisisõnu hinnata tuleks, kui tõenäoline on kasutatava tehnoloogia olemust arvestades, et biomeetrilised andmed aitavad isikut tulevikus identifitseerida kombineerituna muu informatsiooniga. Määruse teksti autorid on püüdnud eristada artikleid 4 ja 9. Vahet tehakse andmete omamisel ja kasutamisel. Seega kui artikkel 4 p 14 biomeetriliste andmete määratlus võib hõlmata laia valikut biomeetrilisi andmebaase, siis artikli 9 kohaldamiseks tuleks vastutaval töötlejal leida piir, kus andmebaaside loomise eesmärk ja kasutamise viis rikuvad oluliselt andmesubjekti eraelu puutumatust.

Õigusliku aluse valikul saab probleemiks asjaolu, et enamasti on biomeetriliste andmete töötlemine hall ala, kus õigusliku aluse valik sõltub igal üksikul juhul suuresti töötlemise viisist ja eesmärgist. Veel üks probleem vastutavatele töötlejatele, mis tuleneb Määrusest on liikmesriikide õigus sätestada eri tingimusi ja piiranguid biomeetriliste andmete töötlemisele ja vastutavad töötlejad võivad oodata riigiti lahknevaid arvamusi.

Eelnevast tulenevalt analüüsitakse järgmistes osades sobiva õigusliku aluse leidmist olukordades, kus vastutav töötleja enda soovil vabatahtlikult kasutab biomeetrilisi süsteeme. Autor alustab kõige kitsamast biomeetriliste andmete määratlusest ehk eriliigiliste isikuandmete töötlemisest. Seega analüüsitakse esiteks andmesubjekti poolt ise avalikustatud isikuandmete töötlemise õiguslikku alust ja seejärel andmesubjekti selgesõnalist nõusolekut. Eesmärk on leida vastus küsimusele, millal on selgesõnaline nõusolek kõige sobivam õiguslik alus ja milline on andmesubjekti kehtiv nõusolek biomeetriliste tehnoloogiate kasutamiseks.

Magistritöö viimases osas analüüsitakse õiguslikke aluseid biomeetriliste andmete töötlemisel nö hallis alas, kus esmapilgul ei ole selge, kas tegemist on tavaliste või eriliigiliste biomeetriliste andmetega. Leitakse vastus küsimusele, kuidas toimub samade isikuandmete tüüpide töötlemisel õigusliku aluse muutus artiklilt 6 artiklile 9. Seetõttu on oluline uurida, milline on artiklite 9 ja 22 koosmõju biomeetriliste andmete töötlemise kontekstis.

2. Õigusliku aluse valik biomeetriliste andmete töötlemiseks eesmärgiga isik tuvastada

Biomeetrilised tehnoloogiad moodustavad osa ühiskonda üha rohkem ümbritsevast nuti-keskkonnast. Biosensoreid leiab nii telefonidest, lennujaamadest, poodidest, koolidest kui ka kodust. Nende tehnoloogiate kasutusviis on lõputu ja seetõttu ka biomeetriliste andmete töötlemiseks õigusliku aluse kehtivuse hindamisel tuleb lähtuda eelkõige kontekstist. Nõusolek, mille andmesubjekt annab oma biomeetriliste andmete töötlemiseks kodutehnikas ei pruugi enam olla kehtiv nõusoleku viis näotuvastustehnoloogia abil telefoni avamiseks. Ühel juhul võib olla tegemist tavaliste isikuandmetega ja teisel juhul eriliigilistega.

Magistritöö esimeses osas leiti, et biomeetrilised andmed on Määruse järgi eriliigilised isikuandmed vaid siis, kui neid kasutatakse konkreetsete tehniliste vahenditega füüsilise isiku kordumatuks tuvastamiseks. Andmesubjekti selgesõnaline nõusolek on üldine alus eriliigiliste isikuandmete töötlemiseks ja väljendab kontrolli teostamist oma isikuandmete kasutamise üle. Sellest hoolimata on vastutavatel töötlejatel võimalik eriliigiliste biomeetriliste andmete töötlemisel valida õiguslikuks aluseks ka midagi muud peale selgesõnalise nõusoleku. Käesolevas osas leitakse, millised on sobivad õiguslikud alused Määruse artiklist 9 lg 2 erinevates olukordades, kus võib öelda, et töödeldakse eriliigilisi biomeetrilisi andmeid. Fookus on andmesubjekti selgesõnalise nõusoleku võrdlemisel teiste alustega, sest magistritöös uuritakse vastutavate töötlejate poolt vabatahtlikult biomeetriliste süsteemide kasutamist.

Nagu eelnevalt leitud, siis biomeetrilised tunnused on suures osas kättesaadavad nii avalikus ruumis kui internetis. Seega alustatakse käesolevat osa analüüsiga, millal on andmesubjekt oma isikuandmed sellisel viisil avalikustanud, et nende edasine töötlemine ei nõua täiendavat õiguslikku alust. Alternatiivina andmesubjekti nõusolekule uuritakse Määruse artiklit 9 lg 2 p e ehk isikuandmete töötlemist, mida andmesubjekt on ise avalikustanud. Piltide ja videote tegemine võib paljastada inimeste mõtteid ja tundeid. Viis, kuidas inimesed kõnnivad näiteks paljastab nende psühholoogilise seisundi, nagu õnnelikkus või depressioon.[87] Eksperimendid on näidanud, et suure hulga fotode tõttu internetis suudavad näotuvastustehnoloogiad juba

[87] Euroopa Komisjon. Horizon 2020. Gait Biometrics 3 (Main goal of the project is to create a prototype of the software, which will be able to identify peoplejust based on the way how they walk). 31.07.2015. Kättesaadav arvutivõrgus: https://cordis.europa.eu/project/rcn/196201/factsheet/en.

tuvastada üpris täpselt fotol olevaid inimesi.[88] Seega tuleb leida vastus küsimusele millal üldse on vaja andmesubjekti poolt avalikustatud eriliigiliste isikuandmete puhul ikkagi endiselt küsida andmesubjekti nõusolekut edasiseks töötlemiseks. Fookuses on vastutava töötleja endaalgatuslik biomeetriline tuvastamine ilma andmesubjekti otsese aktiivse osaluseta.

Seejärel analüüsitakse erinevaid olukordi, kus biomeetrilist tuvastamist kasutatakse andmesubjekti osalusel ligipääsuvõtmena konfidentsiaalsele teabele, teistele isikuandmetele või tehingute autoriseerimiseks. Vastutaval töötlejal on biomeetrilise süsteemi kasutamiseks teoreetiliselt võimalus tugineda andmesubjekti selgesõnalisele nõusolekule. Sobivaima õigusliku aluse leidmiseks võrreldakse vastavates olukordades selgesõnalist nõusolekut teiste võimalike alternatiividega. Käesoleva osa viimases peatükis leitakse, millised on tingimused kehtivale nõusolekule biomeetrilistes tuvastustehnoloogiates. Kehtivale nõusolekule seatavaid tingimusi hinnatakse vastavalt riskidele, mida biomeetriline süsteem endaga kaasa toob.

2.1. Andmesubjekti poolt isikuandmete avalikustamine õigusliku alusena

Käesoleva peatüki eesmärk on leida vastus küsimusele, millal väljub eriliigiliste isikuandmete töötlemine Määruse artikkel 9 lg 2 p e toodud andmesubjekti poolt avalikustatud isikuandmete töötlemise erandist. Andmesubjekti poolt avalikustatud isikuandmete töötlemine oli eriliigiliste isikuandmete töötlemise aluseks juba vanas Direktiivis 95/46/EÜ.[89] Määruses puudub selgitus, mida tähendab „andmesubjekti poolt ilmselgelt avalikustatud“ ja ka õiguskirjandusest ei leia ühest vastust. Kas vastutav töötleja võib sel alusel füüsilise isiku kordumatuks tuvastamiseks kasutada näiteks andmesubjekti poolt sotsiaalmeediasse üles laetud fotosid? Määruse tekstist jääb mulje nagu võiks näotuvastustehnoloogiaid kasutada ilma andmesubjekti selgesõnalise nõusoleku või olulise avaliku huvita. Samasugune erand eriliigiliste isikuandmete töötlemise keelule on ka politseikoostöö ja õigusalase koostöö Direktiivis.[90] Ka politseikoostöö ja õigusalase koostöö Direktiivist jääb mulje, et avalikustamise õiguslik alus on ääretult lai ja lubaks justkui jälitus ühiskonna teket, kus avalikus ruumis kaamerad kordumatult tuvastavad möödakäijaid.

[88] A. Kotsios. Privacy in an Augmented Reality. - International Journal of Law and Information Technology 2015, No 23, lk 171. Edaspidi Kotsios.
[89] Direktiiv 95/46/EÜ art 8 lg 2 p e.
[90] Politseikoostöö ja õigusalase koostöö Direktiiv art 10 p c.

Kuna tegemist on erandiga eriliigiliste isikuandmete töötlemise keelule, siis peab seda alust tõlgendama kitsalt ja selliselt, et andmesubjekt on tahtlikult teinud oma andmed avalikuks.[91] Näiteks ei ole võimalik artikkel 9 lg 2 p e alust kasutada edasiseks isikuandmete töötlemiseks olukorras, kus telekanal näitab turvakaamera salvestust õnnetusjuhtumist. Sellisel juhul ei ole isikud videol tahtlikult ise oma andmeid avalikustanud.[92] Samuti on nii Artikkel 29 Töörühm kui Eesti kohtud rõhutanud eesmärgi piiritlemise põhimõtet andmesubjekti poolt avalikustatud andmete edasisel töötlemisel vastutavate töötlejate poolt.[93] Järgneva analüüsi fookuses on avalikult kättesaadavate biomeetriliste andmete edasine kasutamine suures ulatuses ja süsteemselt kolmandate isikute poolt. Siinkohal jäetakse analüüsist välja biomeetriliste andmete töötlemine, mida füüsiline isik teostab eranditult isiklikel või kodustel eesmärkidel. Selline töötlemine väljub Määruse kohaldamisalast.[94]

Biomeetriliste andmete kontekstis tõusetub andmesubjekti poolt avalikustatud andmete edasise kasutamise küsimus eelkõige eri sotsiaalmeedia kanalitest kättesaadava informatsiooniga. Sotsiaalmeedia hõlmab suurt hulka materjali, sh avalikke postitusi Facebookis, Twitteris, videoid YouToube'is. Digitaalruumis maailmale avalikustatud materjali maht ja olulisus on peaaegu hoomamatu. Seega on vaja küsida, millised mõistlikud ootused privaatsusele võivad olla avaliku sotsiaalmeedia kasutajatel? Kirjanduses on jaotatud sotsiaalmeediat kinniseks ja avatuks.[95] Kinnine tähendab, et sotsiaalmeedia konto on näha vaid valitud sõpradele või kaitstud parooliga. Nii avalik kui erasektor suuresti eeldavad, et sotsiaalmeedia kommunikatsiooni, mis on kättesaadav avalikkusele ilma sõprade nimekirja piiranguta, paroolideta või krüpteeringuta, on õiglane kasutada jälituseks ja sellele ei kehti privaatsuse kaitse põhimõtted.[96] Autor on seisukohal, et kui kasutaja avalikustab privaatset materjali veebilehel, mille kasutajatingimused viitavad avalikkuse ligipääsule, siis säilib tal endiselt õigus privaatsuse kaitsele. Esiteks jäävad endiselt kehtima teised Määruse põhimõtted nagu andmete minimaalsus, eesmärgi piiritletus ja töötlemise läbipaistvus, mis muudab vastutavale töötlejale sotsiaalmeediast saadud andmete edasise töötlemise suhteliselt piiratuks ja

[91] Handbook on European Data Protection Law. Luxembourg: Publications Office of the European Union 2018, lk 162. Edaspidi Handbook.
[92] *Ibid* lk 161.
[93] Artikkel 29 Andmekaitse Töörühm. Opinion 3/13 on purpose limitation. 00569/13/NE. WP 203. 02.04.2013, lk. 14. Kättesaadav arvutivõrgus: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf.
[94] Määrus, preambul p 18.
[95] M. Männiko. Õigus privaatsusele ja andmekaitse. Tallinn: Juura 2011, lk 112. Edaspidi Männiko.
[96] L. Edwards, L. Urquhart. Privacy in public spaces: what expectations of privacy do we have in social media intelligence? - International Journal of Law and Information Technology 2016, Vol 24, lk 281. Edaspidi L. Edwards, L. Urquhart.

andmesubjekti on vaja ikkagi informeerida töötlemisest.[97] Teiseks linnukesega kastis „nõustun tingimustega“ ei saa lepinguga võtta ära põhiõigusi. Selline nõusolek tüüptingimustele ei ole vabatahtlik, konkreetne ega informeeritud ja selle kehtivus on vaid illusioon. Artikkel 29 Töörühm on oma arvamuses seda seisukohta kinnitanud.[98] Käesoleva töö autor arvab, et isikuandmete kasutamisel ei peaks fookuses olema andmete allika ehk konkreetse sotsiaalmeedia kanali avalikkus ja kasutajatingimused, vaid rõhuasetus peaks olema viisil kuidas neid andmeid edasi töödeldakse. Vastutus peab kanduma vastutavale töötlejale, mitte lasuma andmesubjektil. Kirjanduses on välja toodud kaks faktorit, mis toetavad mõistlikku ootust privaatsusele avalikus sotsiaalmeedias: esiteks paljud sotsiaalmeedia kasutajad ei taju neid keskkondi avalikena ja teiseks mõju, mis on otsingumootoritel ja teistel analüütika tööriistadel traditsioonilisele struktureeritud andmete kontseptsioonile.[99] Avalikest allikatest andmete kogumise praktikad on saanud järjest tavalisemaks ja sellist jälitustegevust viiakse läbi nii riigi kui eraisikute poolt.

Eesmärgi piiritlemise põhimõttest lähtuvalt on Eesti kohtud analüüsinud andmesubjekti poolt avalikustatud isikuandmete edasist kasutamist. Riigikohus on analüüsinud korduvat avalikustamist. Ainuüksi sellest, et andmed on isiku nõusolekul varem mingis vormis avalikustatud, ei saa järeldada, et täiendaval avalikustamisel ei pruugi andmesubjekti jaoks olla olulisi tagajärgi. Andmete esialgne ja korduv avalikustamine võivad toimuda väga erinevas vormis ja väga erineva intensiivsusega, sõltuvalt andmete edastaja isikust, infokanalist, kontekstist, auditooriumist jne.[100] Mis puutub isiku enda poolt või tema nõusolekul avalikustatud andmetesse, siis tuleb arvestada, et andmesubjekt ei pruugi oma kunagise otsustuse tegemise hetkel olla ette näinud kõiki korduva avalikustamise viise ja nende tagajärgi oma õigustele.[101] Samuti on Eesti kohtupraktikas leitud, et ka siis, kui isik on ise enda kohta käivaid isikuandmeid avalikustanud, ei saa nende korduval avalikustamisel või töötlemisel siiski IKS § 11 lõikele 1 tugineda,[102] mistõttu ka avalikustatud andmete kasutamiseks on vajalik seaduslikku alust, milleks võib olla andmesubjekti nõusolek.[103] Eesti kohtupraktikast saab

[97] Määrus art 14.
[98] Artikkel 29 Töörühm. Guidelines on consent under Regulation 2016/679. Lk 16.
[99] L. Edwards, L. Urquhart, lk 279.
[100] RKTKo 3-3-1-3-12, p 24.
[101] RKTKo 3-3-1-3-12, p 25.
[102] Isikuandmete kaitse seadus – RT I 2007, 24, 127. § 11 lg 1 sätestas: „Kui andmesubjekt on oma isikuandmed avalikustanud ise, andnud käesoleva seaduse § 12 kohase nõusoleku nende avalikustamiseks või kui isikuandmed avalikustatakse seaduse, sealhulgas käesoleva paragrahvi lõike 2 alusel, siis ei kohaldata isikuandmete töötlemisele käesoleva seaduse teisi paragrahve.“
[103] RKTKo 3-2-1-159-14 p 14.

järeldada, et andmesubjekti poolt avalikustatud isikuandmete edasine kasutamine on äärmiselt kitsalt piiritletud. Vastutav töötleja peab arvesse võtma konteksti muutust, töötlemise intensiivsust ja asjaolu, kui ettenähtav edasine töötlemine kavandataval viisil andmesubjektile oma isikuandmete avalikustamise hetkel oli.

Arvestades eelnevalt leitud kriteeriume, millega vastutav töötleja peab arvestama, saab neist lähtudes analüüsida privaatsuse kaitse ulatust sotsiaalmeedias avalikustatud isikuandmetele. Peamine rahvusvaheline regulatsioon siin on Euroopa põhiõiguste ja vabaduste konventsioon 1955. aastast[104] (edaspidi Inimõiguste Konventsioon) artikkel 8, mis näeb ette era- ja pereelu puutumatuse kaitse.[105] EIK ja EK teevad sotsiaalmeedia andmete puhul vahet, kas tegemist on struktureeritud või struktureerimata andmetega. EIK lahendis *Rotaru v. Romania* leidis kohus, et ainuüksi andmesubjekti jälgimine ei pruugi rikkuda Konventsiooni artiklit 8, küll aga tema kohta andmete süstemaatiline kogumine, kasutamine ja hoidmine rikub tõenäoliselt küll artiklit 8.[106] Samale järeldusele jõudis EIK lahendis *Segerstedt-Wiberg v Sweden*, kus Rootsi politsei hoidis avaldaja kohta avalikest allikatest (ajalehed) kogutud andmeid. Kohus leidis, et ka avalikest allikatest saadud andmed, mis on süstemaatiliselt kogutud, on eraelu puudutavad andmed. Ajalooliselt on politsei laadi jälitust päris politsei jälitusest eristanud süsteemsete kaustade koostamine ja hoidmine.[107] *Segerstedt-Wilburg* lahendist lähtuvalt saab öelda, et avalikult kättesaadavat eraelu puudutavat infot saab jälgida ja koguda nii kaua kuni sellest ei looda detailset kausta konkreetsest andmesubjektist. Biomeetriliste andmete puhul on toodud välja just nende ajaloolist seotust õiguskaitseorganite andmebaasidega ja sellest tulenevat diskrimineerimise hirmu. Näiteks Prantsusmaa andmekaitse järelevalveasutus CNIL on avaldanud mitu arvamust sõrmejälgede kasutamise kohta erasektoris. Juba 2001. aastal leidis CNIL, et hoolimata sellest, et sõrmejälgede andmebaas luuakse erasektoris, muutub see mingil hetkel politsei instrumendiks ja sellega muutub töötlemise eesmärk.[108] EK *Google Spain* lahendis on kohus öelnud, et kuna kõnealune töötlemine võimaldab igal interneti kasutajal omandada läbi otsingutulemuste nimekirja inimese kohta internetist leitavast infost, siis saab vastutav töötleja struktureeritud ülevaate inimest puudutavast infost. See info puudutab tõenäoliselt suurt hulka andmesubjekti eraelu aspektidest, mida ilma otsingumootorita ei oleks

[104] Inimõiguste ja põhivabaduste kaitse konventsioon. - RT II 2000, 11, 57.
[105] Inimõiguste Konventsiooni art 8 lg 1 sätestab: „Igaühel on õigus sellele, et austataks tema era- ja perekonnaelu ja kodu ning sõnumite saladust."
[106] EIKo. 04.05.2000, 28341/95, *Rotaru v. Romania*, p 43. Edaspidi *Rotaru v. Romania.*
[107] EIKo. 06.06.2006, 62332/00, *Segerstedt-Wiberg and Others v. Sweden*, pp 72, 73.
[108] CNIL. 21e rapport d'activité. 2000, Paris 2001, lk 108.

omavahel ühendatud või see oleks olnud väga keeruline. Seetõttu on võimalik luua inimesest detailne profiil. Andmesubjekti õigustesse sekkumise mõju suurendab interneti ja otsingumootorite suur roll käesoleval ajastul, mis teeb sellises nimekirjas oleva info kõikehaaravaks.[109] Kokkuvõtvalt saab järeldada EIKi ja EK praktikatest, et avalikustatud biomeetriliste andmete edasisel töötlemisel on õigusliku aluse valimisel määrav andmete struktureerituse aste. Kui sotsiaalmeediast või muudest avalikest allikatest, nagu meediaväljaannetest kättesaadavatest biomeetrilistest andmetest luuakse põhjalik struktureeritud andmebaas, siis ei või vastutav töötleja tugineda enam Määruse artiklile 9 lg 2 e, vaid peab küsima andmesubjektilt selgesõnalist nõusolekut.

Inimeste elud on suures detailsuses avaldatud sotsiaalmeedia postitustes ja videotes. Arvestades kaasaegseid andmetöötluse meetodeid võib järeldada, et kui ei austata privaatsust avalikustatud isikuandmete osas, ei pruugi varsti enam üldse privaatsust olla. Ei ole õige väita, et inimesed kaudselt annavad ära oma ootused privaatsusele liitudes platvormiga, millel on miljoneid kasutajaid. Ei saa ka tekitada olukorda, kus oma privaatsust on võimelised kaitsma vaid need, kes on tuttavad kaasaegsete andmetöötluse tööriistadega või on tehniliselt piisavalt kirjaoskajad. Andmesubjekti poolt avalikustamist ei saa kasutada õigusliku alusena, kui otsustatakse töödelda sotsiaalmeediast, ajalehtedest, veebilehtedelt või muudest avalikest allikatest saadud eriliigilisi isikuandmeid struktureeritud kujul, oluliselt teises kontekstis, teistel eesmärkidel ja andmesubjekti jaoks ettenägematul viisil. Sellisel juhul on vastutaval töötlejal vaja iga kord küsida biomeetriliseks tuvastamiseks andmesubjektilt selgesõnalist nõusolekut või leida Määruse artiklist 9 lg 2 muu õiguslik alus, kui andmesubjekti poolt eelnev avalikustamine.

2.2. Biomeetriline tuvastamine andmesubjekti osavõtul

Biomeetrilised tehnoloogiad ei ole uued, kuid nende populaarsus on viimastel aastatel kasvanud, kuna nutiseadmete tootjad on hakanud lisama sõrmejälje ja näotuvastustehnoloogiaid mobiiltelefonidele. Apple ja Samsung on teinud biomeetrilised tehnoloogiad tarbijate seas laialt levinuks kasutades biomeetrilisi tunnuseid nii telefonide

[109] EKo. 13.05.2014, Case C-131/12, *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, pp 36, 37. Edaspidi *Google Spain*.

avamiseks kui ka maksete autoriseerimiseks.[110] Ka maksesüsteem PayPal on integreerinud oma mobiilirakenduse mobiiltelefonide biomeetrilise autentimisega, et võimaldada kiiremaid *online* oste.[111] Biomeetrilisi tuvastustehnoloogiad kasutatakse palju töökohtades ligipääsu autoriseerimiseks, tarbija seadmetele ligipääsu võtmena ja mobiilses panganduses, kuid arvatakse, et biomeetrilisel tuvastamisel saab olema kõige suurem mõju finantssektoris.[112] Käesolevas peatükis analüüsitakse eriliigiliste biomeetriliste andmete kasutamist võtmena pääsemaks ligi tundlikemale andmetele, piiratud juurdepääsuga ruumidesse, ärisaladusetele või tehingute autoriseerimiseks ehk biomeetrilisel tuvastamisel osaleb otseselt andmesubjekt ise.

On võimalik, et inimene ühe päeva jooksul kasutab sularahaautomaati, käib töökohas, teeb pangaülekande ja vaatab paarkümmend korda oma mobiiltelefoni. Selle käigus lukustab ta sõrmejäljega lahti oma telefoni, kasutab sõrmejälge nii kontoriukse avamiseks, telefonis rahaülekandeks kui ka automaadist sularaha välja võtmiseks. See on kahtlemata väga mugav kasutaja jaoks, kuid tekitab küsimuse, kui ühes neis süsteemidest peaks toimuma isikuandmete lekkimine, siis kuidas see kasutaja tagab turvalisuse teistes süsteemides, sest oma sõrmejälge ta vahetada ei saa. Teisisõnu biomeetrilised tuvastustehnoloogiad peavad arvestama selliste biomeetrilistele andmetele omaste riskidega inimese privaatsusele, millel on pikaajalised tagajärjed mitmes elusfääris. Käesolevas peatükis uuritakse erinevaid valdkondi, kus vastutav töötleja soovib kasutada biomeetrilist tuvastustehnoloogiat ilma juriidilise kohustuseta seda teha. Magistritöö esimeses osas leiti, et biomeeriliste andmete kasutamisel tuvastamiseks on tegemist eriliigiliste isikuandmetega ja töötlemise üheks õiguslikuks aluseks on andmesubjekti selgesõnaline nõusolek. Vastus tuleb leida küsimusele, kas neis eri situatsioonides on andmesubjekti selgesõnaline nõusolek vastutavale töötlejale kõige sobivam õiguslik alus või võib ka õiguslik alus mõnes olukorras tulla muust Määruse artikkel 9 lg 2 erandist.

---

[110] Alles märtsis 2019 avaldas Apple oma uue tootena maksesüsteemi, mis makse autoriseerimise võtmena kasutab biomeetrilist tunnust. Sarnane toode on varasemalt kasutuses juba Samsungil. Vt Press release. Introducing Apple Card, a new kind of credit card created by Apple. 25.03.2019. Kättesaadav arvutivõrgus: https://www.apple.com/newsroom/2019/03/introducing-apple-card-a-new-kind-of-credit-card-created-by-apple/.

[111] J. Vanian. Lenovo, Intel, and PayPal Team On Fingerprinting Tech For Online Payments. - Fortune. 23.09.2016. Kättesaadav arvutivõrgus: http://fortune.com/2016/09/23/lenovo-intel-paypal-fingerprint-biometrics/.

[112] A. Goode. Biometrics for banking: best practices and barriers to adoption. - Biometric Technology Today. Vol 2018, No 10, lk 5-7. Edaspidi Goode.

2.2.1. Biomeetriline tuvastamine finantssektoris

Konkurentsi surve tõttu on panganduses viimaste aastatega saanud üha olulisemaks klientidele mugava teenuse pakkumine. Kliendil peab olema võimalik pääseda ligi panga teenustele igal ajal ja igas kohas. Samal ajal peab ka olema kindlustatud, et mugava teenuse tõttu finantspettuste hulk ei kasva. Kolmanda probleemina finantssektoris on rangemad rahapesu ja terrorismi tõkestamise regulatsioonid, mistõttu on esmatähtis kliendi identiteedi usaldusväärne tuvastamine. Kõigis neis kolmes omavahel seotud probleemkohas nähakse olulise tööriistana biomeetrilist tehnoloogiat. Biomeetriliste tuvastustehnoloogiate kasutusalad finantssektoris on näiteks:

a. uute klientide identiteedi tuvastamine digitaalselt, kui tahetakse avada uut kontot. „Tunne oma klienti“ reeglid ja autentimine on valukohad, et kliendid saaks kasutada digitaalseid finantsteenuseid. Varasemalt pidid kliendid esitama füüsilise identiteedi dokumendi, nagu passi või juhiloa. Biomeetrilised tehnoloogiad on aga tõestanud, et näotuvastustehnoloogia suudab piisavalt usaldusväärselt kliendi tuvastada. Seetõttu tekib üha rohkem ettevõtteid, kes pakuvad pankadele biomeetrilise tuvastamise teenust (inglise k *Biometric Identity as a Service – BIDaaS*).[113]
b. Biomeetrilised pangakaardid.[114] Sisseehitatud sõrmejälje lugeritega kaarte nähakse kui võimalikku ja mugavat viisi tugevdada turvalisust ilma kliendi kogemust rikkumata. Biomeetrilised kaardid on ka seotud mitmete riiklike ID struktuuridega ja seega pangad kasutavad ära seda infrastruktuuri.
c. Finantsasutuse erinevate süsteemide parem omavaheline integreerimine, kui kasutatakse ühte püsivat kliendi tuvastamise tunnust. Biomeetriliste tehnoloogiate kasutamine seob lähemalt pettuste avastamise, pettuste haldamise ja riskipõhise autentimise lahendused.[115]

Turvaliste panga rakendusliidete olemasolu võimaldab ka kolmandatel isikutel integreerida panga teenuseid oma seadmetesse ja teenustesse. Ennustatakse, et häältuvastamist kasutavate targa kodu seadmete levimine, nagu Amazon Echo, Google Home ja Apple Homepod, viib

[113] Goode.

[114] P. Collinnson. NatWest trials fingerprint debit cards to remove £30 limit. – The Guardian 11.03.2019. Kättesaadav arvutivõrgus: https://www.theguardian.com/money/2019/mar/11/natwest-trials-fingerprint-debit-cards-to-remove-30-limit.

[115] Goode.

vestlusega panga teenuste kasutamiseni kodustes seadmetes.[116] Sektoripõhised regulatsioonid on juba ammu soovitanud biomeetrilisi tuvastussüsteeme oma juhendites.[117]

2018. alguses jõustus uus makseteenuste direktiiv (EL) 2015/2366 (edaspidi PSD2),[118] mille ühe suurema innovatsioonina finantssektorile nähti ette tugeva turvalise autentimise kohustus.[119] Tugeva turvalise autentimise kohustus ise jõustub direktiivist eraldi 2019. septembris Euroopa Komisjoni delegeeritud määruse (EL) 2018/389[120] (edaspidi tugeva turvalise autentimise rakendusakt) jõustumisega. PSD2 artikkel 4 p 30 kohaselt tugev turvaline autentimine tähendab: „autentimine, mille käigus kasutatakse kahte või enamat elementi, mis kuuluvad teadmise (miski, mida teab üksnes kasutaja), omamise (miski, mida omab üksnes kasutaja) või tunnuse (miski, mis on kasutajale omane) kategooriasse ja on sõltumatud, et neist ühe rikkumine ei ohustaks teiste usaldusväärsust, ning mille ülesehitus võimaldab kaitsta autentimisandmete konfidentsiaalsust.“ Tunnuse kategooria ehk miski, mis on kasutajale omane viitab siin biomeetrilisitele andmetele.[121] Samas ei ütle miski, et tunnuse kategooriaga on mõeldud ainult biomeetrilisi andmeid, sest tugev turvaline autentimine peab olema tehnoloogia ja ärimudeli neutraalne.[122] Enamus interneti või elektroonilisi makseid hakkab nõudma sellist mitmefaasilist autentimist. Rakendusaktiga on ette on nähtud erandid nagu viipemaksed kuni 50 eurot, parkimisega seotud tasud, väikemaksed kuni 30 eurot jne.[123] Määruse ja PSD2 vahel tekib konflikt, sest PSD2 kohustab finantssektori vastutavaid töötlejaid kasutama klientide autentimiseks eriliigilisi biomeetrilisi andmeid. Eriliigiliste isikuandmete töötlemiseks ei näe Määrus aga ette õigusliku alusena vastutava töötleja õigustatud huvi või üldist juriidilist kohustust, mis on õiguslikud alused tavaliste isikuandmete töötlemisel.

[116] *Ibid.*
[117] European Banking Authority. Final Guidelines on the security of internet payments. EBA/GL/2014/12_Rev1, 19.12.2014, lk 11. Kättesaadav arvutivõrgus: https://eba.europa.eu/documents/10180/934179/EBA-GL-2014-12+%28Guidelines+on+the+security+of+internet+payments%29_Rev1.
[118] Euroopa Parlamendi ja nõukogu direktiiv (EL) 2015/2366, 25. november 2015, makseteenuste kohta siseturul, direktiivide 2002/65/EÜ, 2009/110/EÜ ning 2013/36/EL ja määruse (EL) nr 1093/2010 muutmise ning direktiivi 2007/64/EÜ kehtetuks tunnistamise kohta (EMPs kohaldatav tekst). – ELT L 337. 23.12.2015. Kättesaadav arvutivõrgus: https://eur-lex.europa.eu/legal-content/ET/ALL/?uri=CELEX%3A32015L2366.
[119] PSD2 art 97 lg 1.
[120] Komisjoni delegeeritud määrus (EL) 2018/389 27. november 2017, millega täiendatakse Euroopa Parlamendi ja nõukogu direktiivi (EL) 2015/2366 regulatiivsete tehniliste standarditega, mis käsitlevad kliendi tugevat autentimist ning ühiseid ja turvalisi teabevahetuse avatud standardeid (EMPs kohaldatav tekst). – ELT L 69, 13.3.2018. Kättesaadav arvutivõrgus: https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX:32018R0389. Edaspidi turvalise autentimise rakendusakt.
[121] Turvalise autentimise rakendusakt preambul p 6.
[122] PSD2 art 98 lg 2 p d.
[123] Turvalise autentimise rakendusakt art 11 – 16.

Eriliigiliste isikuandmete töötlemisel on juriidiline kohustus õiguslik alus ainult tööõiguse, sotsiaalkaitse ja tervishoiu valdkonnas, aga mitte makseteenuste puhul.

Seetõttu tuleb lähemalt vaadata PSD2 ja Määruse kooskõla, et leida sobiv õiguslik alus biomeetriliseks tuvastamiseks. Isikuandmete kaitse on Euroopas põhiõigus *sui generis*[124] ja ka PSD2 preambul ütleb, et makseteenuse osutamisel direktiivi raames kohaldatakse isikuandmete töötlemisele Direktiivi 95/46/EÜ, sh tuleb õiguslik alus leida Direktiivist 95/46/EÜ.[125] Samuti on PSD2 preambuli p 94 märgitud, et iga autentimise elemendi puhul peaks süstemaatiliselt hindama ja võtma arvesse privaatsuse mõõdet, et teha kindlaks riskid ning õiguskaitsevahendid, mille võiks kehtestada andmekaitsega seotud ohtude minimeerimiseks. Siit võib järeldada, et biomeetriliste andmete kasutamisel tuvastamiseks peab vastutav töötleja koostama Määruse järgi andmekaitse mõjuhinnangu.[126] Seega võrreldakse järgnevalt sobivaid õiguslikke aluseid Määrusest kui Direktiiv 95/46/EÜ ülevõtjast ja PSD2-st.

PSD2 art 94 lg 2 sätestab õigusliku aluse kontekstis järgmist: „Makseteenuste pakkujatel on juurdepääs üksnes sellistele isikuandmetele ning nad töötlevad ja säilitavad üksnes selliseid isikuandmeid, mis on neile vajalikud makseteenuste osutamiseks ning üksnes siis, kui makseteenuse kasutajad on andnud sõnaselge nõusoleku.“ Antud artikkel viitab õiguslike alustena nii lepingu täitmiseks töötlemisele kui selgesõnalisele nõusolekule. Jääb lahtiseks, kas tegemist ongi topelt nõudega. Uurides kuidas suhestub PSD2 artikkel 94 Määrusega tuleneb, et Määruse järgi on biomeetriliste andmete kasutamisel tuvastamiseks vaja sõnaselget nõusolekut. Lepingu täitmiseks töötlemine ei ole eriliigiliste biomeetriliste andmete töötlemiseks lubatav alus Määruses. Tekib küsimus, kas selgesõnaline nõusolek on sama Määruses ja PSD2-es. Määrus on PSD2 suhtes *lex generalis* ja PSD2-s on läbivalt viidatud kohustusele olla kooskõlas Määruse eelkäijaga Direktiiviga 95/46/EÜ.[127] Seetõttu on käesoleva magistritöö autor arvamusel, et biomeetrilisele tuvastamisele kohalduvad PSD2 järgi samad nõusoleku kriteeriumid, mis Määruseski.

Nii PSD2 kui Määrus näevad õigusliku alusena ette nõusoleku. Seega tuleb hinnata nõusoleku vabatahtlikkuse kriteeriumit, kui makseteenuse osutajatel on iseenesest kohustus pakkuda tugevat turvalist autentimist ja sellele ei ole alternatiive. Samal ajal PSD2 näeb ette vastutava

[124] Harta art 8 lg 1.
[125] PSD2 preambul p 89.
[126] Määrus art 35 lg 1.
[127] PSD art 94 lg 1; preambul p 89.

töötleja kohustust kasutada vähemalt kahe elemendi kombinatsiooni kolmest. Seega on vastutaval töötlejal võimalus pakkuda tugeva turvalise autentimise elementide vahel andmesubjektile alternatiive. Samuti on tugev turvaline autentimine tehnoloogiliselt neutraalne, mistõttu on vastutaval töötlejal võimalus pakkuda alternatiive ka tehnoloogiate lõikes. Tehnoloogia arengu tõttu ei ole hetkel veel teada, kas element „miski, mis on kasutajale omane“ peab tähendama just biomeetrilisi andmeid. Seega on autor arvamusel, et PSD2 nõuete järgimiseks on vastutavale töötlejale jäetud piisavalt ruumi saada andmesubjektilt vabatahtlik selgesõnaline nõusolek.

Üles jääb veel küsimus, milline õiguslik alus valida, kui tugev turvaline autentimine ei ole kohustuslik, nagu väikemaksete ja muude väikese riskiga tehingute puhul. Sellisel juhul tuleb vastutaval töötlejal lähtuda ainult Määrusest. Teisisõnu, kui vastutava töötleja eesmärk on lihtsalt pakkuda kliendile biomeetrilise tehnoloogia teenust kasutaja mugavuse ja teenuse kiiruse tõttu, siis on tal vaja küsida selgesõnalist nõusolekut Määruse artikkel 9 lg 2 p a järgi.

Finantssektoris on füüsiliste isikute biomeetriline tuvastamine saanud tavaliseks nähtuseks. Käesolevas peatükis leiti, et õiguslik alus selleks võib tuleneda nii PSD2-st kui Määrusest sõltuvalt makseteenuse liigist ja autentimise turvalisuse standarditest. Nii PSD2 kui Määruse järgi on aga vaja saada andmesubjekti selgesõnaline nõusolek, mis peab vastama Määruse selgesõnalise nõusoleku kriteeriumitele.

2.2.2. Töökohas biomeetriline tuvastamine

Valdavalt eelistatakse tööandja territooriumile pääsemiseks, sellel liikumiseks ja ka oma tööjaama sisselogimiseks erinevaid kiipkaarte, koode ja paroole. Teisest küljest on ka kontoriruume, kuhu pääseb sõrmejälje[128] või töötaja kiipkaardile laetud muu biomeetrilise tunnuse abil.[129] Määrus annab töökohas biomeetriliseks tuvastamiseks artiklist 9 võimalike alustena selgesõnalise nõusoleku ja töötlemise vajalikkuse seoses vastutava töötleja tööõigusest tulenevate kohustuste ja eriõigustega.[130]

Kuna tegemist on eriliigiliste isikuandmetega, siis ei saa tööandja neid töödelda töölepingu täitmiseks. Üldnormi, mis lubaks töödelda töötaja biomeetrilisi andmeid, ei ole. Erinormid on

[128] Selline lahendus on näiteks Tartus asuvas IT-ettevõttes Fortumo.
[129] Artikkel 29 Töörühm. Opinion 3/2012 on developments in biometric technologies, lk 12.
[130] Määrus art 9 lg 2 p b.

seotud konkreetsete ametitega, näiteks politseinikud.[131] 2011. aastal avaldas Andmekaitse Inspektsioon oma seisukoha biomeetriliste andmete töötlemisest töökohal. „Biomeetrilisi andmeid töötlevate seadmete kasutamise lubatavus tööandjate poolt sõltub sellest, millise tehnoloogiaga biomeetrilisi andmeid töötlevat süsteemi kasutatakse. Biomeetrilisi andmeid töötlevad süsteemid võib liigitada järgmiselt: 1) süsteemid, mis salvestavad biomeetrilise jäljendi (näiteks silmaiirisekujutise); 2) süsteemid, mis loovad biomeetrilise jäljendi alusel koodi, jäljendit ennast ei salvestata.[132]

Andmekaitse Inspektsioon oli arvamusel, et biomeetrilist jäljendit salvestav süsteem töötleb selgelt biomeetrilisi ehk delikaatseid isikuandmeid ning selliseks töötlemiseks ei saa alus olla tööleping. Samas arvas Andmekaitse Inspektsioon, et biomeetrilise jäljendi alusel loodud koodid ei ole delikaatsed isikuandmed. Samuti kuivõrd seadusest ei tulene tööandjale õigustust töödelda töötaja isikuandmeid territooriumile, ruumidesse või infosüsteemidesse pääsemise õiguse kontrollimiseks, saab selline isikuandmete töötlemine tulla kõne alla töötaja nõusolekul või lepingu täitmise eesmärgil, näiteks kui töölepingus viidatakse juurdepääsu eeskirjadele.[133] Juhend oli koostatud enne Määruse vastu võtmist ja vastavalt sel ajal kehtinud IKSile. Vana IKS nimetas biomeetrilisi andmeid küll delikaatsete isikuandmete nimekirjas, kuid ei defineerinud biomeetrilisi andmeid. Samuti on Andmekaitse Inspektsiooni kodulehel üleval märge, et juhendid on täiendamisel tulenevalt Määrusest. Teisest küljest tugineb Andmekaitse Inspektsioon meedias endiselt oma vanale seiskohale, et biomeetrilistest andmetest loodud koodid ei ole eriliigilised isikuandmed.[134] Vaadates juhendit Määruse artiklite 4 p 14 ja 9 lg 1 järgi, ei saa autor aga nõustuda nende seisukohtadega.

Esiteks seab juhend biomeetriliste andmete kasutamise lubatavuse sõltuvusse tehnoloogiast. Määruse üks aluspõhimõtteid on aga tehnoloogiline neutraalsus ja füüsiliste isikute kaitse ei tohiks sõltuda kasutatavatest meetoditest.[135] Teiseks jääb juhendist ebaselgeks, mida on

---

[131] Politseiametniku daktüloskopeerimise ja DNA-proovi võtmise ning daktüloskopeerimisel saadud andmete ja DNA-proovide edastamise kord. - RT I, 07.06.2013, 13. § 1 lg 2.

[132] Andmekaitse Inspektsioon. Isikuandmete töötlemine töösuhtes. Abistav juhendmaterjal. Tallinn 2011, muudetud 23.05.2014. Lk 54. Kättesaadav arvutivõrgus: https://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/Isikuandmed%20t%C3%B6%C3%B6suhetes%20juhendmaterjal26%2005%202014_1.pdf. Edaspidi Andmekaitse Inspektsioon. Isikuandmete töötlemine töösuhtes.

[133] Andmekaitse Inspektsioon. Isikuandmete töötlemine töösuhtes, lk 54.

[134] Lugeja küsib: kas tööandja tohib mult sõrmejälgi võtta? – Postimees. 04.07.2018. Kättesaadav arvutivõrgus: https://tarbija24.postimees.ee/4518093/lugeja-kusib-kas-tooandja-tohib-mult-sormejalgi-votta.

[135] Määrus, preambul p 15.

mõeldud biomeetrilise jäljendi ja jäljendi alusel loodud koodiga. Juhend toob jäljendi näitena silmaiirisekujutise, kuid kujutised biomeetrilistest tunnustest ei ole biomeetrilised jäljendid. Nagu esimeses osas analüüsitud on Määruse definitsiooni kohaselt biomeetrilised andmed saadud konkreetse tehnilise töötlemise abil, kuhu alla ei käi tavalised fotod. Biomeetriline jäljend on kujutisest loodud teatud tunnuste, näiteks teatud näo mõõtmete, digitaalne esitlus. Seega jääb mulje, et juhendis on segamini aetud biomeetrilise tunnuse toored andmed, biomeetriline jäljend ja jäljendist loodud kood ning koodi all on mõeldud hoopis biomeetrilist jäljendit. Magistritöö esimeses osas leiti, et biomeetriline jäljend on Määruse mõistes biomeetrilised andmed ja biomeetrilise jäljendi kasutamine isiku kordumatuks tuvastamiseks on eriliigiliste isikuandmete töötlemine. Teisest küljest on arusaadav Andmekaitse Inspektsiooni kunagine seisukoht, sest varasemalt ei peetud biomeetrilisi andmeid ka isikuandmeteks, kui tuvastamiseks kasutati biomeetrilist jäljendit. Algselt arvati, et biomeetrilisi jäljendeid ehk koode ei saa nö tagasi pöörata, et isikut tuvastada.[136] Aja jooksul tehnoloogia arenes ja andmekaitse reformi ajaks oli tõestatud et biomeetrilisi jäljendeid saab kas või pooleldi viia kokku andmesubjektiga.[137]

Eriliigiliste biomeetriliste isikuandmete töötlemiseks saab vastutav töötleja ühe võimalusena võtta aluseks andmesubjekti selgesõnalise nõusoleku. Euroopas on aga konsensus, et tööandja vastutava töötlejana ei tohiks tugineda töötaja nõusolekule tema isikuandmete töötlemisel kui vaid erandjuhtudel.[138] Töösuhtes on võimu ebavõrdsus ja tuleb eeldada, et töötaja ei ole andnud nõusolekut vabatahtlikult.[139] Konkreetsemalt biomeetriliste andmete kontekstis on näiteks Prantsusmaa CNIL seisukohal, et biomeetriliste tuvastustehnoloogiate kasutus töökohas saaks toimuda vaid väga erandjuhtudel. Euroopas ainsana on Prantsusmaal ka võetud eraldi määrus töökohas biomeetrilise tuvastustehnoloogia kasutamiseks, mis reguleerib nii tehnoloogia standardeid kui proportsionaalsust.[140] Ka enne Määrust Poola andmekaitse järelevalveasutuse eelkäija Generalnego Inspektora Ochrony Danych Osobowych (edaspidi GIODO) oli seisukohal, et Määruse jõustudes on siseriiklikult vaja sätestada detailsed reeglid töötaja

[136] Artikkel 29 Töörühm. Working Document on biometrics, lk 5.
[137] Kindt 2013, lk 98.
[138] Määrus, preambul p 155; Kindt 2012, lk 335; Artikkel 29 Töörühm. Guidelines on consent under Regulation 2016/679. Lk 7.
[139] Artikkel 29 Töörühm. Guidelines on consent under Regulation 2016/679. Lk 7.
[140] CNIL. Délibération n° 2019-001 du 10 janvier 2019 portant règlement type relatif à la mise en oeuvre de dispositifs ayant pour finalité le contrôle d'accès par authentification biométrique aux locaux, aux appareils et aux applications informatiques sur les lieux de travail. 10.01.2019, art 5. Kättesaadav arvutivõrgus: https://www.cnil.fr/sites/default/files/atoms/files/deliberation-2019-001-10-01-2019-reglement-type-controle-dacces-biometrique.pdf

nõusolekule biomeetriliste andmete töötlemiseks tööandja poolt.[141] Tööandjal on biomeetriliseks tuvastustehnoloogiaks igal juhul vaja läbi viia andmekaitse mõjuhinnang, mis koosneb proportsionaalsuse testist.[142] Tööandja saaks töötaja nõusolekule tugineda vaid siis kui biomeetrilise tuvastussüsteemi kasutamiseks on väga mõjuv põhjus ja ta suudab tõestada, et vähem invasiivsed turvameetmed ei sobi.[143] Illustreerimaks mõjuvat põhjust on õiguskirjanduses toodud näitena tuumajaama piiratud alasid ja ohtlike viirustega laboreid.[144] Andmete asjakohasuse põhimõttest lähtuvalt peab põhjendama tuvastamiseks kasutatavat biomeetrilise tunnuse valikut ning kindlasti ei tohiks näha ette valimatult kõikide töötajate sisestamist biomeetrilisse süsteemi, vaid ainult neid, kelle tööiseloomust see vajalik on. Valitud biomeetriline tunnus ei tohi kedagi kollektiivist ka diskrimineerida. Sealjuures tuleb töötajale anda reaalne alternatiiv biomeetrilisele tuvastamisele, et nõusolek oleks vabatahtlik. Tööandja perspektiivist on see keeruline, sest paigaldada tuleks mitu võrdväärset turvasüsteemi, et töötajal oleks reaalne valik. Esiteks on keeruline leida kaks väga kõrge turvalisuse tasemega võrdväärset süsteemi ja teiseks on see ka väga kulukas.

Teise võimaliku alusena näeb Määruse artikkel 9 lg 2 p b ette vajalikkust seoses vastutava töötleja tööõigusest tulenevate kohustuste ja eriõigustega niivõrd, kuivõrd see on lubatud liidu või liikmesriigi õigusega. Eesti õiguses ei ole üldnormi, mis lubaks tööandjal kasutada biomeetrilisi andmeid töötajate tuvastamiseks. Küll aga näeb töösuhte kontekstis Määruse artikkel 88 ette võimaluse liikmesriikidele sätestada täpsemad eeskirjad tööandja või kliendi vara kaitseks.[145] Sellise normi olemasolu Eesti õiguses võimaldaks tööandjatel töökoha turvameetmena kasutada biomeetrilisi tuvastustehnoloogiaid ka ilma andmesubjekti nõusolekuta. Käesoleval aastal jõustunud isikuandmete kaitse seaduse rakendamise seadus[146] (edaspidi IKS RakS) ei toonud Eesti õigusesse juurde erasektori tööandjatele üldist alusnormi, millele toetuda biomeetriliste tuvastussüsteemide paigaldamiseks töökohta. IKS RakS seletuskirja järgi seadus käsitleb avaliku võimu poolset isikuandmete töötlemist ehk tema

[141] A. Kobylansk, M. Lewoszewski. Poland: A Brief Overview concerning the Implementation of the GDPR. - European Data Protection Law Review 2017, Vol 3, No 4, lk 510. Edaspidi A. Kobylansk, M. Lewoszewski.
[142] Määrus preambul p 90, 35 lg 3 p b ja art 35 lg 7.
[143] CNIL. Délibération n° 2019-001 du 10 janvier 2019 portant règlement type relatif à la mise en oeuvre de dispositifs ayant pour finalité le contrôle d'accès par authentification biométrique aux locaux, aux appareils et aux applications informatiques sur les lieux de travail. 10.01.2019, art 5. Kättesaadav arvutivõrgus: https://www.cnil.fr/sites/default/files/atoms/files/deliberation-2019-001-10-01-2019-reglement-type-controle-dacces-biometrique.pdf; A. Kobylansk, M. Lewoszewski, lk 510; Artikkel 29 Töörühm. Opinion 3/2012 on developments in biometric technologies, lk 11.
[144] Kindt 2012, lk 315; Artikkel 29 Töörühm. Opinion 3/2012 on developments in biometric technologies, lk 13.
[145] Määrus art 88 lg 1.
[146] Isikuandmete kaitse seaduse rakendamise seadus. - RT I, 13.03.2019, 2.

sekkumisvolitusi ja seaduse eelnõu puudutab eelkõige seda, kuidas avalik võim töötleb isikuandmeid.[147] Kehtivasse isikuandmete kaitse seadusesse[148] (edaspidi kehtiv IKS) on lisatud küll õigus töödelda isikuandmeid isikute ja vara kaitseks nii avalikus kui erasektoris, kuid sellest õigusest on välistatud eriliigilised isikuandmed.[149]

Alternatiivina on huvitav Artikkel 29 Töörühma varasem seisukoht, et isiku gruppi kuuluvuse tuvastamine ei ole biomeetriline jäljend.[150] Autor on sellise seisukohaga nõus, sest Määruse järgi on eriliigilised biomeetrilised andmed vaid sellised, mis suudavad füüsilist isikut teistest eristada. Kui kasutatav turvasüsteem tuvastab ainult, et töötaja kuulub 40-pealisse kollektiivi, siis ei saa seda lugeda Määruse mõistes füüsilise isiku kordumatuks tuvastamiseks. Seega võiks tööandja kaaluda sellist tehnoloogiat, kus inimese füüsiliste või käitumuslike tunnuste abil tuvastatakse ainult grupikuuluvus. Sellisel juhul saaks tööandja võtta isikuandmete töötlemise aluseks töölepingu Määruse artikkel 6 lg 1 p b järgi.

Eelnevast tulenevalt on autor seisukohal, et Andmekaitse Inspektsiooni juhis töökohas biomeetriliste andmete töötlemisele ei ole enam ammu asjakohane. Erasektori tööandjad, kes Eestis praegu kasutavad biomeetrilisi tuvastussüsteeme, teevad seda tõenäoliselt ilma kehtiva õigusliku aluseta, kui nad just ei ole võtnud aluseks töötaja selgesõnalist nõusolekut. Hetkel saaks tööandja töötaja biomeetrilisel tuvastamisel tugineda vaid töötaja selgesõnalisele nõusolekule, mida on aga äärmiselt keeruline põhjendada ja praktikas ellu viia.

2.3. Selgesõnaline nõusolek biomeetrilise tuvastamise alusena

Käesolevas peatükis leitakse millised on Määruse artikkel 9 lg 2 p a selgesõnalise nõusoleku tingimused eriliigiliste biomeetriliste andmete töötlemiseks. Esiteks selgitatakse vahet tavalisel ja selgesõnalisel nõusolekul ja seejärel tuvastatakse kriteeriumid, millele vastutav töötleja peab vastama, et saada andmesubjektilt kehtiv selgesõnaline nõusolek.

[147] Seletuskiri isikuandmete kaitse seaduse rakendamise seaduse eelnõu juurde 778 SE. Justiitsministeerium 13.12.2018, lk 1. Edaspidi: Seletuskiri isikuandmete kaitse seaduse rakendamise seaduse eelnõu juurde.
[148] Isikuandmete kaitse seadus. - RT I, 04.01.2019, 11.
[149] IKS § 10 lg 2.
[150] Artikkel 29 Töörühm. Opinion 3/2012 on developments in biometric technologies, lk 33.

2.3.1. Selgesõnalise nõusoleku erinevus tavalisest nõusolekust

Määruse kohaselt saab isikuandmete töötlemisel andmesubjekti nõusolekule tugineda üksnes siis, kui see on võetud kõiki Määruse nõudeid järgides. Kui isikuandmete töötlemine põhineb nõusolekul, mille suhtes pole kõiki Määruse nõuded järgitud, pole sellise nõusoleku alusel isikuandmete töötlemine kehtiv. Seega on äärmiselt oluline selgitada, millised tingimused Määrus nõusolekule seab ning kuidas praktikas neid nõudeid täita. Andmesubjekti nõusolek on vabatahtlik, konkreetne, teadlik ja ühemõtteline tahteavaldus, millega andmesubjekt kas avalduse vormis või selge nõusolekut väljendava tegevusega nõustub tema kohta käivate isikuandmete töötlemisega. Vabatahtlikkus, konkreetsus, teadlikkus ja ühemõtteline tahteavaldus pole Euroopa Liidu tasandil isikuandmete kaitses uued kriteeriumid, mistõttu saab nende tingimuste tõlgendamisel arvesse võtta ka varasemaid arvamusi, mis põhinesid Direktiivil 95/46/EÜ.

Selgesõnalist nõusolekut on vaja teatud olukordades, kus kohane oleks isiku suurem kontroll isikuandmete üle. Selgesõnalist nõusolekut küsitakse nii Määruse artiklis 9 lg 2 eriliigiliste isikuandmete töötlemiseks kui artiklis 22 lg 2 profiilianalüüsi ja automatiseeritud otsuste puhul. Määrus näeb ette, et „avalduse vormis või selge nõusolekut väljendava tegevusega“ tehtud tahteavaldus on eeldus tavaliseks nõusolekuks.[151] Tavalise nõusoleku nõuded on tehtud rangemaks kui oli Direktiivis 95/46/EÜ. Seega on vaja selgitada, mis lisanõuded on selgesõnalise nõusoleku saamisele tulnud Määrusega. Termin selgesõnaline viitab viisile, kuidas andmesubjekt oma nõusolekut väljendab. See tähendab, et andmesubjekt peab tegema selge nõusoleku avalduse. Artikkel 29 Töörühm on arvamusel, et selline nõusolek peaks olema kirjalik ja kui võimalik, siis ka allkirjastatud andmesubjekti poolt.[152] Samal ajal ei ole Määruses mingit kirjaliku selgesõnalise nõusoleku nõuet. Näiteks loetakse selgesõnaliseks nõusolekuks ka digitaalruumis andmesubjekti poolt täidetud elektroonilist vormi, e-kirja saatmist, skänneritud dokumendi üles laadimist või elektroonilist allkirja.[153] Selgesõnaline nõusolek võib olla antud ka suuliselt, näiteks kui see salvestatakse. Oluline on, et kehtiva nõusoleku andmine on tõendatav. Artikkel 29 Töörühm on arvamusel, et selgesõnalise nõusoleku võib anda ka veebilehte külastades kui külastaja klikib „jah“ või „ei“ isikuandmete töötlemisele, kui talle on selgelt antud infot, et sellega nõustub ta oma isikuandmete töötlemisega.[154]

[151] Määrus art 4 p 11.
[152] Artikkel 29 Töörühm. Guidelines on consent under Regulation 2016/679. Lk 18.
[153] Artikkel 29 Töörühm. Guidelines on consent under Regulation 2016/679. Lk 18.
[154] Artikkel 29 Töörühm. Guidelines on consent under Regulation 2016/679. Lk 19.

Järgnevalt leitakse, kuidas vastavad Määruse selgesõnalise nõusoleku tingimused biomeetriliste tuvastustehnoloogiate kasutamisele ja täpsemalt milline on konkreetne teave, millega andmesubjekt peab nõustuma enne, kui talle saab pakkuda biomeetrilist tuvastusteenust.

2.3.2. Tingimused selgesõnalisele nõusolekule

Biomeetriliste tuvastustehnoloogiate kasutusviisid tehinguteks, identiteedi tuvastamiseks või ligipääsu andmiseks on väga mitmekülgsed. Eelnevalt leiti, et mitmes olukorras peab vastutav töötleja saama eriliigiliste biomeetriliste andmete töötlemiseks andmesubjekti selgesõnalise nõusoleku. Lisaks finantssektorile ja töösuhetele, on andmesubjekti nõusolekut vaja üldiseks biomeetriliste tuvastusteenuste osutamiseks, nagu näotuvastamisel põhinev raamatulaenutus. Andmesubjekti nõusolek on vabatahtlik, konkreetne, teadlik ja ühemõtteline tahteavaldus. Järgnevalt analüüsitakse nõusoleku elemente biomeetriliste andmete kasutamiseks isiku tuvastamisel.

Esiteks peab nõusolek olema vabatahtlik ehk nõusolek peab olema vabalt tagasivõetav. Inimese biomeetrilisi tunnuseid ei saa üldiselt uuendada või kustutada, sest nad on püsivad. Siit tuleb probleem, mis saab siis kui tuvastamiseks kasutatav biomeetriline tunnus andmebaasist lekib või biomeetrilise informatsiooniga seade läheb kaduma. Kuidas saab inimene veel kasutada sama füüsilist tunnust turvaliseks identifitseerimiseks? PIN-kaartide ja paroolidega ei ole sellist probleemi, neid saab kergesti välja vahetada. Seega muutub biomeetrilises tuvastustehnoloogias eriti oluliseks andmete minimaalne seostatavus nende allikaga, et andmesubjekt saaks ka edaspidi sama tunnust kasutada biomeetrilistes tehnoloogiates. Oluline on ka, et biomeetrilised andmed sisaldaks võimalikult vähe teisi eriliigilisi isikuandmeid, mille töötlemiseks pole andmesubjekti nõusolekut saadud, sest vastasel juhul oleks tegemist liigse isikuandmete kogumisega. Originaalpilti biomeetrilisest tunnusest, nagu foto näost, või vahepealseid andmeid, mis tekivad pildist tuvastamiseks kasutatava tunnuse eemaldamisel, ei tohi säilitada. Seda on öelnud nii erinevad rahvusvahelised juhendid kui Euroopa andmekaitseinspektor.[155] Siin tuleb meenutada esimeses osas analüüsitud biomeetrilist

[155] International Working Group on Data Protection in Telecommunications, lk 8; Euroopa andmekaitseinspektor, Opinion of the European Data Protection Supervisor on a research project funded by the European Union under the Seventh Framework Programme (FP7) for Research and Technology Development - Turbine (TrUsted Revocable Biometric IdeNtitiEs, 01.02.2011, lk 7. Kättesaadav arvutivõrgus: https://edps.europa.eu/sites/edp/files/publication/11-02-01_fp7_en.pdf.

jäljendit, kui matemaatilist esitlust inimese füüsilisest või käitumuslikust tunnusest. Biomeetrilises tuvastustehnoloogias on vaja biomeetrilise tunnuse originaalkujutist ainult võrdlemise etapis leidmaks, kas andmete allikas vastab süsteemis salvestatud biomeetrilisele jäljendile. Seega allika kasutamise eesmärk on täidetud, kui võrdlus on läbi viidud.[156] Kui biomeetriline jäljend ei ole tehniliselt tagasivõetav, siis ei saa ka rääkida tagasivõetavast nõusolekust. Näiteks Soome tugevate elektrooniliste identifitseerijate seaduses nähti juba 2010. aastal ette vastutava töötleja kohustus kustutada biomeetriline jäljend või anda välja uus identifitseerimist võimaldav jäljend, kui identifitseerimist võimaldav seade on ohustatud või kadunud.[157] Seega oluliste omaduste hulka biomeetrilises süsteemis kuulub võimalus luua mitu iseseisvat biomeetrilist jäljendit samast allikast ja samal ajal ka võimalus võtta tagasi biomeetriline identiteet juhul kui varem välja antud identiteet on ohustatud või kadunud. Seda meetodit on mitu aastat uuritud ja paljud meetodid on ka väljatöötatud selliseks tagasivõetavaks biomeetriliseks identiteediks.[158] Üldiselt on aktsepteeritud arusaam, et biomeetrilisi tehnoloogiaid tuvastamise eesmärgil võib kasutada üksnes siis, kui ei kasutata originaalkujutist, näiteks pilti sõrmejäljest või näost, vaid kasutatakse biomeetrilise omaduse alusel loodud matemaatilist jäljendit. Teise nõudena on vaja, et tunnuseid oleks võimalik uuesti kasutada eri süsteemides. Isiku nõusolekuga neist kõrvale kalduda ei saa.

Teise vabatahtlikkuse määrajana tuuakse välja alternatiivide andmine. Artikkel 29 Töörühm rõhutab ka, et juhtudel kus töödeldakse biomeetrilisi andmeid ilma tugeva alternatiivita, nagu salasõna või viipekaart, siis ei saa lugeda nõusolekut vabatahtlikuks. Näiteks klubisse sissepääsuks biomeetrilise tuvastamise küsimisel peavad kliendid olema vabad otsustamaks, kas nad tahavad end sellesse süsteemi lisada. Valikut anda sõrmejälg või mitte kasutada teenust, ei saa lugeda kehtivaks nõusolekuks õigusliku alusena.[159] CNIL lubab biomeetrilisi süsteeme tuvastamiseks kasutada vaid siis, kui andmesubjektile pakutakse alternatiivseid tuvastamise vahendeid. See kehtib nii olukorras, kus biomeetrilist tuvastamist kasutatakse isiklikel ja kodustel eesmärkidel kui ka mitte kodustel eesmärkidel.[160] Näiteks mobiiltelefoni

[156] Määrus art 17 lg 1 p a.
[157] Act 617/2009 on Strong Electronic Identification and Electronic Signatures. Soome 01.09.2009, tõlgitud 19.04.2010, art 26, lg 3.
[158] Euroopa Komisjon. Joint Research Centre. Technical report series. Biometrics at the Frontiers: Assessing the Impact on Society. For the European Parliament Committee on Citizens' Freedoms and Rights. Justice and Home Affairs (LIBE) 2005, lk 97.
[159] Artikkel 29 Töörühm. Opinion 3/2012 on developments in biometric technologies, lk 11.

[160] CNIL. Biométrie dans les smartphones des particuliers : application du cadre de protection des données. 24.07.2018. Kättesaadav: https://www.cnil.fr/fr/biometrie-dans-les-smartphones-des-particuliers-application-du-

avamiseks kasutatav biomeetriline tehnoloogia võib klassifitseeruda isiklike ja koduste eesmärkide erandi alla vaid siis, kui muuhulgas on andmesubjektil võimalik avada telefon ka PIN koodiga. CNIL leidis ka ühes otsuses, et pangal on lubatud häältuvastamisega makseid teha, kui pank pakub kliendile alternatiivseid tehingu autoriseerimise võimalusi.[161] Seetõttu on CNIL ka üldreeglina keelanud töökohtades biomeetrilise tuvastamise ja lubanud seda vaid üksikutel juhtudel sõltumata asjaolust, kas töötajale pakutakse alternatiive, sest töösuhtes ei saa eeldada nõusoleku vabatahtlikkust eriliigiliste isikuandmete töötlemiseks.[162]

Nõusolek peab olema ka konkreetne. Konkreetsuse nõue käib käsikäes andmesubjektile antud informatsiooni täpsusega isikuandmete töötlemisest. Siin arvestatakse hindamisel keskmise andmesubjekti mõistlikke ootusi.[163] Samuti tuleb nõusoleku konkreetsuse juures arvestada, et nõusolek antakse vaid konkreetsete töötlemise eesmärkide jaoks. Inimesed peavad aru saama, millele nad nõusoleku annavad. Töötlemisest tulenevad tagajärjed peavad olema andmesubjekti jaoks ettenähtavad. Siin tõusetub probleemina biomeetriliste süsteemide ebatäpsus. Biomeetrilised süsteemid põhinevad tõenäosusel ja neid peetakse oma olemuselt paratamatult ebatäpseteks.[164] Tuvastamise ebaõnnestumistega seoses on mitmed biomeetriliste tehnoloogiate juhised toonud välja vajaduse tuvastada igal biomeetrilisel süsteemil veamäär ja tuvastamise tagasilükkamise määr ning neid on vaja üle vaadata regulaarselt.[165] E. Kindt on ka arvamusel, et andmesubjektile on vaja teada anda, mis on süsteemi vea määr.[166] Küll aga on Suurbritannia järelevalveasutus *Information Commissioner's Office* (edaspidi ICO) samas küsimuses oma 2011. aasta lahendis leidnud, et IBM ei pidanud avaldama andmesubjektidele detaile biomeetrilise tuvastustehnoloogia täpsusest, mh veamäära. Põhjuseks oli, et tegemist oli IBMI-i konfidentsiaalse teabega.[167]

---

cadre-de-protection-des-donnees. Edaspidi: CNIL. Biométrie dans les smartphones des particuliers : application du cadre de protection des données.

[161] CNIL. Biométrie dans les smartphones des particuliers : application du cadre de protection des données.

[162] CNIL. Le contrôle d'accès biométrique sur les lieux de travail. 28.03.2019. Kättesaadav arvutivõrgus: https://www.cnil.fr/fr/le-controle-dacces-biometrique-sur-les-lieux-de-travail

[163] Handbook on European Data Protection Law. Luxembourg: Publications Office of the European Union, 2014 lk 59.

[164]Pato, J. N. Millet, L. I. (koost). Biometric Recognition. Challenges and opportunities. Whither Biometrics Committee. Washington, D. C: The National Academies Press 2010. lk 3. https://dataprivacylab.org/TIP/2011sept/Biometric.pdf.

[165] Artikkel 29 Töörühm, Opinion 3/2012 on developments in biometric technologies. Lk 29.

[166] Kindt 2012, lk 340.

[167] Information Commisioner's Office. Freedom of Information Act 2000 (Section 50). Decision Notice 28.02.2011. Kättesaadav arvutivõrgus: https://ico.org.uk/media/action-weve-taken/decision-notices/2011/590086/fs_50320566.pdf.

Süsteemi täpsus ja kasutatavate andmete kvaliteet on ülimalt olulised. Teisest küljest biomeetrilised tunnused ajas muutuvad, näiteks inimene vananeb ja seetõttu muutub käe geomeetria ja nägu. Seega peab vastutav töötleja hoolitsema selle eest, et tuvastamiseks kasutatavad isikuandmed oleksid asjakohased. Andmesubjektidel on Määruse järgi õigus, et töödeldakse nende täpseid isikuandmeid.[168] Seda võib ka tõlgendada, et neil on õigus nõuda biomeetriliste süsteemide täpsust. Euroopa inimõiguste konventsiooni artikkel 8 proportsionaalsuse test hõlmab efektiivsuse ja piisavuse demonstreerimist, mistõttu peavad biomeetrilised süsteemid jõudma täpsuse astmeni, mil nad oleks efektiivsed ja piisavad. Kui biomeetrilised süsteemid ei tööta täpselt ja usaldusväärselt, siis on sellised süsteemid ebaefektiivsed ja ebaproportsionaalsed, kuna ei paku näiteks lubatud tuvastamise või tehingu usaldusväärsust. Andmete töötlus peab olema asjakohane eesmärgi suhtes ja kui tuvastussüsteemi täpsus on nii madal, et ei suuda efektiivselt inimesi tuvastada, siis ei ole see asjakohane eesmärgi täitmiseks.

Biomeetrilise tuvastussüsteemi täpsusega nõustumine on oluline andmesubjektile ka seetõttu, et süsteemi veamääraga kaasnevad andmesubjektile tagajärjed, millest ta peab olema teadlik nõusolekut andes. 2005. aastal Euroopa Komisjoni tellitud Paul de Hert raportis biomeetriliste tehnoloogiate kohta on öeldud, et tarbijaõigus peaks tegema selgeks, et igaüks, kellelt vabatahtlikult küsitakse biomeetrilist identifitseerijat, oleks põhjalikult informeeritud, pädev arusaamaks tegevuse mõjust ja nõustuma sellise tegevusega ilma ohuta saada kahjustada.[169] Biomeetriliste süsteemide ebatäpsus ja ligipääsu piiratus osadele inimestele viib riskini diskrimineerida teatud kasutajaid. Samal ajal biomeetrilised süsteemid teevad ka isiku kohta automaatseid otsuseid, mistõttu on vajalik andmesubjekti teavitada rakendatavast korrast, kui tuvastatakse süsteemi viga. Nii avalikus sektoris kui erasektoris peavad tuvastussüsteemi ebaõnnestumise vastumeetmed olema tasakaalus – nad ei või olla vähem turvalised isiku jaoks ja ka mitte stigmatiseerivad. Näiteks kui süsteemi kasutamise eesmärk on pakkuda suuremat turvalisust mingi teenuse kasutamisel, siis inimestel, kelle sõrmejälgi ei ole võimalik lugeda, tuleb tagada samal tasemel väärikus ja süsteemi turvalisus nagu kõigile teistele.[170] Isiku tuvastamise ebaõnnestumise protsess on vajalik nii tavaliste süsteemivigade puhuks kui ka juhtudeks, kus näiteks nägemispuudega inimesel on raskusi iirise mustri tuvastamisel või kui inimesel on vigastuse tõttu nägu sidemetes ja ta ei saa näotuvastust kasutada. Seega

[168] Määrus art 5 lg 1 p d.
[169] P. d. Hert, Biometrics: legal issues and implications. Background paper for the Institute of Prospective Technological Studies, DG JRC – Euroopa Komisjon, Sevilla, jaanuar 2005, lk 27.
[170] Euroopa Komisjon, Joint Research Centre. Biometrics at the Frontiers, lk 11.

ebaõnnestumised biomeetrilise süsteemi kasutamisel võivad esineda just haavatavamatel ühiskonna gruppidel tulenevalt haigusest, füüsilisest puudest, etnilisest vähemusest[171] või vanusest. Seega süsteem peab suutma tulla toime kiiresti ja efektiivselt valede tagasilükkamistega. Avalikus sektoris on see lahendatud inimeste sekkumisega näiteks piirikontrollis.[172] Artikkel 29 Töörühm ei erista avalikku ja erasektorit vaid ütleb: „igal juhul peavad olema kohaldatud täpsed ebaõnnestumise kaitsemeetmed, et tagada väärikus ja põhiõiguste kaitse igale isikule, kes ei ole võimeline süsteemi sisenemise protsessi läbima.“[173]

Seega andes teadlikku nõusolekut biomeetrilise tehnoloogia kasutamiseks eesmärgiga end tuvastada, peab andmesubjekt olema teadlik, kas tehnoloogia vastab ta ootustele. Andmesubjektide ootused biomeetrilise tunnuse abil tuvastamisele on eelkõige, et tehnoloogia ei rikuks nende õigust väärikusele, õigust mitte olla diskrimineeritud ja et süsteem oleks eesmärgi suhtes efektiivne ja tõhus.

2.4. Peatüki kokkuvõte

Inimese füüsiliste ja käitumuslike tunnuste abil tuvastamist saab praeguse tehnoloogia seisu ja ühiskonna arenguga digitaalruumis viia läbi nii inimest ennast kaasates kui ka ilma inimese otsese osaluseta. Biomeetrilised tunnused on vabalt püütavad erinevate sensoritega või laialt kättesaadavad internetist. Seetõttu täpsustati käesolevas osas millised on vastutava töötleja võimalused kasutada andmesubjekti poolt avalikustatud biomeetrilisi andmeid ja millal on vaja küsida andmesubjekti selgesõnalist nõusolekut biomeetriliste andmete edasiseks töötlemiseks. Teiseks uuriti millistele õiguslikele alustele saab vastutav töötleja tugineda, kui ta kasutab enda soovil eriliigilisi biomeetrilisi andmeid ja kasutatav tehnoloogia nõuab andmesubjekti aktiivset osalust, näiteks silma asetamine silmaiirise skanneri ette.

Andmesubjekti poolt avalikustatud biomeetriliste andmete kontekstis uuriti nii Eesti kui EIKi ja EK kohtupraktikat ja jõuti järeldusele, et andmesubjekti poolt avalikustatud isikuandmete edasine kasutamine on äärmiselt kitsalt piiritletud. Vastutav töötleja peab arvesse võtma töötlemise struktureerituse astet, konteksti muutust, töötlemise intensiivsust ja asjaolu, kui

[171] Artikkel 29 Töörühm. Opinion 3/2012 on developments in biometric technologies, lk 21.
172 Euroopa Parlamendi ja nõukogu määrus (EÜ) nr 444/2009, 28. mai 2009 , millega muudetakse nõukogu määrust (EÜ) nr 2252/2004 liikmesriikide väljastatud passide ja reisidokumentide turvaelementide ja biomeetria standardite kohta. – ELT L 142, 06.06.2009, art 1 lg 2 p a.
[173] Artikkel 29 Töörühm, Opinion 3/2012 on developments in biometric technologies, lk 15.

ettenähtav edasine töötlemine kavandataval viisil andmesubjektile oma isikuandmete avalikustamise hetkel oli. Teisisõnu kui sotsiaalmeediast või veebilehtedelt saadud isikuandmetest luuakse põhjalik struktureeritud andmebaas, siis ei või vastutav töötleja tugineda enam Määruse artiklile 9 lg 2 p e, vaid peab küsima andmesubjektilt selgesõnalist nõusolekut.

Teiseks uuriti õiguslikke aluseid eriliigiliste biomeetriliste andmete töötlemisel finantssektoris ja töökohas. Finantsteenuste valdkonnas kohustab PSD2 finantsasutusi kasutama enamus elektrooniliste maksete jaoks mitmefaasilist tuvastamist, millest üks etapp on biomeetriline tuvastamine. Käesolevas peatükis leiti, et nii PSD2 kui Määruse järgi peab vastutav töötleja õigusliku alusena saama andmesubjekti selgesõnalise nõusoleku, millele kohalduvad Määruse selgesõnalise nõusoleku kriteeriumid. Samuti kui ei ole juriidilist kohustus biomeetriliselt klienti tuvastada, näiteks väikemaksete jaoks, siis peab finantsasutus saama kliendilt jällegi selgesõnalise nõusoleku.

Töökohas eriliigiliste biomeetriliste andmete töötlemise puhul leidis autor, et tööandjal ei ole praktiliselt võimalik kasutada biomeetrilist tuvastamist töökohas, sest ainus alus selleks saaks olla töötaja selgesõnaline nõusolek. Töötaja selgesõnalise nõusoleku kehtivust eriliigiliste isikuandmete töötlemisel on aga ääretult keeruline tõendada ja selle tagamine on tööandjale praktikas kulukas. Hetkel ei ole Eesti õiguses alusnormi, mis lubaks tööandjal oma vara kaitseks või muudel põhjustel kasutada biomeetrilist tuvastustehnoloogiat oma tööõigusest tulenevate huvide kaiseks.

Viimaseks analüüsiti käesolevas peatükis selgesõnalise nõusoleku elemente biomeetriliste tehnoloogiate kontekstis. Andmesubjekti nõusolek on vabatahtlik, konkreetne, teadlik ja ühemõtteline tahteavaldus. Selleks, et eriliigiliste biomeetriliste andmete töötlemiseks antud nõusolek oleks vabatahtlik peab tuvastamiseks salvestama seadmes vaid biomeetrilise jäljendi, kasutatav tehnoloogia peab võimaldama ühest füüsilisest või käitumuslikust omadusest luua mitu erinevat biomeetrilist jäljendit ja biomeetrilisele tuvastustehnoloogiale tuleb anda alternatiive, mis oleks sama turvalised, näiteks PIN kood. Nõusolek on konkreetne ja teadlik, kui kasutatav biomeetrilise tuvastamise meetod vastab andmesubjekti ootustele, ehk andmesubjekti teavitatakse süsteemi veamäärast, süsteem on piisavalt täpne isiku tuvastamiseks ja tuvastamiseks valitud biomeetrilised tunnused ei diskrimineeri süsteemi kasutajat.

3. Õigusliku aluse muutumine biomeetriliste andmete töötlemisel

Käesolevas osas analüüsitakse õiguslikke aluseid biomeetriliste andmete töötlemisel olukordades, kus töötlemise eesmärk ei ole ainult isik tuvastada või isiku tuvastamine ei olegi eesmärk, vaid kaasnev mõju. Arvestades, et biomeetrilised andmed muutuvad eriliigilisteks isikuandmeteks vaid nende kasutuseesmärgist lähtuvalt, siis analüüsitakse erinevaid biomeetrilisi tehnoloogiaid, kus saab tõmmata piiri tavaliste ja eriliigiliste biomeetriliste andmete vahele.

Üha rohkem inimesi elab nö targas keskkonnas, mis koosneb meie igapäevastesse objektidesse sisestatud sensoritest, kuvaritest ja andmetöötluse elementidest. Sellised seadmed on omavahel ühendatud ja vahetavad kasutajatega infot, et pakkuda individuaalseid ja mugavaid teenuseid. Selliste keskkondade eesmärk on elukvaliteeti tõsta läbi andmetöötluse ja automatiseerimise. Näiteks kantavad liitreaalsuse seadmed (inglise k. *augmented reality*) annavad liikuvuse, nägemise ja kuulmise erivajadustega inimestele võimaluse oma elukvaliteeti parendada. Kõnetuvastustehnoloogia võimaldab reaalajas sõnu kuvada ja selliselt aitab kurte arusaamisel, mida nende vestluskaaslane ütleb. Aspergeri sündroomiga inimesi aitab aga reaalajas emotsioonide tuvastustehnoloogia ja pimedaid aitab igapäevaelus ruumi- ja näotuvastustehnoloogia.[174] Iga biomeetrilise tunnuse jaoks on potentsiaalselt sensor võimeline seda kaugusest koguma ja töötlema. Distantsilt töötavad biomeetrilised sensorid on suhteliselt uus tehnoloogia, kuid väga kiiresti arenev valdkond. Küll aga andmesubjektide teadmatus, milliseid tunnuseid distantsilt inimese kohta kogutakse võib olla väga häiriv.[175] Biomeetrilisi andmeid võidakse nähtamatult koguda nii koduses keskkonnas kui avalikus ruumis ja väga erinevatel eesmärkidel. Kaasnevaks probleemiks on andmesubjektide kontrolli kadu targa keskkonna andmetöötluses.[176]

Käesolevas magistritöö osas analüüsitakse esiteks biomeetriliste andmete töötlemist asjade internetis, nagu roboti kujul koduabiline, mis reageerib häälkäsklustele või enesemõõtmise seadmed (inglise k. *Quantified Self*), mis loovad detailseid mustreid andmesubjekti käitumisharjumustest ja füüsilistest omadustest. Sealjuures analüüsitakse ka seadmeid, mis

[174] A. Kotsios. Privacy in an Augmented Reality. *International Journal of Law and Information Technology*, 2015, 23, 157-185. lk 162.
[175] E. Sedenberg, jt. A window into the soul: Biosensing in public. Surveillance, Privacy and Public Space. 2018. lk 4.
[176] F. Pichierri, D. Dimitrova. Smart environments in the health context, self-management and data protection in the STARR project. - International Review of Law, Computers & Technology 2018, Vol 32:1. Edaspidi Pichierri, ja Dimitrova; Artikkel 29 Töörühm. Opinion 8/2014 on the on Recent Developments on the Internet of Things.

koguvad vähetähtsaid isikuandmeid, kuid koostoimes teiste andmetega, on võimalik andmesubjekt nende põhjal tuvastada. Vastust otsitakse küsimustele, kas need seadmed töötlevad eriliigilisi biomeetrilisi andmeid ja millisel õiguslikul alusel.

Teiseks uuritakse käitumuslike biomeetriliste andmete töötlemist *online* keskkonnas ja leitakse, millisel hetkel *online* käitumisel põhinev analüütika tööriist töötleb eriliigilisi biomeetrilisi andmeid. Kuna käitumuslike andmete analüüs on lähedalt seotud profiilianalüüsiga Määruse artikli 22 järgi, siis vastatakse ka küsimusele, mis on vahe profiilianalüüsil ja inimese käitumisel põhineval biomeetrilisel tuvastamisel.

Käesoleva osa viimases peatükis uuritakse, millised võimalused on liikmesriigil kehtestada Määruse kõrvale eriliigiliste biomeetriliste andmete töötlemise eriregulatsioon. IKS RakS tegi Määruse ülevõtmiseks muudatused mitmetesse seadustesse. Sellegipoolest ütleb IKS RakS seletuskiri, et IKS RakS avaldab praktikas mõju eelkõige avaliku sektori andmetöötlejatele.[177] Seetõttu leitakse magistritöö lõpetuseks, kas Eesti õiguses peaks tegema eriliigiliste biomeetriliste andmete töötlemisel eraõiguslikes suhetes õigusliku aluse valikule täpsustusi.

3.1. Õiguslik alus asjade internetis biomeetriliste andmete töötlemiseks

Käesolevas peatükis analüüsitakse olukordi, kus tarbeseadmed töötlevad muuhulgas biomeetrilisi andmeid ja biomeetriliste andmete töötlemise ainus eesmärk seadmetes ei ole füüsilise isiku kordumatu tuvastamine.

Asjade internet viitab infrastruktuurile, kus miljonid sensorid on ühendatud tavaliste igapäevaste esemetega ja need sensorid koguvad, töötlevad, säilitavad ja edastavad andmeid koostoimes teiste seadmetega. Asjade internet toetub andmete ulatusliku töötlemise põhimõttele, kus läbi sensorite vahetatakse andmeid märkamatult ja pidevalt.[178] Seetõttu jäetakse analüüsist välja seadmed, kus töödeldakse isikuandmeid lokaalselt ja need ei välju kunagi seadmest. Nende puhul pole tegemist asjade internetiga.

Kasutatavad sensorid suudavad reaalajas koguda erinevaid andmeid kasutaja igapäevaharjumuste-või keskkonna kohta. Artikkel 29 Töörühma on arvamusel, et

[177] Seletuskiri isikuandmete kaitse seaduse rakendamise seaduse eelnõu juurde, lk 130.
[178] Artikkel 29 Töörühm. Opinion 8/2014 on the on Recent Developments on the Internet of Things, lk 4.

isikuandmete analüüs koduses kontekstis asjade internetis tõenäoliselt paljastab detaile elanike elustiilist ja harjumustest või lihtsalt nende kodusoleku fakti.[179] Direktiivi 2002/58/EÜ (edaspidi e-privaatsuse direktiiv)[180] preambuli punkt 24 kohaselt „elektrooniliste sidevõrkude kasutajate lõppseadmed ja sellistes seadmetes säilitatav teave moodustavad osa kasutajate eraelust, mida tuleb kaitsta inimõiguste ja põhivabaduste kaitse Euroopa konventsiooni kohaselt.“ Seega on kodudes ja eraelu kontekstis kasutatava asjade interneti kogutud andmete puhul tegemist igal juhul isikuandmetega. Käesolevas töös huvi pakkuvad asjade interneti seadmed võib jagada kolmeks: kantavad seadmed (inglise k. *Wearable Computing)*, enesemõõtmise seadmed (inglise k. *Quantified Self*) ja koduseadmed, millel on otsene kasutajaliides kasutajaga. Seega jäävad analüüsist välja suuremad süsteemid nagu targad linnad ja tark transpordisüsteem.

Kantavate seadmete mõistega kirjeldatakse igapäevaelu esemeid, nagu kellad, prillid ja riietele kinnitatud seadmed, kuhu on lisatud sensorid nende esemete funktsionaalsuse laiendamiseks. Paljudel juhtudel on seadme üheks omaduseks pilti, videot või häält jäädvustav kaamera või mikrofon. Kantavate seadmetega sarnased on enesemõõtmise seadmed, mida kantakse sooviga salvestada andmeid oma elustiili ja harjumuste kohta, nagu unemustrite või aktiivsuse jälgimine. Sellised seadmed jälgivad andmesubjekti käitumises trende ja muutusi aja jooksul.[181] Loodavad andmekogud on piisavalt detailsed, et võimaldada andmesubjekti tuvastamist[182] ja seega kvalifitseeruvad vähemalt tavaliste biomeetriliste andmete alla. Kantavate seadmete ja nende riskide kohta on avaldanud juhise ka Eesti Andmekaitse Inspektsioon 2015. aastal.[183]

Asjade interneti seadmeid paigutatakse tihti kodudesse ja neid on võimalik kontrollida interneti vahendusel. Näiteks liikumisanduritega seadmed võivad tuvastada ja salvestada, kui keegi on kodus, millised on tema liikumise mustrid ja seejärel algatada eelnevalt määratud tegevusi, nagu ruumi temperatuuri muuta või valgusteid sisse lülitada. Enamik selliseid koduseid

[179] *Ibid* lk 6.
[180] Euroopa Parlamendi ja nõukogu direktiiv 2002/58/EÜ, 12. juuli 2002, milles käsitletakse isikuandmete töötlemist ja eraelu puutumatuse kaitset elektroonilise side sektoris (eraelu puutumatust ja elektroonilist sidet käsitlev direktiiv). – ELT L 201, 31.7.2002.
[181] *Ibid* lk 5.
[182] *Ibid* lk 8.
[183] Andmekaitse Inspektsioon. Kantavad seadmed ja privaatsus. Juhis organisatsioonidele ja kodukasutajale seaduse rakendamisel. 09.11.2015. Kättesaadav arvutivõrgus: https://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/Juhised/Juhis-kantavad%20seadmed%20ja%20privaatsus.pdf. Edaspidi Andmekaitse Inspektsioon. Kantavad seadmed ja privaatsus.

seadmeid on pidevalt ühendatud ja võivad saata andmeid tagasi tootjale. Näiteks on mitmed liikmesriikide andmekaitse järelevalveasutused avaldanud muret asjade internetiga seotud mänguasjade levimisega ja neis biomeetriliste andmete töötlemisega.[184] Sellised mängusjad võivad salvestada vestlusi lapsega või töötada tehisintellekti abil, mis tähendab veel keerukamat lapse andmete töötlemist ja temast profiili loomist.[185]

Eelnevast on selge, et tegemist on igal juhul Määruse järgi isikuandmetega, kui kogutakse andmeid inimeste isiklikest seadmetest ja seejuures ei ole oluline, mis andmetega täpselt tegu on. Tuvastamaks, millal asjade internetis töödeldakse Määruse mõistes biomeetrilisi andmeid, tuleb vaadata uuesti magistritöö esimeses osas analüüsitud biomeetriliste andmete definitsiooni. Esiteks töötlevad asjade interneti seadmed suurel hulgal erinevaid inimese füüsilisi, füsioloogilisi ja käitumuslikke omadusi, nagu hääl, pilt või liikumismustrid. Teiseks kriteeriumiks on, kas need kogutavad biomeetrilised tunnused võimaldavad füüsilist isikut kordumatult tuvastada. Nagu esimeses osas leitud on see mõiste kitsam tavalisest tuvastatavuse kriteeriumist ja samal ajal on see mõiste ka suhteline. Esimeses osas jõuti järeldusele, et süsteem tuvastab isikut kordumatult, kui see suudab füüsilist isikut iga kord piisava täpsusega eristada teistest isikutest tema biomeetriliste tunnuste põhjal. Sealjuures tuleb arvestada tehnoloogia mõjuga isikuandmete töötlemisele ehk tõenäosust, et selle abil oleks potentsiaalselt võimalik isik tuvastada tema biomeetriliste tunnuste abil. Hinnata tuleb, kui suur roll on biomeetrilistel tunnustel isiku tuvastamisele, kui inimese käitumuslike või füüsiliste omadustega liidetakse muud informatsiooni. Esiteks asjade interneti seadmetes töödeldakse andmeid enamasti ainult seadme kasutaja või väikese inimeste grupi kohta, mistõttu kogutavad biomeetrilised tunnused võimaldavad üpris suure tõenäosusega tuvastada konkreetset isikut.

Teiseks asjade internetis informatsiooni genereerimine vähetähtsatest või anonüümsetest andmetest tehakse kergeks laialdase sensorite kasutusega.[186] Esimeses osas leiti, et biomeetrilisi andmeid ei saa pea kunagi lugeda anonüümseteks nende tugeva seotuse tõttu indiviidiga. Seega tuleb uurida, kas vastutav töötleja saab näiteks tugineda argumentatsioonile, et seadmel on mitmeid kasutajaid ja kasutatud on anonümiseerimise meetodeid, mistõttu ei ole

[184] Saksamaa on näiteks võtnud turult ära häältuvastamisega seotud nukke ja arvamusi on avaldanud ka Iirimaa. Data Protection Commission. Advice on Connected Toys and Devices. 04.12.2018. https://www.dataprotection.ie/en/guidance-landing/data-protection-commission-advice-connected-toys-and-devices; Bundesnetzagentur. Bundesnetzagentur removes children's doll "Cayla" from the market. Press release 2017. Kättesaadav arvutivõrgus: https://www.bundesnetzagentur.de/SharedDocs/Pressemitteilungen/EN/2017/17022017_cayla.html.
[185] Data Protection Commission. Advice on Connected Toys and Devices. 04.12.2018.
[186] Artikkel 29 Töörühm. Opinion 8/2014 on the on Recent Developments on the Internet of Things, lk 8.

andmete kombineerimisel võimalik kedagi eristada. Nii Artikkel 29 Töörühm kui Euroopa andmekaitseinspektor on rõhutanud anonüümse isikuandmete töötlemise kadumist asjade interneti levikuga.[187] Euroopa andmekaitseinspektor on näiteks öelnud, et suurandmete töötlust peaks pidama isikuandmete töötluseks ka siis kui on kasutatud anonümiseerimise meetodeid, sest üha lihtsam on tuletada isiku identiteet kombineerides väidetavalt anonüümseid andmekogusid teiste andmehulkadega, sh avalikult kättesaadavate andmetega.[188] Nagu teises osas analüüsitud, on biomeetrilised tunnused valdavalt avalikult kättesaadavad. Seega peaks asjade internetist saadud andmeid lugema isikuandmeteks ka pärast anonümiseerimise meetodi rakendamist, sest uuesti identifitseerimise risk on lihtsalt nii kõrge.[189] Eelnevast tulenevalt peab vastutav töötleja eeldama, et igasugune biomeetriliste tunnuste kogumine või töötlemine asjade interneti vahendusel võimaldab inimese tuvastamist tema füüsiliste ja käitumuslike omaduste põhjal. Seega on täidetud Määruse artikkel 4 kriteerium, et töödeldavad inimese füüsilised ja käitumuslikud omadused peavad võimaldama kordumatut tuvastamist.

Kolmanda tingimusena peab biomeetrilisi tunnuseid töötlema konkreetsete tehniliste vahenditega. Töö esimeses osas leiti, et selle all mõeldakse tehnilist töötlemist, mis ei ole tavaline ja väiksemahuline. Oma olemuselt vastab asjade internet juba konkreetse tehnilise töötlemise kriteeriumile, sest andmeid töödeldakse suures ulatuses ja tehniliselt keerulises süsteemis. Esimeses osas leiti ka, et eelkõige tuleb silmas pidada andmebaaside loomist. Samuti töö teises osas leiti, et oluline on andmete struktureerituse aste. Autor on seega seisukohal, et konkreetse tehnilise töötlemise kriteerium on täidetud, kui kogutakse füüsilise isiku mistahes füüsilisi või käitumuslikke andmeid ning töötlemine on automaatne ja struktureeritud. Seda olenemata asjaolust, kas konkreetne seade biomeetriliste tunnuste põhjal võrdleb füüsilist isikut või loob kogutud isikuandmetest lihtsalt andmebaasi.

Kokkuvõtteks leiab autor, et igasugune inimese füüsiliste või käitumuslike tunnuste töötlemine asjade internetis vastab Määruse artikkel 4 biomeetriliste andmete definitsioonile.

[187] *Ibid* lk 8; Euroopa andmekaitseinspektor. Opinion 4/2015. Towards a new digital ethics. Data, dignity and technology. 11.09.2015, lk 13. Kättesaadav arvutivõrgus: https://edps.europa.eu/sites/edp/files/publication/15-09-11_data_ethics_en.pdf. Edaspidi EDPS. Opinion 4/2015. Towards a new digital ethics.
[188] EDPS. Opinion 4/2015. Towards a new digital ethics. Lk 6.
[189] Artikkel 29 Töörühm. Opinion 8/2014 on the on Recent Developments on the Internet of Things. Lk 11.

3.1.1. Eriliigilised biomeetrilised andmed asjade internetis

Magistritöö esimeses osas leiti, et biomeetriliste andmete klassifitseerimiseks eriliigilisteks isikuandmeteks Määruse artikkel 9 järgi tuleb vahet teha andmete omamisel ja kasutamisel. Eriliigilised on biomeetrilised andmed vaid siis, kui neid kasutatakse füüsilise isiku kordumatuks tuvastamiseks.[190] Esimeses osas leiti, et kui Määruse artikkel 4 tavaliste biomeetriliste andmete määratlus võib hõlmata laia valikut biomeetrilisi andmebaase, siis artikli 9 kohaldamiseks tuleks vastutaval töötlejal leida piir, kus andmebaaside loomise eesmärk ja kasutamise viis rikuvad oluliselt andmesubjekti eraelu puutumatust. Samuti leiti, et oluline on andmete hoidmise konkreetne kontekst. Sama oluline on ka, kui kergesti andmed oma kogumise viisilt võimaldavad tuvastamist ja kuidas kogumise viis on sobiv biomeetriliseks võrdlemiseks teiste juba olemasolevate biomeetriliste andmebaasidega.

Eelnevat seisukohta toetab senine EIKi praktika eriliigiliste isikuandmete määratlemisel. Esiteks lahendis *S. and Marper* võrdsustas EIK isiku eraelu puutumatuse riive struktureeritud sõrmejälgede andmebaasi ja DNA-proovide säilitamise puhul. Seejuures tähtsustas kohus võimalust võrrelda sõrmejälgi andmebaasis sisalduvate isikustatud ja isikustamata andmetega.[191] EIK ei ole oma praktikas teinud vahet biomeetriliste andmete liikidel, vaid on seisukohal, et sõrmejäljed ei erine teistest isikuandmetest, mis omavad väliseid identifitseerimise tunnuseid, nagu fotod või hääle näidised.[192] Teises lahendis *P.G. and J.H. v. the United Kingdom* analüüsis EIK hääle salvestuste kogumist ja hoidmist.[193] Kohus leidis, et püsivalt häälsalvestuse hoidmine edasiseks analüüsiks oli otseselt seotud isiku tuvastamisega, kui salvestust kombineerida muude isikuandmetega. Kohus oli seisukohal, et eraelu puutumatuse riivega on tegemist siis, kui häälsalvestusi töödeldakse edasi teiste isikuandmetega. Seejuures rõhutas kohus andmete hoidmise süstemaatilisust ja pikaajalisust.[194] EIK on biomeetriliste andmete puhul arvamusel, et nende oluline mõju isiku privaatsusele tuleneb asjaolust, et näiteks sõrmejälg sisaldab endas unikaalset informatsiooni konkreetse isiku kohta, mis lubab selle isiku identifitseerimist väga erinevates olukordades. Seetõttu on biomeetrilised andmed võimelised mõjutama inimese eraelu viisil, mida ei saa lugeda neutraalseks või vähetähtsaks.[195] Oluline mõju inimese privaatsusele tähendab, et nende andmete kasutamist on vaja veenvalt põhjendada.

[190] Määrus artikkel 9 lg 1.
[191] *S. and Marper* pp 85-86.
[192] *Ibid* p 81, 84.
[193] EIKo. 25.09.2001, no. 44787/98, *P.G. and J.H. v. the United Kingdom*. Edaspidi *P.G. and J.H. v. the United Kingdom.*
[194] *P.G. and J.H. v. the United Kingdom, pp 59-60.*
[195] *S. and Marper*, p 84.

Õiguskirjanduses, Artikkel 29 Töörühma arvamustes ja Euroopa andmekaitseinspektori hinnangul mõjutab ka asjade internet oluliselt andmesubjekti eraelu puutumatust. Artikkel 29 Töörühm loeb näiteks biomeetrilisi andmeid isikuandmete liigiks, millel on suur mõju nii asjade interneti kasutajate kui teiste isikute eraelule.[196] Biomeetriliste andmete töötlemist asjade internetis praktikas on näiteks analüüsitud Euroopa Horizon 2020 projekti STARR (*Decision SupporT and self-mAnagement system for stRoke survivoRs*) puhul. STARR-i projekt põhines targa keskkonna loomises insuldist taastuvate patsientide kodudesse, et monitoorida nende paranemist. Tulemusena leiti, et tervise ja biomeetrilisi andmeid töötlevate tarkade seadmete panek patsientide kodudesse kujutab endast suurt ohtu patsientide privaatsusele.[197] Seda ka juhul kui tehniliselt on kõikvõimalik tehtud privaatsuse tagamiseks.[198] Asjade interneti eesmärk on pakkuda kasutajale märkamatut, kuid andmetöötluse perspektiivis väga invasiivset teenust.[199] Andmesubjekt kaotab kontrolli oma andmete üle väga kergesti. Interaktsioon asjade vahel, isikute ja asjade vahel ning asjade ja *back-end* süsteemide vahel viib andmete vooluni, mida on ääretult raske hallata. Asjadevaheline kommunikatsioon võib alata automaatselt või vaikimisi ilma, et andmesubjekt oleks sellest teadlik. CNIL näiteks juhendab inimesi oma koduseid asjade interneti seadmeid välja lülitama või ka voolust välja ühendama, sest võimatu on teada millal nad isikuandmeid koguvad ja kuidas.[200] Olukorras, kus kombineeritakse andmeid erinevatest sensoritest erinevatel laialt määratletud eesmärkidel, on kerge tekkima andmete töötlemise funktsiooni laienemine (inglise k. *function creep*).[201] Näiteks seadmed STARRi projektis töötlevad nii tervise, elustiili kui ka emotsionaalse heaolu andmeid ja neid töödeldakse kombineeritult edasi suurandmete analüütikaga. Artikkel 29 Töörühm oli seisukohal, et olukorras, kus ilma asjade interneti seadmeteta oleks olnud väga keeruline andmeid ühendada, mõjutab isikuandmete töötlemine tõenäoliselt oluliselt isiku põhiõigust privaatsusele ja isikuandmete kaitsele.[202] Enesemõõtmise seadmed illustreerivad hästi, kui palju andmeid on võimalik tuletada algeliste sensorite abil kogutud toorete andmete

[196] Artikkel 29 Töörühm. Opinion 02/2013 on apps on smart devices. 00461/13/NE. WP 202. 27.02.2013, lk 9. Kättesaadav arvutivõrgus: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf. Edaspidi Artikkel 29 Töörühm. Opinion 02/2013 on apps on smart devices.
[197] Pichierri, ja Dimitrova, lk 175.
[198] *Ibid*, lk 178.
[199] *Ibid*, lk 179.
[200] CNIL. Enceintes intelligentes : des assistants vocaux connectés à votre vie privée. 20.12.2018. https://www.cnil.fr/fr/enceintes-intelligentes-des-assistants-vocaux-connectes-votre-vie-privee. Edaspidi CNIL. Enceintes intelligentes : des assistants vocaux connectés à votre vie privée.
[201] Paindlike ja laiade eesmärkide probleemi asjade internetis on Artikkel 29 Töörühm rõhutanud mitmes arvamuses. Vt. Artikkel 29 Töörühm. Opinion 8/2014 on the on Recent Developments on the Internet of Things, lk 8; Artikkel 29 Töörühm. Opinion 02/2013 on apps on smart devices, lk 2.
[202] Artikkel 29 Töörühm. Opinion 8/2014 on the on Recent Developments on the Internet of Things. lk 15.

agregeerimisel. Näiteks liikumisandur kogub ainult andmeid isiku liikumismustri kohta, kuid lõpptulemusena avaldatakse inimese üldine füüsiline seisund. Niinimetatud sensorite segunemisel (inglise k. *sensor fusion*) saadud uued isikuandmed pakuvad uusi võimalusi, mida ei olnud ette näha esialgsel andmete kogumisel. Eelnevast tulenevalt võib väita, et nii asjade internet kui biomeetriliste andmete töötlus eraldiseisvalt mõjutavad isikute eraelu olulisel määral, kuid nende ühendamise tagajärg on veel suurema mõjuga indiviidi eraelu puutumatusele.

Määruse preambulist tuleneb eriliigiliste isikuandmete kohta, et kaitset väärivad isikuandmed, mille töötlemise kontekst võib põhiõigusi ja -vabadusi olulisel määral ohustada.[203] Asjade internet kahtlemata annab sellise konteksti biomeetriliste andmete töötlemisele. Siiski tehnoloogia neutraalsuse põhimõttest ja asjade interneti seadmete mitmekesisusest tulenevalt ei saa käesolevas magistritöös selgelt määrata ette, millal töödeldakse eriliigilisi biomeetrilisi andmeid kõikides seadmetes. Sellegipoolest kui biomeetrilised andmed osalevad struktureeritud andmebaasina suurandme- või pilvetöötluses võib üpris kindlalt väita, et tegemist on eriliigiliste biomeetriliste andmete töötlemisega. Asjade interneti olemusest lähtuvalt tuleb eeldada, et mingil ajahetkel võivad muutuda ka kõige tühisemad või anonümiseeritud andmed inimese füüsiliste või käitumuslike omaduste kohta eriliigilisteks biomeetrilisteks andmeteks või võimaldavad tuvastada teisi eriliigilisi isikuandmeid, näiteks tervise andmeid. Eelnevast tulenevalt võib tuvastada kriteeriumid, mille alusel hinnata, kas asjade interneti seadmed töötlevad eriliigilisi biomeetrilisi andmeid:

a. kogutavad biomeetrilised andmed on universaalsed, püsivad ja unikaalsed ehk sobivad tuvastamiseks;
b. biomeetriliste andmete säilitamise aeg ehk tõenäosus, kas andmete kasutamise viis on ettenähtav või mitte;
c. andmete hoidmise struktureerituse aste, ehk kui vähe vaeva võtab nende ühildamine tuvastussüsteemiga.

[203] Määrus preambul p 51.

3.1.2. Õigusliku aluse valik

Sõltuvalt kas vastutav töötleja leiab, et töötleb asjade internetis eriliigilisi või tavalisi isikuandmeid, peab ta valima õigusliku aluse vastavalt kas Määruse artiklist 6 või 9. Kui isikuandmeid kogutakse ainult isiklikel eesmärkidel ja koduseks kasutamiseks ja andmeid töödeldakse lokaalselt seadmes, siis rakendub koduse erandi reegel.[204] Näiteks kui avada isiklik mobiiltelefon sõrmejäljega ja biomeetriline võrdlemine toimub lokaalselt seadmes, siis võib see käia koduse erandi alla.[205] Praktikas, aga on asjade interneti ärimudel üles ehitatud andmete süstemaatilisele edastamisele seadme tootjatele, rakenduste arendajatele ja veel kolmandatele isikutele. Seega kodune erand on piiratud asjade interneti kontekstis ja seetõttu autor asjade interneti puhul sellel rohkem ei peatu. Käesoleva magistritöö teemast väljub ka tavaliste biomeetriliste andmete töötlemine, mistõttu ei analüüsita Määruse artikkel 6 õiguslike aluste kasutust asjade internetis.

Euroopa Liidus reguleerivad isikuandmete kaitset asjade internetis nii Määrus kui ka e-privaatsuse direktiiv parandatud Direktiiviga 2009/136/EÜ.[206] Eestis on e-privaatsuse direktiiv üle võetud elektroonilise side seadusega (edaspidi ESS).[207] ESSi ja e-privaatsuse direktiivi kohaldatakse igasugustele lõppkasutaja seadmetele, mis edastavad infot otse seadmest kolmandale isikule või asetavad infot seadmele.[208] Näiteks kohaldub e-privaatsuse direktiiv kui seadme tootja soovib ligipääsu seadmes talletatud tooretele andmetele. Sellisel juhul peavad kõik osapooled olema kindlad, et andmesubjekt on andnud oma nõusoleku. Kasutaja nõusolek peab olema saadud enne seadmel olevale infole ligipääsu andmist.[209]

Määrust ja e-privaatsuse direktiivi saab kohaldada koos. Nende koosmõju on järgmine: seade, näiteks sammulugeja, kogub andmed oma sisemisse mällu. Selleks, et kasutaja saaks need andmed kätte läbi rakenduse oma telefonis, on vaja seadme tootjal andmed sammulugejast oma serverisse üles laadida. Serverisse üles laadimiseks on vaja andmesubjekti nõusolekut e-

[204] Andmekaitse Inspektsioon. Kantavad seadmed ja privaatsus, lk 7; CNIL. Biométrie dans les smartphones des particuliers : application du cadre de protection des données.
[205] CNIL. Biométrie dans les smartphones des particuliers : application du cadre de protection des données.
[206] Euroopa Parlamendi ja nõukogu direktiiv 2009/136/EÜ, 25. november 2009 , millega muudetakse direktiivi 2002/22/EÜ universaalteenuse ning kasutajate õiguste kohta elektrooniliste sidevõrkude ja -teenuste puhul, direktiivi 2002/58/EÜ, milles käsitletakse isikuandmete töötlemist ja eraelu puutumatuse kaitset elektroonilise side sektoris, ning määrust (EÜ) nr 2006/2004 tarbijakaitseseaduse jõustamise eest vastutavate siseriiklike asutuste vahelise koostöö kohta (EMPs kohaldatav tekst). – ELT L 337, 18.12.2009.
[207] Elektroonilise side seadus. - RT I 2004, 87, 593.
[208] ESS § 2 p 60; Artikkel 29 Töörühm. Opinion 8/2014 on the on Recent Developments on the Internet of Things. lk 7.
[209] Artikkel 29 Töörühm. Opinion 02/2013 on apps on smart devices, lk 10.

privaatsuse direktiivi artikkel 5 lg 3 järgi.[210] Artikkel 5 lg 3 kohaldub kõikidele isikutele, kes loevad või laevad informatsiooni tarkadele seadmetele sõltumata, kas tegemist on avaliku või eraisikuga, vastutava töötleja või volitatud töötlejaga. Nõusoleku nõue kohaldub ka igale informatsioonile sõltumata andmete olemusest. See tähendab, et andmed ei ole piiratud isikuandmetega.[211] Näiteks kui reklaamiagentuur soovib samuti otse ligipääsu andmetele seadmel, et pakkuda käitumise analüüsil põhinevaid reklaame, siis on tal vaja andmesubjekti nõusolekut e-privaatsuse direktiivi artikkel 5 lg 3 järgi. Kui aga sama reklaamiagentuur soovib ligipääsu serveris olevatele agregeeritud andmetele, siis selleks on vaja õiguslikku alust Määrusest.[212] Samal ajal on olukordi, kus on vaja andmesubjekti isikuandmete töötlemiseks õiguslik alus kombineerida nii Määrusest kui e-privaatsuse direktiivist. Näiteks autorendi ettevõte rendib füüsilisele isikule targa auto. Auto tootjal on vaja saada e-privaatsuse direktiivi järgi nõusolek auto kasutajalt ehk füüsiliselt isikult, sest auto töötleb tema isikuandmeid. Autorendi ettevõte aga lähtub enda ja kliendi vahel õigusliku aluse valikul Määrusest.[213] Seega Määrust kohaldatakse juhtudel, kus töötlemine läheb kaugemale seadmes isikuandmete säilitamisest ja ligipääsu andmisest.

Artikkel 29 Töörühm on öelnud, et e-privaatsuse direktiivi nõusoleku kehtivuse hindamiseks kasutatakse samu kriteeriumeid, mis Määruse nõusoleku kehtivuseks.[214] Nii Määruse kui e-privaatsuse direktiivi järgi tuleb andmesubjekti nõusolek saada enne andmete väljastamist seadmest. Nõusolekut on siiski vaja eristada, kas see on antud informatsiooni lugemiseks seadmelt või see on vajalik õiguslik alus eri tüüpi andmete töötlemiseks. Mõlemad nõusolekud on küll üheaegselt kohaldatavad ja alluvad eri õiguslikele regulatsioonidele, kuid igal juhul peab nõusolek olema vaba, konkreetne ja teadlik.[215] Seega kui seade kogub kasutaja kohta biomeetrilisi andmeid ja neile andmetele seadmes antakse juurdepääs kolmandale isikule, siis nõusolek tuleb saada e-privaatsuse direktiivi alusel. Samal ajal sellele nõusolekule kehtivad aga magistritöö teises osas leitud biomeetriliste andmete töötlemiseks nõusoleku tingimused.

---

[210] E-privaatsuse direktiivi artikkel 5 lg 3 ütleb järgmist: „Liikmesriigid tagavad, et elektrooniliste sidevõrkude kasutamine teabe salvestamiseks või juurdepääsuks abonendi või kasutaja lõppseadmesse salvestatud teabele on lubatud ainult tingimusel, et asjaomasele abonendile või kasutajale esitatakse direktiivi 95/46/EÜ kohaselt selge ja arusaadav teave muu hulgas andmete töötlemise eesmärgi kohta ning talle antakse võimalus keelduda vastutava andmetöötleja teostatavast töötlemisest. See ei takista tehnilist salvestamist või juurdepääsu, mille ainus eesmärk on teostada või toetada side edastamist elektroonilises sidevõrgus või mis on hädavajalik sellise infoühiskonna teenuse osutamiseks, mida abonent või kasutaja on selgesõnaliselt taotlenud."

[211] Artikkel 29 Töörühm. Opinion 02/2013 on apps on smart devices, lk 7.

[212] Artikkel 29 Töörühm. Opinion 8/2014 on the on Recent Developments on the Internet of Things, lk 14.

[213] *Ibid.*

[214] *Ibid.*

[215] Artikkel 29 Töörühm. Opinion 02/2013 on apps on smart devices, lk 14.

Nagu eelnevalt leitud, siis ka tavaliste biomeetriliste andmete kogumisel asjade internetis peaks vastutav töötleja eeldama, et need muutuvad ühel hetkel eriliigilisteks isikuandmeteks. Selline olukord võib tekkida eelkõige, kui inimest mõõtev seade kogub tooreid andmeid, mis iseenesest ei ole eriliigilised isikuandmed, kuid neist võib tuletada eriliigilisi isikuandmeid. Vastutav töötleja peab olema valmis küsima andmesubjektidelt selgesõnalist nõusolekut, kui ta töötleb isikuandmeid otse andmesubjekti seadmelt. Vastutavad töötlejad peaksid eeldama sellist kvalifikatsiooni muutust ja võtma vastavaid samme. Sealjuures ei ole oluline, kas nõusolek õigusliku alusena tuleneb Määrusest või e-privaatsuse direktiivist, sest eriliigiliste biomeetriliste andmete töötlemiseks on vajalik, et nõusolek vastaks magistritöö teises osas leitud kriteeriumitele.

Asjade internetis andmete töötlemine võib puudutada ka isikuid, kes ei ole tegelikud seadme kasutajad. Artikkel 29 Töörühm rõhutab, et see faktor ei välista EL õiguse kohaldamist. EL-i andmekaitse reeglite kohaldamine ei sõltu, kes omab seadet või terminali, vaid oleneb andmete töötlemisest.[216] Seega biomeetriliste andmete töötlemisel peab seade suutma eristada isikuid, kelle isikuandmeid töödeldakse ja küsima igaühelt nõusolekut. Asjade interneti seadmed puutuvad tihti kokku rohkem kui ühe inimese andmetega ja seetõttu järgmises peatükis analüüsitakse, kuidas leida sobiv õiguslik alus määramata isikute ringilt.

3.1.3. Nõusoleku saamine määramata isikute ringilt

On paratamatu, et asjade internet ja tehisintellekt hakkavad inimesi ümbritsema üha rohkem. Isik võib juhuslikult liituda targa ruumiga, mis ei ole tema oma. Näiteks võib külastada kellegi teise tarka kodu, olla kaassõitja targas autos, minna kaubanduskeskusesse või siseneda erinevate tarkade seadmetega varustatud kontorisse. Sellisel juhul võivad seadmed ka nende kohta isikuandmeid koguda, mida võib omakorda väärkasutada. Privaatsuse kaitseks tarkades keskkondades on Määrus ette näinud vaikimisi ja lõimitud andmekaitse põhimõtted.[217] Küll aga ennustatakse, et moodustumas on nn liidetud ühiskond, kus kantavad seadmed, kodutehnika, transpordivahendid ja avalikud ruumid koguvad pidevalt nendega kokku puutuvate inimeste isikustatud ja isikustamata andmeid ning omakorda ühendavad need andmetega, mis on saadud teistest seadmetest või tarkadest ruumidest. M. L. Jones on

[216] Artikkel 29 Töörühm. Opinion 8/2014 on the on Recent Developments on the Internet of Things, lk 13.
[217] Määrus art 25 lg 1-2.

kirjeldanud sellist keskkonda „targa avalikkusena." „Asjade internet on sellise tuleviku algus, kuid tark avalikkus kirjeldab kogemust, kus isikud liiguvad läbi võrgustunud keskkonna ja nad on osa liidetud reaalsusest, mis on mõneti erinev kui olla liidetud läbi erinevate ekraanide, nagu praegusel ajal harjunud oleme."[218] Vaikimisi ja lõimitud andmekaitse põhimõtetega arvestav privaatsuse haldamine sellises keskkonnas jääb tehnoloogiliseks väljakutseks. Asjade interneti seadmed, millega puutub kokku määramatu hulk inimesi, on aga tegelikkus juba praegu. Seega tuleb vastata küsimustele, kuidas määrata vastutav töötleja, kes vastutab kõikidelt andmesubjektidelt nõusoleku saamise eest ja kuidas saadakse kehtiv nõusolek. Nagu eelnevalt leitud, tähendab andmesubjekti vaba ja teadlik nõusolek reaalset kontrolli teostamist oma isikuandmete kasutamise üle.

Tehisintellektiga varustatud seadmete puhul on keeruline eristada andmesubjekti, vastutavat töötlejat ja volitatud töötlejat. Kui andmesubjekt omab seadet, siis on tema ka vastutav töötleja, sest tema otsustab, mis eesmärkidel isikuandmeid töödeldakse ja valib töötlemise viisi ehk otsustab seadet kasutada. Kerge on tuvastada töötlemiseks õigusliku aluse olemasolu, kui seadmel on üks kasutusotstarve, näiteks tark hambahari, mis kogub omaniku igapäevase rutiini ja hügieeni kohta andmeid. Nagu eelnevalt leitud, on siin määravaks, kas andmeid töödeldakse seadme sees või saab kasutaja andmeanalüüsi tulemusi näha näiteks oma mobiilirakendusest. Esimesel juhul on tegemist koduse erandiga ja teisel juhul on vaja kasutaja nõusolekut.

Kasutaja ise võib ka muutuda vastutavaks töötlejaks. Näiteks külaline viibib ajutiselt seadme omaniku kodus. Targa kodu süsteemid opereerivad suuresti video ja häältuvastuse baasil ja on tõenäoline, et tihti kogutakse ka eriliigilisi isikuandmeid. Näiteks lasevad mõned koduseadmed enne kasutama hakkamist salvestada kasutajate hääle näidised, et eristada pereliikmeid üksteisest.[219] Kui need töödeldavad andmed ei välju kasutatavast seadmest, siis jääb vastutavaks töötlejaks seadme omanik, kes peab hoolitsema nõusoleku tõendatavuse eest. Siin tuleb aga jällegi viidata erandile, mille kohaselt isiklikel ja kodustel eesmärkidel isikuandmete töötlemisele Määrust ei kohaldata. Teisisõnu, kui tegemist on isikliku kodu või isikliku sõiduautoga, kus töödeldakse andmeid lokaalselt, siis ei teki vajadust Määrusest õiguslikku alust otsida. Asjade interneti olemus ja targa keskkonna kontseptsioon aga tähendavad, et isikuandmeid pidevalt jagatakse ja töödeldakse edasi uutel viisidel, mistõttu autori hinnangul isiklikel ja kodustel eesmärkidel töötlemise erandit ei saa enamikul juhtudel kasutada. Artikkel

[218] M. L. Jones. Privacy without Screens & the Internet of Other People's Things. - Idaho Law Review 2015, Vol 51, lk 641.
[219] CNIL. Enceintes intelligentes : des assistants vocaux connectés à votre vie privée.

29 Töörühm on rõhutanud, et seadmete kasutajad peaksid teavitama mitte-kasutajaid seadme olemasolust ja isikuandmete tüüpidest, mida nende kohta kogutakse. Kasutajad peaksid austama teiste inimeste soovi mitte lasta enda andmeid seadmel töödelda.[220]

Kui liitreaalsuse seadme kasutaja laeb sotsiaalmeediasse või oma veebilehele üles video või foto, mis ta on seadmega teinud, siis saab temast vastutav töötleja, kui ta tegutseb mõne ettevõtte või assotsiatsiooni nimel või kasutab sotsiaalmeediat ärilistel või poliitilistel eesmärkidel. Vastutav töötleja saab temast ka juhul, kui tema sotsiaalmeedia profiil on avatud avalikkusele ilma valitud kontaktide lukuta.[221] Pärast materjali sotsiaalmeediasse üles laadimist saab sotsiaalmeedia pakkuja samuti vastutavaks töötlejaks, kui töötleb või kogub üles laetud andmeid. See tähendab, et sotsiaalmeedia pakkuja on vastutav töötleja ka andmete osas, mida on võimalik üles laetud fotost või videost eraldada, nagu biomeetrilised andmed või asukohaandmed. Seega on ilma nõusolekuta kolmanda isiku isikuandmete töötlemise eest vastutavad mõlemad nii sotsiaalmeedia kasutaja kui ka platvormi pakkuv ettevõte.[222]

Kuna käesolevas magistritöös uuritakse vaid vabatahtlikult kasutatavaid seadmeid, siis ei pääse andmesubjekti nõusolekust ka avalikus ruumis ega koduses keskkonnas. Nõusolekut ei ole vaja küsida isikul, kes kogub isikuandmeid vaid eraelulistel või kodustel eesmärkidel. Küll aga peavad targa keskkonna seadmete tootjad saama biomeetriliste andmete töötlemiseks andmesubjekti selgesõnalise nõusoleku. Õiguskirjanduses rõhutakse vajadusele disainida sellised seadmed tugevate tuvastustehnoloogiatega, mis võimaldaks isikutel vahet teha ja teada, kas nõusolek on antud isikuandmete töötlemiseks ehk nõusoleku saamine sõltub seadme disainist. Näiteks võib tehisintellektiga seade selgelt küsida uue andmesubjekti nõusolekut häälkäskluse või ekraani kaudu.[223]

[220] Artikkel 29 Töörühm. Opinion 8/2014 on the on Recent Developments on the Internet of Things, lk 24; CNIL. Enceintes intelligentes : des assistants vocaux connectés à votre vie privée.
[221] A. Kotsios, lk 168.
[222] *Ibid*, lk 170.
[223] W. Barfield, U. Pagallo (koost). Research Handbook on the Law of Artificial Intelligence. Cheltenham: Edward Elgar Publishing Limited 2018, lk 299.

3.2. Kasutaja käitumist analüüsivad tööriistad

Biomeetriline tehnoloogia erasektoris on suhteliselt uus ja kõikidest biomeetrilistest andmetest kõige vähem on uuritud käitumuslikke biomeetrilisi andmeid ja nende kasutamist isiku kordumatuks tuvastamiseks.[224] Määruse vastuvõtmisel tekitas lahkarvamusi, kas käitumuslikud biomeetrilised andmed saavad olla eriliigilised biomeetrilised andmed. Arvati, et käitumuslikud andmed ei ole nii täpsed, et kedagi kordumatult tuvastada.[225] Sellegipoolest on teada, et käitumuslikke biomeetrilisi andmeid kasutatakse veebilehe külastajate tuvastamiseks samamoodi nagu näo või sõrmejälje abil tuvastatakse inimesi mobiiltelefonide avamiseks või maksete autoriseerimiseks.[226] Näiteks pakub ettevõte BioCatch[227] käitumuslikku biomeetrilist tuvastamist väga edukalt nii e-kaubanduses kui panganduses.[228] Erinevus käitumuslike ja füsioloogiliste biomeetriliste andmete vahel on, et inimese jaoks on tema käitumuslike omaduste lugemine tuvastamisel vähem tajutav. Ignoreerida ei saa aga asjaolu, et interneti kasutajate käitumismustreid analüüsivad igapäevaselt lugematu arv analüütika tööriistu ja iga veebilehe omanik soovib teada võimalikult palju oma külastajate harjumustest. Selliste tööriistade kasutamise eesmärk ei ole enamasti kedagi konkreetselt tuvastada, kuid nagu asjade interneti puhul puuduvad siingi selged piirid kasutajate harjumuste anonüümse statistika ja biomeetrilise tuvastamise võimalikkuse vahel. Seetõttu uuritakse järgnevalt milliste tingimuste täitumisel muutub *online* käitumise töötlemine tavalisteks ja eriliigilisteks biomeetrilisteks andmeteks.

3.2.1. Käitumuslike andmete analüüs internetis

Elektroonikaseadmete ja otsingumootorite igapäevane kasutamine annab väärtusliku ülevaate inimeste funktsioneerimisest ja eelistustest. Ettevõtted tavaliselt eraldavad ja analüüsivad neid andmeid, et ennustada inimeste käitumist ja kohandada oma turundust vastavalt. Määruse järgi kutsutakse seda profiilianalüüsiks ja sellele kehtivad oma reeglid.[229] Samal ajal käitumise

[224] L. Wang, X. Geng, lk xv.
[225] P. de Hert, V. Papakonstantinou.
[226] Käitumuslikku biomeetriat kasutab näiteks *The Royal Bank of Scotland* pettuste avastamiseks. Vt S. Cowley. Banks and Retailers Are Tracking How You Type, Swipe and Tap. – The New York Times 13.08.2018.
[227] BioCatch on platvorm, mis põhineb tehisintellekti abil käitumusliku biomeetria analüüsil. Platvorm pakub reaalajas kasutaja tuvastamise abil digitaalset identiteeti. Platvormil on 90 miljonit kasutajat. Leitav arvutivõrgus: https://www.biocatch.com/.
[228] Näiteks *The Royal Bank of Scotland* kasutab BioCatchi tehnoloogiat. Vt arvutivõrgus https://www.biocatch.com/.
[229] Määrus art 22.

analüüsi saab kasutada ka isiku tuvastamiseks või autentimiseks. Seega tuleb selgitada, millal käitumise analüüsi alusel loodud profiilid vastavad eriliigiliste biomeetriliste andmete definitsioonile ja kas teenuse pakkujad peavad seetõttu vastama erilistele nõuetele.

Inimeste tegevus internetis jätab jälgi ja identiteeti on võimalik tuvastada näiteks nn küpsiste abil.[230] Interneti kasutajaid on võimalik tuvastada ka ilma küpsisteta puhtalt nende *online* käitumise alusel käitumispõhiste jälgimistehnoloogiate abil.[231] Jälgimistehnoloogiad kasutavad mustrite tuvastamise meetodit ning saavad andmeid isiku veebis surfamise harjumustest, seadmele alla laetud rakenduste tegevusest või keskkonnateguritest.[232] Selline jälgimine võib toimuda märkamatult ja ilma jälgitava isiku teadmiseta. Määrus ei täpsusta, mida tähendavad käitumuslikud tunnused artikkel 4 definitsioonis. Selleks, et sobida käitumuslike biomeetriliste andmete definitsiooniga peab aga käitumisel põhinev biomeetria vastama töö esimeses osas toodud tunnustele ehk olema universaalne, unikaalne ja püsiv. Need tunnused on olulised, et biomeetrilised andmed võimaldaks isikuid üksteisest eristada teatud täpsusega. Siit tuleb käitumusliku biomeetria põhiprobleem, et inimese käitumine ei ole ajas nii püsiv kui näiteks sõrmejälg ega nii unikaalne ühele inimesele kui silmaiirise muster. Seega kasutatavat käitumisel põhinevat biomeetriat kirjeldatakse kui dünaamilist olles samal ajal endiselt universaalne kõigile inimestele ja püsiv.[236] Artikkel 29 Töörühma arvates on tüüpilised käitumuslikud biomeetrilised andmed käsitsi kirjutatud allkiri, klahvivajutuse, rühi ja kõnnaku analüüs ning alateadvuslikke mõtteid paljastavad mustrid nagu valetamise puhul jne.[237] Mõõdetavate käitumuslike biomeetriliste andmete taksonoomia jaguneb viite kategooriasse: oskused, stiil, eelistused, teadmised, motoorika ja strateegia, mida kasutatakse igapäevaste ülesannete täitmisel, nagu auto juhtimine.[238] Biomeetriline tuvastustehnoloogia võib üheaegselt koguda andmeid kõigist viiest kategooriast. Seega käitumuslikud biomeetrilised andmed viitavad mõtlemise ja liikumise mustritele, mis avaldatakse objektiivselt arusaadaval kujul. *Online* keskkonnas tähendab see, et arusaadavad mustrid isiku käitumisest, nagu konkreetne seadme kasutusviis või sisu otsimise mustrid, peaksid kuuluma samuti käitumuslike biomeetriliste andmete kategooriasse, kui neid saab kasutada isiku kordumatuks tuvastamiseks.

[230] Küpsis on väga väike fail, mis laetakse alla kasutaja seadmele kui ta külastab veebilehte. Küpsised jälgivad kasutaja liikumist veebilehel või koguvad andmeid kasutaja seadmest, nagu asukoht või seadme andmed.
[231] Krausova, lk 162.
[232] *Ibid.*
[236] *Ibid*, lk 165.
[237] Artikkel 29 Töörühm. Opinion 3/2012 on developments in biometric technologies. Lk 4.
[238] L. Wang, X. Geng, lk xviii.

Magistritöö esimeses osas toodi välja kordumatu tuvastamise probleem käitumuslike isikuandmetega, mille järgi käitumisel põhinevad biomeetrilised süsteemid on kõige ebatäpsemad. Praktikas tähendab see, et käitumispõhist biomeetrilist tuvastamist pakkuvad teenused koguvad korraga kümneid inimese käitumuslikke omadusi, et oleks võimalik inimest kordumatult tuvastada. Näiteks BioCatch kogub kasutajate andmeid enam kui 2000 erineva käitumusliku omaduse kohta.[239]

Käitumuslik tuvastamine *online* keskkonnas põhineb lõppkasutaja seadme tegevuse jälgimisel. Biomeetria olemusest tulenevalt on Määruse mõistes biomeetrilised andmed ainult jäljendid, mis põhinevad füüsilise isiku tegevuse analüüsil. Tegevusmustreid võib saada kaudselt seadmega tehtud kõnedest, logidest, programmi käivitamisest jne. Küll aga seadme tegevus ise ei loo sidet kasutaja isiksusega, nagu automaatsed uuendused operatsioonisüsteemis. Seega uurides, kas teatud jäljend kuulub biomeetriliste andmete alla, tuleb analüüsida, millist tüüpi andmeid kasutati jäljendi loomisel.[240] Seadme tegevus võib luua seose füüsilise isikuga vaid lisainformatsiooni abiga. Nn seadme sõrmejälg,[241] mis põhineb funktsionaalsetel detailidel ja ei ole kasutaja tegevusega seotud, ei saa olla isikuandmed.[242] Kui aga analüüsitakse seadme tegevust kombineerituna kasutaja tegevusega, siis on tulemuseks biomeetriline jäljend. Teisest küljest, kui kasutaja käitumuslikud andmed võetakse mitme kasutaja andmetest ja loetakse vigaselt üheks kasutajaks, siis sellise ebatäpsusega andmeid ei saa lugeda biomeetriliseks jäljendiks isegi siis, kui see võimaldab tuvastada, et isikud on ühe pere liikmed.[243] Määrus ei ütle, et konkreetne tehniline töötlemine peab olema seotud ainult isiku füüsiliste, füsioloogiliste või käitumuslike andmega. A. Krausova on arvamusel, et biomeetrilised andmed on Määruse mõistes ka sellised jäljendid, mis on saadud mitme sensori andmete liitmisel, sh kui liidetakse eri liiki andmeid.[244] Teisisõnu kui seadme tehnilised detailid ja kasutaja käitumise andmed koos võimaldavad konkreetset isikut piisava täpsusega tuvastada, siis on tegemist biomeetrilise jäljendiga.[245]

Saamaks aru, mis on käitumuslike andmete kasutamise reaalsus internetis praegusel ajal tuleb vaadata ettevõtteid, kes on oma ärimudeli nende peale üles ehitanud. Esiteks kui vaadata konkreetset näidet käitumuslikust tuvastamisest, siis pakub e-kaubanduses sellist

[239] BioCatch. Kättesaadav arvutivõrgus: https://www.biocatch.com/company/our-story.
[240] Krausova, lk 168.
[241] Seadme sõrmejälg on seadme kohta kaugusest kogutud informatsioon seadme tuvastamiseks.
[242] Krausova, lk 169.
[243] Krausova, k 170.
[244] *Ibid*, lk 169.
[245] Fenomeni nimetatakse ka informatsiooni segunemiseks (inglise k. *information fusion*).

tuvastustehnoloogiat BioCacth. BioCatch hõlmab enam kui 2000 kognitiivse, käitumusliku ja psühholoogilise parameetri töötlemist.[246] Nende hulgas on näiteks viis, kuidas kasutaja hoiab mobiiltelefoni, kuidas ta vaatleb veebilehte või kuidas reageerib lehe kasutajaliidesele. Tegemist on passiivse tuvastamisega, mis suudab eristada päris inimest *botist* ja läbib ka nn elususe testi.[247]

Samal ajal on väga levinud analüütika tööriist HotJar, mis ei seosta end kuidagi biomeetriliste andmete töötlemisega.[248] Küll aga jälgib nende tehnoloogia samuti veebilehe külastajate käitumist suure täpsusega. HotJari eesmärk on näha, kuidas klient veebilehel liigub, kuhu ta vajutab, mis on arusaamatud kohad ning millisel hetkel ta kaotab huvi. Selleks kasutab HotJar muuhulgas soojuskaarte (inglise k. *heatmap*), videosalvestusi kliendi tervest sessioonist veebilehel ja mustrite loomist kliendi teekonnast alates esimesest veebilehe külastusest kuni ostuni.[249] Kokkuvõtvalt HotJar teeb detailse profiili igast konkreetsest veebilehe külastajast tema eelistuste, motoorika ja strateegia põhjal.

Vahe kahe eelkirjeldatud ärimudeli vahel võib olla väga väike ja väga tehniline, miks üks tuvastab füüsilisi isikuid ja teine mitte. Vahe võib ka olla vaid asjaolus, et ühe eesmärk on tuvastada füüsilisi isikuid, kuid vahendid selleks on mõlemal. Nagu käesolevas magistritöös läbivalt analüüsitud tuleb siingi rõhutada, et eriliigilisteks muudab biomeetrilised andmed asjaolu, kui kerge on neid kasutada vastutaval töötlejal ise või kolmandatel isikutel tuvastamiseks. Vastutav töötleja peab jälgima magistritöös eelnevalt leitud kriteeriume ehk andmekogu detailsust, struktureeritust ja säilitamise aega. Autor leiab, et mida detailsem on isiku kohta loodud profiil, seda unikaalsem on see isikule. Kui ühe grupi, näiteks ühe veebilehe külastajate kohta kogutakse samu käitumuslikke andmetüüpe, siis muutuvad need andmetüübid vastavas grupis ka universaalseteks. Seega tekib küsimus kas HotJari ja sarnaste programmide poolt peetavad andmekogud võimaldavad kerge vaevaga kasutajatest biomeetrilisi profiile luua, mida kasutada tuvastamiseks eri valdkondades. Sellele oskab ilmselt kõige paremini vastata mõni IT-ekspert, kuid olemasoleva info puhul võib väita, et see on ääretult tõenäoline.

[246] BioCatch. Kättesaadav arvutivõrgus: https://www.biocatch.com/company/our-story.
[247] BioCatch. What is behavioural biometric? Data Sheet. *Sine anno.* Kättesaadav arvutivõrgus: https://www.biocatch.com/hubfs/White%20Papers/What%20is%20Behavioral%20Biometrics.pdf?hsCtaTracking=07028355-5500-4d50-b976-f7be210efa8d%7C598e23f9-e463-49f2-a5d0-1e2eb83cb04b.
[248] HotJar on platvorm, mis visualiseerib kasutajakogemust veebilehel. Tegemist on tööriistaga disaineritele, turundajatele ja tootejuhtidele. Leitav arvutivõrgus: https://www.hotjar.com/.
[249] HotJar. Kättesaadav arvutivõrgus: https://www.hotjar.com/tour.

Käitumuslikud mustrid on isiku identiteedi väljendus ja seega väärivad kaitset nagu ülejäänud biomeetrilised andmed. Nagu asjade interneti puhul, tuleb siingi jõuda järeldusele, et andmete kombineerimine erinevatest allikatest võib kergesti luua isiku biomeetrilise jäljendi. Jäljend ise kuulub tavaliste isikuandmete kategooriasse, kuid eriliigiliste isikuandmete kategooriasse liigitumisel saab määravaks jäljendi kasutus. Kasutus tähendab nii kogumist, säilitamist ja töötlemist koos muude andmetega. Turul on mitmeid *online* käitumise põhiseid analüütika programme erinevate eesmärkide täitmiseks. Kahtlemata on nii ettevõtetele kui klientidele kasulikud tööriistad, mis suudavad luua mugavamaid ja individuaalsemaid teenuseid. Küll aga peaksid vastutavad töötlejad jälgima, et nad ei looks klientidest detailseid biomeetriliste jäljendite kogusid, mida saaks kasutada isiku universaalseks tuvastamiseks teistes süsteemides. Näiteks käesolevas peatükis analüüsitud HotJar ei pruugi luua sellist universaalset biomeetrilist jäljendit kemikaalide müügi *business-two-business* platvormil. Küll aga HotJari analüütika kasutamine panga veebilehel, kus kasutatakse paralleelselt käitumuslikku biomeetrilist tuvastustehnoloogiat, võib luua tuvastamiseks sobiva biomeetrilise jäljendi. Identiteedivarguse risk on mõlemal programmil, kuid tuvastustehnoloogias on sellega arvestatud ja tagatud kõrgem turvalisus. Eelnevast tulenevalt peab vastutav töötleja sobiva analüütika programmi valimisel hindama juba kasutuses olevate programmide ja uue programmi koosmõju ja tagajärgi.

3.2.2. Õigusliku aluse valik käitumuslike andmete analüüsiks

Käitumuslike biomeetriliste jäljendite loomine tugineb käitumises mustrite märkamisel ja isiku psühholoogiliste omaduste analüüsil. Artikkel 29 Töörühm on oma arvamuses öelnud, et psühholoogial põhinevad biomeetrilised meetodid mõõdavad isiku reaktsioone konkreetsetele situatsioonidele või konkreetsetele testidele, et kinnitada psühholoogilist profiili.[250] Selline biomeetriline tuvastamine käib Määruse artikkel 9 lg 1 alla ja õiguslik alus tuleks leida artikkel 9 lg 2 eranditest eriliigiliste biomeetriliste andmete töötlemise keelule. Eelmises peatükis analüüsitud BioCatchi tehnoloogia rakendamiseks oleks üldjuhul vaja artiklist 9 andmesubjekti selgesõnalist nõusolekut, kui tegemist ei ole eriolukorraga nagu finantssektoris juriidilise kohustuse täitmine.

[250] Artikkel 29 Töörühm. Opinion 3/2012 on developments in biometric technologies, lk 4.

Profiilide loomine käib ka profiilianalüüsi alla. Määruse artikkel 4 punkt 4 sätestab profiilianalüüsi definitsiooni järgmiselt: „igasugune isikuandmete automatiseeritud töötlemine, mis hõlmab isikuandmete kasutamist füüsilise isikuga seotud teatavate isiklike aspektide hindamiseks, eelkõige selliste aspektide analüüsimiseks või prognoosimiseks, mis on seotud asjaomase füüsilise isiku töötulemuste, majandusliku olukorra, tervise, isiklike eelistuste, huvide, usaldusväärsuse, käitumise, asukoha või liikumisega.“ Üldiselt seisneb biomeetria ja profiilianalüüsi erinevus nende eesmärgis. Biomeetriat kasutatakse isiku tuvastamiseks või autentimiseks, kuid profiilianalüüsi kasutatakse füüsilise isiku hindamiseks ja selle isiku teatud gruppi paigutamiseks.[251] Sellegipoolest on profiilianalüüs ja biomeetriline tuvastamine tehniliselt seotud nagu eelmises peatükis toodud analüütika tööriistade näitel võib ka järeldada.

Profiilianalüüs võib põhineda ka eriliigilistel isikuandmetel. On teada, et biomeetrilised andmed sisaldavad informatsiooni, mida saab kasutada teatud isikuomaduste hindamiseks, nagu tervis, sugu, etniline päritolu või emotsionaalne seisund. A. Krausova on arvamusel, et profiilianalüüs ise suudab ka luua isikut tuvastavaid biomeetrilisi andmeid kuigi esialgne eesmärk ei olnud töödelda biomeetrilisi andmeid.[252] Profiilianalüüsi eesmärk on anda hinnang, kuid analüüs ei pea siiski jõudma andmete põhjal tehtud otsuseni. Seega võib profiilianalüüs kuuluda eriliigiliste biomeetriliste andmete klassifikatsiooni, kui luuakse piisavalt täpsed biomeetrilised profiilid, mida demonstreeris ka eelmises peatükis toodud HotJari näide.

Määruse artikkel 22 lg 2 loetleb profiilianalüüsiks järgnevad õiguslikud alused: andmesubjekti ja vastutava töötleja vahelise lepingu sõlmimine või täitmine; vastutava töötleja suhtes kohaldatav liidu või liikmesriigi õigus; põhineb andmesubjekti selgesõnalisel nõusolekul.[253] Sama artikli lõige 4 aga sätestab, et profiilianalüüsil põhinevaid otsuseid ei või teha eriliiki isikuandmete töötlemisel, välja arvatud kui selleks on andmesubjekti selgesõnaline nõusolek või õiguslikuks aluseks on avalik huvi. Seega võib tavalisi biomeetrilisi andmeid töötlev *online* analüütika tööriist valida õiguslikuks aluseks Määruse artikkel 22 lg 2 järgi kõik kolm varianti, kuid eriliigiliste biomeetriliste andmete töötlemiseks ainult selgesõnalise nõusoleku või avaliku huvi. Kuigi kogutud käitumuslike andmete põhjal biomeetrilise jäljendi loomine ei olnud esialgu vastutaval töötlejal plaanis, võib tuvastatud käitumismustritel olla hiljem teine eesmärk. Määruse artikkel 6 lõige 4 kirjeldab sellist olukorda, kus vastutav töötleja peab hindama uue eesmärgi kooskõla esialgse eesmärgiga, et tuvastada kas esialgu valitud õiguslik

[251] Krausova lk 170.
[252] *Ibid*, lk 171.
[253] Määrus art 22 lg 2 pp a-c.

alus on veel kehtiv. Seejuures tuleb arvestada isikuandmete laadi ja kas tegemist on eriliigiliste isikuandmetega.[254] Biomeetriliste andmete puhul peab vastutav töötleja hindama, kas uus eesmärk muudab tavalised biomeetrilised andmed eriliigilisteks.

Selleks, et profiil kvalifitseeruks biomeetrilisteks andmeteks, peab see olema võimeline eristama isikut inimeste grupist. Samal ajal ei pea olema võimalik isiku täpset identiteeti tuvastada.[255] Kui vastutav töötleja loob *online* keskkonnas kasutaja käitumisest profiili, siis peab ta pidevalt hindama, kas loodud profiil võimaldab ühte isikut eristada teistest. Sealjuures ei ole oluline identiteedi tuvastamine, vaid oluline on eristusvõime. Oluline ei ole ka asjaolu, kas vastutav töötleja suudaks andmesubjektiga reaalses maailmas ühendust võtta. Kui ühte isikut on käitumusliku profiilianalüüsi tulemusel võimalik eristada teistest, on tegemist biomeetriliste andmetega.

Käitumise põhisel jälgimisel on tagajärjed teenuse pakkujatele, kes jälgivad kasutajate *online* aktiivsust, mida tihti loetakse anonüümseteks andmeteks, sest konkreetsete kasutajate identiteet ei ole teada. *Online* käitumise põhine profiili loomine on Määruse mõistes profiilianalüüs ja vastutav töötleja peaks lähtuma artiklist 22. Küll aga võib sõltuvalt kogutavate andmete hulgast ja viisist olla üheaegselt tegu ka biomeetriliste andmete töötlemisega. Sellisel juhul tuleb ikkagi lähtuda artiklist 22. Kui aga profiilianalüüsi viisi tõttu selgub, et töödeldakse eriliigilisi biomeetrilisi andmeid, siis on töötlemise õiguslikeks alusteks vaid andmesubjekti selgesõnaline nõusolek või avalik huvi.

3.3. Ettepanekud siseriikliku õiguse täiendamiseks

Magistritöö eelnevatest peatükkidest on selge, et biomeetriliste andmete valdkonnas vajab veel palju seadusandja poolt eraldi reguleerimist. Samuti on puudus täpsustavatest eeskirjadest andmekaitse järelevalveasutuste poolt. Määrus ei ole saavutanud harmoniseerimise eesmärki biomeetriliste andmete vallas ega andmesubjektide piisavat kaitset, mistõttu uuritakse käesolevas peatükis kuidas täiendada Eesti õigust, et andmesubjektide õigus privaatsusele oleks tagatud.

[254] Määrus art 6 lg 4 p c.
[255] Artikkel 29 Töörühm. Opinion 01/2012 on the data protection reform proposals. 00530/12/NE. WP 191. Brüssel, 2012. lk 10.

3.3.1. Võimalused Määruse kõrval siseriikliku õiguse täiendamiseks

Määruse preambul p 8 ütleb: „Kui käesolevas määruses on ette nähtud eeskirjade täpsustamine või piiramine liikmesriigi õigusega, võivad liikmesriigid sidususe seisukohast vajalikul määral ja liikmesriigi õiguse sätete arusaadavaks muutmiseks isikutele, kelle suhtes neid kohaldatakse, integreerida määruse elemente oma õigusesse.“ Määrus annab liikmesriikidele mitu võimalust näha ette Määrusest erinevaid eeskirju ja õigusakte biomeetriliste andmete kontekstis. Esiteks ütleb artikkel 9 lg 2 p a, et andmesubjekti nõusolekut ei saa kasutada õigusliku alusena eriliigiliste isikuandmete töötlemiseks, kui liidu või liikmesriigi õigus seda ei luba.[256] Teiseks sätestab artikkel 9 lg 4 järgmist: „Liikmesriigid võivad säilitada või kehtestada täiendavad tingimused, sealhulgas piirangud seoses geneetiliste, biomeetriliste või terviseandmete töötlemisega.“ Seejuures ei täpsusta Määrus, kas siin on mõeldud, et liikmesriik võib täiendada tavaliste biomeetriliste andmete töötlemist või eriliigiliste. Võib argumenteerida, et süstemaatilise tõlgendamise järgi vastav säte asub eriliigilisi isikuandmeid reguleerivas artiklis ja seetõttu ei käi tavaliste biomeetriliste andmete kohta. Teisest küljest Määrus teistes artiklites ka ei erista rangelt artiklite kohaldamisala. Näiteks artikkel 6 reguleerib õiguslikke aluseid tavaliste isikuandmete töötlemiseks, kuid lõikes 4 kirjeldab töötlemise eesmärgi laiendamist ilma andmesubjekti nõusolekuta ka eriliigiliste isikuandmete puhul.[257] Seega tõlgendab autor, et Määrus lubab siseriiklikult sätestada erinormid nii tavalistele kui eriliigilistele biomeetrilistele andmetele. Tähele tuleb panna, et Määruse artikkel 9 lg 4 näeb ette vaid täiendavate tingimuste ja piirangute kehtestamist, ehk Määrus annab minimaalse kaitse taseme, millest siseriikliku õigusega allapoole minna ei või.

Lisaks artiklile 9 on Määrus peatükis IX „Isikuandmete töötlemise eriolukordi käsitlevad sätted“ näinud ette mitmeid olukordi, kus liikmesriik võib kehtestada siseriiklikke õigusakte eraõiguslikes suhetes isikuandmete töötlemisele. Käesoleva magistritöö teema raames on seal biomeetriliste andmete jaoks oluline artikkel 88 isikuandmete töötlemisest töösuhtes. Artikkel 88 lg 1 sätestab: „Liikmesriigid võivad õigusaktide või kollektiivlepingutega ette näha täpsemad eeskirjad, et tagada õiguste ja vabaduste kaitse seoses töötajate isikuandmete töötlemisega töösuhete kontekstis, eelkõige seoses töötajate värbamisega, töölepingu, sealhulgas õigusaktides või kollektiivlepingutes sätestatud kohustuste täitmisega, juhtimisega, töö kavandamise ja korraldamisega, võrdsuse ja mitmekesisusega töökohal, töötervishoiu ja tööohutusega, tööandja või kliendi vara kaitsega ning tööhõivega seotud õiguste ja hüvitiste

[256] Määrus art 9 lg 2 p a.
[257] Määrus art 6 lg 4 p c.

isikliku või kollektiivse kasutamisega ning töösuhte lõppemisega.“ Määruse preambul p 155 täpsustab, et eelkõige on oodatud töösuhtes nõusoleku alusel isikuandmete töötlemise täiendavad tingimused.

Õiguskirjanduses on valdavalt toodud välja probleemi andmete töötlemise üle kontrolli kaoga tarkade seadmete keskkonnas ja keerulistes andmetöötlussüsteemides. Nii Euroopa andmekaitseinspektor kui mitmed õigusteadlased on leidnud, et klassikalised andmesubjektide õigusi kaitsvad meetmed ei oma enam praktilist kasu digitaalruumis.[258] Näiteks STARRi projekti osalised tõdesid, et kuigi nad on tehniliselt teinud kõikvõimaliku patsientide privaatsuse kaitsmiseks ja läbipaistvuse tagamiseks, jääb tehniliselt keerulises süsteemis nagu STARR ikkagi kõrge risk, et andmesubjektid ei saavuta kontrolli oma andmete üle ega suuda hallata oma informatsioonilist privaatsust.[259] Tarkades keskkondades ei suuda inimesed määratleda millal, kus, mis ulatuses ja eesmärkidel nende kohta infot kogutakse. Seetõttu on rõhutatud nõusolekut konfliktse õigusliku alusena tehniliselt keerulistes või andmete poolest massiivsetes süsteemides.[260] Andmesubjektid saavad informeeritud otsuseid teha, kui nad suudavad adekvaatselt hinnata riske ja kasu enda kohta käiva info avaldamisest.[261] Oluline on küll läbipaistvus ja andmesubjekti informeerimine, kuid selge ei ole kas see info on ka arusaadav andmesubjektidele ja kas neil on piisavat tehnilist teadmist, et sellest aru saada või teadmisi kuidas oma andmete töötlemist kontrollida. Andmesubjekti privaatsusotsuseid mõjutavad kognitiivsed ja käitumuslikud tendentsid.[262] Nii õigusteadlased kui Euroopa andmekaitseinspektor rõhutavad, et inimesed ei ole oma otsustes ratsionaalsed või neil on süstemaatilised kõrvalekalded ratsionaalsusest.[263] Seega on teadvustatud, et oleks ebaõiglane usaldada ainult andmesubjekti oma andmete kontrollimisel, kuna see kallutaks koormuse ebaõiglaselt andmesubjektile.[264]

Võimalik on ka, et andmesubjekt ei hooli privaatsusest lootuses saada kasu tehnoloogiast ja ei mõtle tagajärgedele. Isegi kui andmesubjekt on informeeritud ja ratsionaalne isik, kes hoolib oma privaatsusest, on tal endiselt raske hallata oma privaatsust tulenevalt keerulisest süsteemist, mis koosneb eri tehnoloogiatest ja osapooltest. Selline süsteem teeb keeruliseks

[258] EDPS. Opinion 4/2015. Towards a new digital ethics; Pichierri, ja Dimitrova; D. J. Solove. Privacy Self-Management and the Consent Dilemma. – Harvard Law Review 2013,Vol 126. Edaspidi Solove.
[259] Pichierri, ja Dimitrova.
[260] Solove, lk 1881.
[261] Pichierri, ja Dimitrova..
[262] Solove, lk 1883.
[263] EDPS. Opinion 4/2015. Towards a new digital ethics; Pichierri, ja Dimitrova; Solove.
[264] Pichierri, ja Dimitrova.

jälgida andmete voogu ja hallata privaatsust eraldi eri osapooltega.[265] Teiseks on raske andmete avaldamisel hinnata plusse ja miinuseid, sest mitmed kahjud tekivad alles andmekildude agregeerimisel pika aja jooksul erinevate osapoolte poolt.[266]

Eelnevast tuleneval tuleb näha vajadust õigusnormidega võtta andmesubjektilt vähemaks koormust oma privaatsust üksinda hallata. Biomeetrilisi andmeid töödeldakse keerulistes tehnoloogiates ja kaasnevaid riske on mitmeid. Teisest küljest ei saa ka alahinnata uute tehnoloogiate, sh asjade interneti olulisust Euroopa ühisturule[267] ega üldisele inimeste heaolule. Samas on teadvustatud, et uute tehnoloogiate kasutusele võtule on ülimalt oluline inimeste usaldus ja kontrolli tajumine oma isikuandmete üle.[268] Eelnevat arvesse võttes on inimeste privaatsuse haldamiseks vaja täpsemaid reegleid, et jõuda lähemale informatsioonilisele enesemääramisõigusele ja kontrollile.

3.3.2. Ettepanekud Eesti õiguse täiendamiseks eriliigiliste biomeetriliste andmete töötlemiseks

Eestis on biomeetriliste andmete kasutus eraõiguslikes suhetes pea täiesti reguleerimata. Samal ajal näiteks Prantsusmaa on erasektoris biomeetriliste andmete kasutust reguleerinud juba mitukümmend aastat, mistõttu on neil biomeetriliste andmete kontekstis omaette õigusharu välja arenenud.[269] Magistritöö eesmärk ei ole jõuda järgi mitmekümneaastase kogemusega CNIL-ile, vaid esitada ettepanekud, millega alustada Eestis biomeetriliste andmete töötlemise kontekstis inimeste põhiõiguste kaitse tagamist. Eelkõige õigust eraelu kaitsele, inimväärikusele, autonoomsust teha enda kohta otsuseid ja õigust informatsioonilisele enesemääramisele.

---

[265] Pichierri, ja Dimitrova; Solove.
[266] Solove, lk 1881.
[267] Euroopa Komisjon. Research & Innovation in Internet of Things. Policy 2018. Kättesaadav arvutivõrgus: https://ec.europa.eu/digital-single-market/en/research-innovation-iot.
[268] EDPS. Opinion 4/2015. Towards a new digital ethics, lk 10; Pichierri, ja Dimitrova, lk 178.
[269] Prantsusmaa reguleeris erasektoris biomeetriliste andmete töötlemist juba 2004. aastast ning CNILil on näiteks töökohas biomeetriliste andmete töötlemise reguleerinuf eraldi määrusega. Vt Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Version consolidée au 28 août 2004. Kättesaadav arvutivõrgus:
https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000006068624&dateTexte=20040828;
CNIL. Délibération n° 2019-001du 10 janvier 2019 portant règlement type relatif à la mise en œuvre de dispositifs ayant pour finalité le contrôle d'accès par authentification biométrique aux locaux, aux appareils et aux applications informatiques sur les lieux de travail. 01.10.2019. Kättesaadav arvutivõrgus: https://www.cnil.fr/sites/default/files/atoms/files/deliberation-2019-001-10-01-2019-reglement-type-controle-dacces-biometrique.pdf.

Määrus jätab enamasti lahtiseks, millise õigusjõuga normidega võib liikmesriik Määruses sätestatust kõrvale kalduda. Seega on allpool tehtud ka ettepanekud, kas eesmärki aitaks saavutada paremini normatiivakt või juhendmaterjalina eeskiri. Autor jätab siinkohal analüüsimata, millistesse konkreetsetesse õigusaktidesse tuleks täiendusi teha, sest see eeldaks vastavate õigusvaldkondade väga head tundmist Eesti õiguses ja sügavat analüüsi, mis väljub käesoleva magistritöö raamidest.

A. Nõusoleku piiramine andmete minimaalsuse ja turvalisuse kaalutlustest lähtuvalt

Võttes aluseks eelnevalt analüüsitud EIKi[270] seisukohad biomeetriliste andmete töötlemise riskidest, mitmed Artikkel 29 Töörühma ja Euroopa andmekaitseinspektori soovitused[271] ja liikmesriikide juhised,[272] teeb autor ettepaneku piirata andmesubjekti nõusolekut õigusliku alusena, kui tagatud ei ole teatud turvalisuse standard. Biomeetrilised andmed on eriliigiliste isikuandmete nimekirjas oma kasutusotstarbest tulenevate riskide tõttu. Biomeetriliste andmete oluline mõju isiku privaatsusele tuleneb asjaolust, et nad sisaldavad endas unikaalset informatsiooni konkreetse isiku kohta, mis lubab selle isiku identifitseerimist väga erinevates olukordades.[273] Konventsiooni isikuandmete töötlemisest ja standardid privaatsusele ja andmete kaitsele[274] konsultatsiooni komitee oli arvamusel, et uutes tehnoloogiates biomeetriliste andmete kasutamine viib vältimatult rohkemate andmete kogumisele, kui on vajalik. Selline töötlemine on võrreldav situatsiooniga, kus tavaline inimese nimi paljastab etnilise päritolu.[275] Biomeetrilised andmed sisaldavad nii genotüübi, rassi, etnilise päritolu kui haiguste infot. Vastutavad töötlejad ei tunnista pea kunagi, et nende soov on töödelda tervise või rassi andmeid, aga kui biomeetrilised andmed on kogutud, siis on andmesubjektil ja ka järelevalveasutusel vähene kontroll nende edasise kasutuse üle. Teisisõnu on andmesubjekti diskrimineerimise risk kõrge. Need riskid on ka teiste isikuandmetega, aga biomeetrilised tunnused on printsiibis muutumatud, universaalsed, ja oma olemuselt lubavad isikuid

[270] *S. and Marper; M.K. v. France*.
[271] Artikkel 29 Töörühm. Opinion 3/2012 on developments in biometric technologies; Euroopa andmekaitseinspektor. Comments on the Communication of the Commission on interoperability of European databases.
[272] Bundesnetzagentur. Bundesnetzagentur removes children's doll "Cayla" from the market**;** Data Protection Commission. Advice on Connected Toys and Devices; Commission Nationale de l'informatique et des Libertés. Biométrie dans les smartphones des particuliers: application du cadre de protection des données.
[273] *S. and Marper*, p 84.
[274] Isikuandmete automatiseeritud töötlemisel isiku kaitse konventsioon. – RT II 2001, 1, 3.
[180] Europa Nõukogu. Consultative Committee of the Convention for the Protection of Individuals with regard to automatic processing of personal data. Progress report on the application of the principles of Convention 108 to the collection and processing of biometric data. 2005, lk 19, p 74. Kättesaadav arvitvõrgus: https://rm.coe.int/16806840ba.

identifitseerida Seega teevad nad kergemini võimalikuks soovimatu identifitseerimise, profileerimise ja jälgimise. Arvestada tuleb ka biomeetriliste tehnoloogiate aina kasvavat standardiseeritust ja koostalitlevust, mistõttu ka identiteedivarguse risk kasvab paralleelselt ettevõtete ja organisatsioonide arvuga, kes kasutavad biomeetrilisi süsteeme. Andmete minimaalsuse põhimõttest ja isikuandmete turvalisusest lähtudes tuleks imperatiivse normiga sätestada:

a. Biomeetriliste andmete kasutamine tuvastustehnoloogiates on lubatud ainult biomeetrilise jäljendi abil. Biomeetrilisi andmeid saab hoiustada ja töödelda erinevas vormis, näiteks nö toorelt, kus tuvastamine toimub inimese näopildi alusel ja andmete allikas on äratuntav ilma suurema vaevata. Alternatiivina võetakse toorest biomeetrilisest allikast ainult teatud tunnused ja sellest omakorda moodustatakse jäljend, näiteks matemaatiline filter näopildil, mis filtri muutmisega loob uue jäljendi.[276] Igal juhul on andmesubjekti privaatsus paremini kaitstud, kui kasutatakse ainult matemaatilist biomeetrilist jäljendit. See vastab paremini andmete minimaalsuse põhimõttele, kuna töödeldakse ja talletatakse ainult see informatsioon, mida on tingimata vaja isiku tuvastamiseks ja mitte rohkem. Ka Artikkel 29 Töörühm on biomeetrilise süsteemi tehniliste meetmete nimekirjas toonud välja, et biomeetrilisi andmeid peaks hoidma jäljendina, kui see on võimalik.[277] Eeltoodud riske saab vähendada ainult sellega, kui biomeetrilisi tunnuseid on süsteemis piisavalt muudetud ja kõik üleliigsed andmed allikast automaatselt kustutatud.
b. Biomeetrilised tuvastustehnoloogiad peavad võimaldama luua mitu erinevat jäljendit ühest ja samast isiku füüsilisest või käitumuslikust omadusest. Selliselt hoitakse identiteedivarguse risk võimalikult madalal, sest andmesubjekt ei kasuta enda tuvastamiseks täpselt sama biomeetrilist jäljendit mitmes eri süsteemis.

B. Üldnorm töökohas biomeetriliste andmete töötlemiseks

Käesoleva magistritöö teisest osast selgus, et hetkel ei ole Eestis tööandjatel sobivat õiguslikku alust millele toetuda töötajate biomeetriliseks tuvastamiseks. Tööandja saaks toetuda vaid töötaja selgesõnalisele nõusolekule, kuid töösuhtes on sellise nõusoleku kehtivust keeruline tõendada ja töötajatele pakutavate alternatiivide ellu viimine on tööandja jaoks ka kulukas. Samas IKS RakS on toonud biomeetriliste andmete töötlemise õiguse ainult teatud

[276] Euroopa Komisjon. Join Researc Centre. Biometrics at the Frontiers, lk 97.
[277] Artikkel 29 Töörühm. Opinion 3/2012 on developments in biometric technologies, lk 31.

valdkondadesse nagu eriliiki isikuandmete töötlemine kaitseväeteenistuses.[278] Nagu eelnevalt välja toodi, puudutab IKS RakS eelkõige seda, kuidas avalik võim töötleb isikuandmeid. Määruse ülevõtmisega muudeti Töölepingu seaduses (edaspidi TLS)[279] vaid § 41, kuhu lisati lg 2, mis sätestab: „Tööandja peab tagama töötaja isikuandmete töötlemise vastavalt õigusaktides sätestatule.“ Muudatus ei anna alust eriliiki isikuandmete töötlemiseks töölepingu täitmiseks. Samuti ei anna eriliiki isikuandmete töötlemiseks võimalust IKS § 10, mille alusel saab erasektoris töödelda isikuandmeid eesmärgiga kaitsta vara ja isikuid. Ka Andmekaitse Inspektsioon on kritiseerinud IKS RaksSi sellepoolest, et TLS muudatuses viidatakse üldisemalt kohustusele. „Selline üldine viide ei ole piisavalt selge, kuidas on tööandjal lubatud töötaja isikuandmeid töödelda. Näiteks tuleks töösuhete kontekstis eraldi ära reguleerida ka jälgimisseadmestike (töökorralduslikud kaamerad, turvakaamerad, GPS-seadmed, arvutiprogrammid töötajate tegevuse kontrollimiseks jne) kasutamine.“[280]

Ometi võib biomeetrilise tuvastamise vajadusest töökohas aru saada. Nagu käesolevas magistritöös ka leiti, loetakse biomeetrilist tuvastamist väga usaldusväärseks identifitseerimise viisiks, mis suudab vastu seista ka pettuste ohule paremini kui tavalised PIN-koodid ja paroolikaardid. Seega on mõistetav, miks suure turvariskiga keskkondades oleks biomeetriline tuvastamine soovitav. Näiteks on CNIL lubanud töötajate biomeetrilist tuvastamist lennujaamas.[281] Seetõttu on autor arvamusel, et tööandja vara kaitseks või muude tööandja oluliste huvide kaitseks tuleks eriliigiliste biomeetriliste andmete töötlemiseks ette näha normatiivaktis üldine alusnorm biomeetrilise tuvastustehnoloogia kasutamiseks töökohas.

Määruse artikkel 5 lg 1 p b ütleb, et isikuandmed on asjakohased, olulised ja piiratud sellega, mis on vajalik nende töötlemise eesmärgi seisukohalt. Andmete olulisus viitab sellele, et töödeldakse ainult andmeid mis on olulised konkreetsete eesmärkide jaoks. Näiteks biomeetriline tuvastamine töökohas võib olla oluline, kui ruumidesse ligipääs on ainult konkreetsetel töötajatel ja ühelegi teisele kolleegile ligipääsuõigust delegeerida ei või. Tööandjal on biomeetriliseks tuvastustehnoloogiaks igal juhul vaja läbi viia andmekaitse mõjuhinnang, mis kujutab endast sisuliselt proportsionaalsuse testi.[282] Mõjuhinnangus tuleb

[278] Kaitseväeteenistuse seadus. - RT I, 10.07.2012, 1, § 14^1 lg 1.
[279] Töölepingu seadus. - RT I 2009, 5, 35.
[280] Andmekaitse Inspektsioon. Andmekaitse Inspektsiooni arvamus isikuandmete kaitse seaduse rakendamise seaduse eelnõule. 16.04.2018, lk 9. Kättesaadav arvutivõrgus: https://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/eelnoule_arvamuse_avaldamine_-_iks_rs_eelnou.pdf.
[281] CNIL. Le contrôle d’accès biométrique sur les lieux de travail.
[282] Määrus preambul p 90, 35 lg 3 p b ja art 35 lg 7.

kindlasti arvestada juba eelnevalt välja toodud diskrimineerimise ja identiteedivarguse riskidega. Seega tuleb tööandjal mõjuhinnangus näidata, et tema seatud eesmärke ei saavuta mõni tavaline tuvastustehnoloogia. Eelnevast tulenevalt peab töökohas biomeetrilise tuvastamise alusnorm tagama järgmist:

a. Määratlema, millised on niivõrd olulised tööandja huvid, mis lubaksid tal töötajatelt biomeetrilist tuvastamist nõuda ja;
b. Tööandja peab läbi proportsionaalsuse testi suutma demonstreerida meetme vajalikkust ja tuvastamiseks valitud füüsilise või käitumusliku omaduse sobivust tuvastamiseks ja;
c. Biomeetrilise tuvastamise viis ei tohi kedagi töötajatest diskrimineerida

C. Koostada juhend biomeetriliste andmete töötlemisest

Andmekaitse Inspektsiooni poolt tuleks luua biomeetriliste andmete töötlemise juhis, mis täpsustab nii tavaliste kui eriliigiliste biomeetriliste andmete definitsiooni Määruse artikkel 9 lg 4 alusel. Eriliigilisi biomeetrilisi andmeid tuleb näha kontekstis ja hinnata ka vastavalt kontekstile andmete töötlemise mõju privaatsusele. Õiguskaitse peaks hakkama kohe andmete kogumisest, mitte nende kasutamisest. Seega juhend peaks võtma arvesse kogutud andmete sobivust biomeetriliseks tuvastamiseks.

Arvestades eelnevat analüüsi käesolevas magistritöös tuleks biomeetrilisteks andmeteks lugeda esiteks biomeetrilised jäljendid ehk käitumuslike ja füüsiliste omaduste mõõdetavad digitaalsed esitlused. Teiseks tuleks biomeetrilisteks andmeteks lugeda ka andmekogud, mis oma struktureerituse astmelt, andmete säilitamise ajaperioodilt ja teiste olemasolevate biomeetriliste andmebaasidega ühilduvuse poolest võimaldavad väheste ressurssidega sisestada andmekogu biomeetrilise tuvastamise süsteemi. Samamoodi peaks biomeetrilisteks andmeteks lugema füüsiliste või käitumuslike omaduste andmekogud, mis iseseisvalt ei erista konkreetset isikut teistest, kuid kombineeritult muu infoga muutuvad vahelüliks füüsilise isiku identiteedil ja muul infol.

Online analüütika tööriistade puhul peaks juhend täpsustama vahet kasutajakogemuse analüüsil ja biomeetrilisel tuvastamisel. Sealjuures tuleb rõhutada andmekaitse mõjuhinnangu läbiviimisel vastutava töötleja kohustust hinnata kasutatavate analüütika tööriistade koosmõju füüsilise isiku privaatsusele. Vastasel korral võib tulemuseks olla, et luuakse biomeetriliste

jäljendite andmebaase, kuid neid ei ole kaitstud samal tasemel nagu tuvastustehnoloogias kasutatavad jäljendid.

Täiendused juhendis on vajalikud, sest Määruse artiklid 4 p 14 ja 9 lg 1 biomeetrilistest andmetest on liiga kitsad, et kaitsta andmesubjektide põhiõigusi uutest tehnoloogiatest tulenevate ohtude eest. Määruse grammatilisel tõlgendamisel jõuab tulemusele, nagu biomeetrilised andmed oleks vaid üks ühele võrdlemisega tuvastustehnoloogias kasutatavad andmed. See aga ei vasta EK ega EIKi praktikale ning ei vasta ka tehnoloogia kasutusviisidele praktikas. Ilma vastava lisata definitsioonile jääks andmesubjektide privaatsus suures osas kaitsmata. See on ka põhjus, miks nii paljud õigusteadlased on ühel nõul, et Määrus ei ole lahendanud biomeetriliste andmete probleemi efektiivselt.[283]

Vastutaval töötlejal ei pruugi olla kavatsust kasutada kogutavaid andmeid biomeetriliseks tuvastamiseks ja seega Määruse järgi võib seda lugeda kui, et vastutav töötleja ei pea alluma eriregulatsioonile. Samal ajal süstemaatiline inimeste füüsiliste või käitumuslike andmete kogumine tähendab, et keegi saab alati kasutada loodud andmebaasi otsinguteks, andmebaas on osaliselt või tervenisti ligipääsetav kolmandatele isikutele ja seda võib, kas seaduslikult või ebaseaduslikult kasutada tuvastamiseks.

3.4. Peatüki kokkuvõte

Magistritöö kolmandas osas analüüsiti biomeetriliste tehnoloogiate nö halli ala, kus tavalised isikuandmed võivad töötlemise käigus muutuda eriliigilisteks biomeetrilisteks andmeteks. Selleks vaadati lähemalt asjade interneti seadmeid ja *online* käitumispõhiseid analüütika tööriistu. Analüüsi eesmärgiks oli leida, millest vastutav töötleja peab lähtuma õigusliku aluse valikul, kui töötleb biomeetrilisi andmeid keerulistes andmetöötlussüsteemides. Seejärel selgitas autor, millised on võimalikud õiguslikud alused. Osa lõpetuseks kinnitas autor magistritöö alguses esitatud hüpoteesi tõele vastavust. Magistritöö hüpotees oli, et Eesti õiguses on vaja sätestada Määrusest täpsem regulatsioon eriliigiliste biomeetriliste isikuandmete töötlemiseks.

Esiteks leidis autor, et asjade internetis inimese füüsiliste või käitumuslike omaduste töötlemine vastab Määruse artikkel 4 p 14 biomeetriliste andmete definitsioonile. Autor on

[283] Kindt 2018; Jasserand; P. de Hert, V. Papakonstantinou.

arvamusel, et vastutav töötleja peab eeldama, et igasugune biomeetriliste tunnuste kogumine või töötlemine asjade interneti vahendusel võimaldab inimese tuvastamist tema füüsiliste ja käitumuslike omaduste põhjal. Määruse preambuli järgi on eriliigilisste isikuandmete klassifikatsioonil määrav kontekst. Autor leiab, et asjade internet annab sellise konteksti biomeetrilistele andmetele ja tavalised biomeetrilised andmed muutuvad eriliigilisteks asjade internetis, kui nad osalevad struktureeritud andmebaasina suurandme- või pilvetöötluses. Sealjuures tuvastas autor senise EIKi praktika põhjal, et hindamiskriteeriumiteks on väliste identifitseerimistunnuste olemasolu, nagu hääl või sõrmejälg, biomeetriliste andmete säilitamise aeg ehk töötlemisviiside ettenähtavus ja andmete hoidmise struktureerituse aste, ehk kui vähe vaeva võtab nende ühildamine tuvastussüsteemiga.

Edasi otsis autor sobivaid õiguslikke aluseid asjade internetis eriliigiliste biomeetriliste andmete töötlemisele. Õiguslik alus võib tulla nii Määrusest kui e-privaatsuse direktiivist, mis Eesti kontekstis tähendab ESSist. E-privaatsuse direktiiv eeldab õigusliku alusena seadme kasutaja nõusolekut. Määruse ja e-privaatsuse direktiivi nõusolekule kehtivad samad tingimused, seega kui vajalik on selgesõnaline nõusolek, siis tuleb biomeetriliste andmete töötlemseks lähtuda magistritöö teises osas leitud kriteeriumitest. Samuti saab Määrust ja e-privaatsuse direktiivi kohaldada koos sõltuvalt osapoolte omavahelisest õigussuhtest ja töötlemisviisist. E-privaatsuse direktiivi kohaldatakse kui tahetakse ligipääsu otse seadmele. Määrust kohaldatakse juhtudel, kus töötlemine läheb kaugemale seadmes isikuandmete säilitamisest ja ligipääsu andmisest.

Asjade interneti tegelikkus on, et ühe seadmega võib puutuda kokku määramatu isikute ring, kelle isikuandmete töötlemiseks on vaja leida õiguslik alus. Käesolevas magistritöös uuriti vabatahtlikult kasutatavaid seadmeid, mistõttu on õiguslikuks aluseks eriliigiliste biomeetriliste andmete puhul selgesõnaline nõusolek. Vastutavateks töötlejateks võivad olla nii seadme omanik kui tootja üheaegselt. Seega peaks ka seadme omanik teavitama läheduses inimesi, et nende isikuandmeid kogutakse ja saama neilt nõusoleku. Küll aga sõltub kehtiva nõusoleku olemasolu suuresti seadme disainist, sest seadmed peaksid suutma vahet teha andmesubjektidel ja teadma, kas biomeetriliste andmete töötlemiseks on saadud nõusolek.

Seejärel uuris autor inimese käitumuslike omaduste analüüsi *online* analüütika tööriistades. Autor leidis, et esiteks loob analüütika tööriist biomeetrilise jäljendi, kui kogutud käitumuslikud andmed võimaldavad üht isikut teistest eristada. Teiseks nagu käesolevas

magistritöös läbivalt analüüsitud tuleb siingi rõhutada, et eriliigilisteks muudab biomeetrilised andmed asjaolu, kui kerge on neid kasutada vastutaval töötlejal ise või kolmandatel isikutel tuvastamiseks. Samuti nagu asjade interneti puhul, tuleb siingi jõuda järeldusele, et andmete kombineerimine erinevatest allikatest võib kergesti luua isiku biomeetrilise jäljendi. Turul on mitmeid *online* käitumise põhiseid analüütika programme erinevate eesmärkide täitmiseks. Küll aga peaksid vastutavad töötlejad jälgima, et nad ei looks klientidest detailseid biomeetriliste jäljendite kogusid, mida saaks kasutada isiku universaalseks tuvastamiseks teistes süsteemides. Eelnevast tulenevalt peab vastutav töötleja sobiva analüütika programmi valimisel hindama juba kasutuses olevate programmide ja uue programmi koosmõju ja tagajärgi andmesubjektile. *Online* käitumise põhine profiili loomine on Määruse mõistes profiilianalüüs ja vastutav töötleja peaks lähtuma artiklist 22. Küll aga võib sõltuvalt kogutavate andmete hulgast ja viisist olla üheaegselt tegu ka biomeetriliste andmete töötlemisega. Sellisel juhul tuleb ikkagi lähtuda artiklist 22. Kui aga profiilianalüüsi viisi tõttu selgub, et töödeldakse eriliigilisi biomeetrilisi andmeid, siis on töötlemise õiguslikeks alusteks vaid andmesubjekti selgesõnaline nõusolek või avalik huvi.

Magistritöö lõpetuseks esitas autor ettepanekud, millega alustada Eestis biomeetriliste andmete töötlemise kontekstis inimeste põhiõiguste kaitse tagamist. Eelkõige õigust eraelu kaitsele, inimväärikusele, autonoomsust teha enda kohta otsuseid ja õigust informatsioonilisele enesemääramisele. Andmete minimaalsuse põhimõttest ja isikuandmete turvalisusest lähtudes tuleks imperatiivse normiga sätestada:

a. Biomeetriliste andmete kasutamine tuvastustehnoloogiates on lubatud ainult biomeetrilise jäljendi abil.
b. Biomeetrilised tuvastustehnoloogiad peavad võimaldama luua mitu erinevat jäljendit ühest ja samast isiku füüsilisest või käitumuslikust omadusest.

Autor on ka arvamusel, et tööandja vara kaitseks või muude tööandja oluliste huvide kaitseks tuleks eriliigiliste biomeetriliste andmete töötlemiseks ette näha normatiivaktis üldine alusnorm biomeetrilise tuvastustehnoloogia kasutamiseks töökohas. Selline alusnorm peaks tagama järgmist:

a. Määratlema, millised on niivõrd olulised tööandja huvid, mis lubaksid tal töötajatelt biomeetrilist tuvastamist nõuda ja;

b. Tööandja peab läbi proportsionaalsuse testi suutma demonstreerida meetme vajalikkust ja tuvastamiseks valitud füüsilise või käitumusliku omaduse sobivust tuvastamiseks ja;
c. Biomeetrilise tuvastamise viis ei tohi kedagi töötajatest diskrimineerida.

Andmekaitse Inspektsiooni poolt tuleks luua biomeetriliste andmete töötlemise juhis, mis täpsustab nii tavaliste kui eriliigiliste biomeetriliste andmete definitsiooni. Täiendused juhendis on vajalikud, sest Määruse artiklid 4 ja 9 biomeetrilistest andmetest on liiga kitsad, et kaitsta andmesubjektide põhiõigusi uutest tehnoloogiatest tulenevate ohtude eest.

Kokkuvõte

Biomeetrilised tehnoloogiad on teinud viimaste aastatega kasvuhüppe ja omandanud mitmes valdkonnas keskse arengusuuna. Biomeetriliste tehnoloogiate abil avatakse mobiiltelefone, autoriseeritakse makseid, tuvastatakse ligipääsuõigus töökohas ja luuakse uusi analüütika tööriistu turundajatele ja tootejuhtidele. Andmekaitse reformi paketi raames lisati biomeetrilised isikuandmed *expressis verbis* Määruse eriliigiliste isikuandmete nimekirja artiklis 9 lg 1. Samal ajal Määrus ei toonud biomeetrilisi isikuandmeid eriliigiliste isikuandmete nimekirja absoluutsel kujul, vaid jaotab biomeetrilised andmed kaheks: tavalised isikuandmed ja eriliigilised isikuandmed. Eriliigiliste biomeetriliste andmete töötlemisele kohalduvad kitsamad õiguslikud alused, kui tavalistele. Samas on jäetud kahe isikuandmete klassifikatsiooni erinevus mitmeti mõistetavaks ja lõplik vastutus isikuandmete õige liigitamise üle lasub vastutaval töötlejal. Vahe tegemine, kas biomeetriliste andmete puhul on tegemist tavaliste või eriliigiliste isikuandmetega, on oluline vastutavale töötlejale töötlemiseks õigusliku aluse valikul.

Seetõttu uuris käesolev magistritöö, kuidas vastutav töötleja peaks valima sobiva õigusliku aluse eriliigiliste biomeetriliste andmete töötlemiseks erasektoris. Täpsemalt oli fookuses õigusliku aluse valik olukorras, kus vastutav töötleja soovib vabatahtlikult pakkuda või kasutada biomeetrilist tuvastamist. Magistritöö hüpotees oli, et Eesti õiguses on vaja sätestada Määrusest täpsem regulatsioon eriliigiliste biomeetriliste isikuandmete töötlemiseks. Magistriöös otsiti vastust järgmistele küsimustele:

1. Mis on biomeetrilised isikuandmed Määruse mõistes?
2. Millal on biomeetriliste andmete puhul tegemist eriliigiliste isikuandmetega ja millal mitte?
3. Milline õiguslik alus on vastutavale töötlejale potentsiaalselt kõige sobivam eriliigiliste biomeetriliste andmete töötlemiseks erinevate valdkondade lõikes?
4. Millistele tingimustele peab vastama andmesubjekti selgesõnaline nõusolek biomeetriliste andmete töötlemiseks?
5. Kas ja kuidas oleks vaja täiustada Eesti õigust biomeetriliste andmete töötlemise seisukohalt?

Magistritöö esimeses osas otsiti vastust küsimusele, mis on biomeetrilised isikuandmed Määruse mõistes. Selleks analüüsis autor Määruse artikkel 4 p 14 biomeetriliste andmete definitsiooni nelja elementi:

a. isikuandmed;
b. konkreetse tehnilise töötlemise abil saadavad isikuandmed;
c. füüsilise isiku füüsilised, füsioloogilised ja käitumuslikud omadused;
d. isikuandmed, mis võimaldavad kõnealust füüsilist isikut kordumatult tuvastada või kinnitavad selle füüsilise isiku tuvastamist.

Artikkel 4 definitsiooni paremaks mõistmiseks pani autor esiteks Määruse biomeetriliste andmete mõiste perspektiivi üldtuntud biomeetriliste andmete tunnustega. Biomeetriliste andmete üldisteks tunnusteks on universaalsus, püsivus ja unikaalsus. Need tunnused ongi biomeetriliste tehnoloogiate riskide põhjuseks, mistõttu on biomeetrilised andmed leidnud koha Määruse eriliigiliste isikuandmete nimekirjas. Universaalsus tähendab, et tunnus esineb piisavalt paljudel inimestel, et võrdlemine oleks võimalik. Püsivus tähendab, et tunnus peab olema ajas suhteliselt muutumatu ehk stabiilne. Biomeetrilised andmed peavad biomeetrilistes süsteemides kasutamiseks olema ka igale inimesele unikaalsed või vähemalt eristatavad. Samal ajal jätavad sellised andmed jälgi, nagu sõrmejäljed klaasil, või on kergelt kättesaadavad fotode kujul internetis, mistõttu on identiteedivarguse risk kõrge. Samuti sisaldavad biomeetrilised omadused nii genotüübi, rassi, etnilise päritolu kui haiguste infot, mistõttu on ka diskrimineerimise oht kõrge.

Järgnevalt leidis autor, et inimese füüsilised ja käitumuslikud omadused on Määruse järgi isikuandmed. Teine biomeetriliste andmete definitsiooni element „konkreetse tehnilise töötlemise abil saadavad isikuandmed“ on üks ebaselgemaid definitsiooni osasid. Määrus ei täpsusta, mida mõeldakse biomeetriliste andmete definitsioonis konkreetse tehnilise töötlemise all kui ainult, et selle eesmärk on isik tuvastada. Biomeetrilised andmed on sellepoolest väga erinevad teistest isikuandmetest, et nende klassifikatsioon sõltub puhtalt töötlemise viisist ja kasutatavatest tehnilistest vahenditest. Autor jõudis seisukohale, et Määruse kriteeriumiga konkreetsest tehnilisest töötlemisest on eelkõige peetud silmas välistada biomeetriliste andmete definitsioonist tavaline ja väikesemahulise töötlemine, nagu ajalehes piltide avaldamine. Seega tuleb autori hinnangul lugeda Määruse biomeetriliste andmete konkreetse tehnilise töötlemise tingimus täidetuks, kui töödeldakse inimese füüsilisi ja käitumuslikke omadusi tehniliste vahenditega viisil, kus biomeetrilised omadused tehakse tehniliselt mõõdetavaks ja inimeste vahel võrreldavaks. Samuti loeb autor konkreetseks tehniliseks töötlemiseks olukorrad, kus luuakse biomeetrilistest tunnustest andmekogusid, mis mõistliku vaevaga võimaldavad isikut grupist eraldada ja millel on oht tekitada andmesubjektile olulist kahju.

Kolmas definitsiooni element „isikuandmed füüsilise isiku füüsiliste, füsioloogiliste ja käitumuslike omaduste kohta“ on lai valik mõõdetavatest inimese tunnustest. Käitumuslikeks tunnusteks on näiteks hääl, allkiri, rüht või ka tegevuste sooritamise strateegia. Küll aga ollakse nii õiguskirjanduses kui Artikkel 29 Töörühma poolt arvamusel, et inimese füüsilisi ja füsioloogilisi tunnuseid võib kasutada sünonüümidena.

Määruse artikkel 4 definitsiooni osa „isikuandmed, mis võimaldavad kõnealust füüsilist isikut kordumatult tuvastada või kinnitavad selle füüsilise isiku tuvastamist“ on võtmekriteerium biomeetriliste andmete eriliigilisteks isikuandmeteks kvalifitseerimisel. Artikkel 9 lg 1 järgi on keelatud töödelda füüsilise isiku kordumatuks tuvastamiseks kasutatavaid biomeetrilisi andmeid. „Kordumatu tuvastamise“ kriteeriumit Määrus ei selgita ja seetõttu uuris autor, mida selle termini all mõeldud on. Autori hinnangul võib väita, et biomeetriliselt süsteemilt eeldatakse isiku eristamist grupist tema biomeetriliste tunnuste põhjal ja seda eristusvõimet hinnatakse kontekstis. Teisest küljest on biomeetrilised süsteemid tuntud oma ebatäpsuse poolest ja seega ei suuda ükski biomeetriline süsteem garanteerida alati kordumatut tuvastamist. Autor leidis, et silmas tuleb pidada Määruse tehnoloogilist neutraalust ja seega ei tohiks ennetavalt välistada ühtegi biomeetrilisi süsteemi tulenevalt sooritusest. Sealjuures tuleks arvestada ka, et biomeetrilised tunnused kannavad teatud vahelüli rolli isiku identiteedi ja teiste andmebaaside vahel. Näiteks tudengiorganisatsiooni andmebaas suurest hulgast liikmete fotodest võib olla biomeetrilised andmed, kui andmebaasi on kerge kombineerida õiguskaitseorganite tuvastussüsteemidega. Teisisõnu hinnata tuleks, kui tõenäoline on kasutatava tehnoloogia olemust arvestades, et biomeetriliste andmete põhjal saab isikut tulevikus tuvastada kombineerituna muu informatsiooniga, mis iseseisvalt kedagi automaatselt ei tuvastaks.

Seejärel leidis autor vastuse, kuidas eristada eriliigilisi ja nn tavalisi biomeetrilisi andmeid. Eriliigilised isikuandmed on isikuandmete grupp, mis vajab kõrgemat kaitset tagajärgede tõttu, mida nende väärkasutamine võib endaga kaasa tuua. Biomeetrilised andmed on Määruse järgi eriliigilised isikuandmed vaid siis, kui neid kasutatakse konkreetsete tehniliste vahenditega füüsilise isiku kordumatuks tuvastamiseks. Teisisõnu teeb Määrus vahet biomeetriliste andmete omamisel ja kasutamisel. Sellegipoolest näitavad EIKi lahendid, kui ohtlikuks eraelu puutumatusele loeb EIK biomeetrilisi andmebaase olenemata nende võimalikest kasutusviisidest. Sellega peaks arvestama vastutav töötleja, kui kaalub kas tema töödeldavad biomeetrilised andmed käivad artikkel 9 eriliigiliste isikuandmete nimekirja või mitte. Ei saa eirata asjaolu, et Määruse teksti autorid on püüdnud eristada artikleid 4 ja 9. Seega autor jõudis

järeldusele, et artikkel 4 p 14 biomeetriliste andmete määratlus võib hõlmata laia valikut biomeetriliste tunnuste ettevalmistust tuvastamiseks ja biomeetrilisi andmebaase. Artikkel 9 kohaldamine eeldab, kas biomeetriliste andmete otsest kasutamist füüsilise isiku tuvastamiseks või kui eesmärk ei ole tuvastamine, siis tuleb vastutaval töötlejal leida piir, kus andmebaaside loomise eesmärk ja kasutamise viis rikuvad oluliselt andmesubjekti eraelu puutumatust.

Õigusliku aluse valikul saab probleemiks asjaolu, et enamasti on biomeetriliste andmete töötlemine hall ala, kus õigusliku aluse valik sõltub igal üksikul juhul suuresti töötlemise viisist ja eesmärgist. Vastutaval töötlejal on võimalik valida nn tavaliste biomeetriliste andmete puhul õiguslik alus Määruse artiklist 6, artiklist 9 eriliigiliste biomeetriliste andmete puhul ja artiklist 22 biomeetriliste andmete kasutamisel profiilianalüüsiks.

Seejärel otsis autor vastust küsimusele, milline õiguslik alus on vastutavale töötlejale potentsiaalselt kõige sobivam eriliigiliste biomeetriliste andmete töötlemiseks erinevate valdkondade lõikes. Kuna biomeetriliste andmete klassifikatsioon sõltub kontekstist, siis asetas autor biomeetrilist andmetöötlust eri kontekstidesse, et leida ühised jooned isikuandmete muutumisel biomeetrilisteks andmeteks ja edasi eriliigilisteks isikuandmeteks. Täpsemalt analüüsiti biomeetrilist tuvastamist finantsteenuste osutamisel, töökohas, asjade internetis ja *online* käitumispõhistes analüütika tööriistades. Sealjuures tõi autor igas valdkonnas välja õiguslike aluste võrdluse.

Finantsteenuste valdkonnas analüüsiti Määruse ja PSD2 kooskõla. PSD2 kohustab finantsteenuse osutajaid kasutama enamus elektrooniliste maksete jaoks mitmefaasilist tuvastamist, millest üks etapp on biomeetriline tuvastamine. Autor leidis, et nii PSD2 kui Määrus näevad sobiliku õigusliku alusena andmesubjekti selgesõnalist nõusolekut, kuid lähtuda tuleb Määruse selgesõnalise nõusoleku tingimustest kui *lex generalisest*. Samuti kui vastutav töötleja soovib vabatahtlikult pakkuda kliendile biomeetrilise autentimise võimalust, tuleb küsida kliendilt selgesõnalist nõusolekut Määruse artikkel 9 lg 2 p a järgi.

Töökohas eriliigiliste biomeetriliste andmete töötlemise puhul leidis autor, et tööandjal ei ole praktiliselt võimalik kasutada biomeetrilist tuvastamist töökohas, sest ainus alus selleks saaks olla töötaja selgesõnaline nõusolek. Töötaja selgesõnalise nõusoleku kehtivust eriliigiliste isikuandmete töötlemisel on aga ääretult keeruline tõendada. Autor tuvastas, et hetkel ei ole Eesti õiguses alusnormi, mis lubaks tööandjal oma vara kaitseks või muudel põhjustel kasutada biomeetrilist tuvastustehnoloogiat.

Biomeetrilised tunnused on vabalt püütavad erinevate sensoritega või laialt kättesaadavad internetist. Määrus näeb ühe eriliigiliste isikuandmete töötlemise alusena ka asjaolu, kui andmesubjekt on ise oma isikuandmed avalikustanud. Seetõttu täpsustas autor, millised on vastutava töötleja võimalused kasutada andmesubjekti poolt avalikustatud biomeetrilisi andmeid ja millal on vaja küsida andmesubjekti selgesõnalist nõusolekut biomeetriliste andmete edasiseks töötlemiseks. Andmesubjekti poolt avalikustatud biomeetriliste andmete kontekstis jõudis autor nii Eesti kui EIKi ja EK kohtupraktika põhjal järeldusele, et andmesubjekti poolt avalikustatud isikuandmete edasine kasutamine on äärmiselt kitsalt piiritletud. Vastutav töötleja peab arvesse võtma töötlemise struktureerituse astet, konteksti muutust, töötlemise intensiivsust ja asjaolu, kui ettenähtav edasine töötlemine kavandataval viisil andmesubjektile oma isikuandmete avalikustamise hetkel oli. Teisisõnu kui sotsiaalmeediast või veebilehtedelt saadud biomeetrilistest andmetest luuakse põhjalik struktureeritud andmebaas, siis ei või vastutav töötleja tugineda enam Määruse avalikustamise erandile, vaid peab küsima andmesubjektilt selgesõnalist nõusolekut.

Asjade interneti kontekstis leidis autor, et inimese füüsiliste või käitumuslike omaduste töötlemine vastab Määruse biomeetriliste andmete definitsioonile. Vastutav töötleja peab eeldama, et igasugune biomeetriliste tunnuste kogumine või töötlemine asjade interneti vahendusel võimaldab inimese tuvastamist tema füüsiliste ja käitumuslike omaduste põhjal. Autor leidis, et asjade internet annab sellise konteksti biomeetriliste andmete töötlemisele, et need muutuvad eriliigilisteks isikuandmeteks, kui nad osalevad struktureeritud andmebaasina suurandme- või pilvetöötluses. Sealjuures tuvastas autor senise EIKi praktika põhjal, et hindamaks tehnoloogia mõju biomeetriliste andmete muutumisele eriliigilisteks isikuandmeteks, tuleb hinnata järgmisi kriteeriumie: universaalsete ja püsivate väliste identifitseerimistunnuste olemasolu, nagu hääl või sõrmejälg; biomeetriliste andmete säilitamise aeg ehk töötlemisviiside ettenähtavus; isikuandmete hoidmise struktureerituse aste, ehk kui vähe vaeva võtab nende ühildamine tuvastussüsteemiga. Õiguslik alus asjade internetis biomeetriliste andmete töötlemisele võib tulla nii Määrusest kui e-privaatsuse direktiivist, mis Eesti kontekstis tähendab ESSi. E-privaatsuse direktiiv eeldab õigusliku alusena seadme kasutaja nõusolekut. Määruse ja e-privaatsuse direktiivi nõusolekule kehtivad samad tingimused.

Inimeste internetikäitumise jälgimise kontekstis uuris autor, millal on tegemist profiilianalüüsi ja käitumuslikel andmetel põhineva biomeetrilise tuvastamisega. Nagu eelnevalt leitud tuleb siingi rõhutada, et eriliigilisteks muudab biomeetrilised andmed asjaolu, kui kerge on neid

kasutada vastutaval töötlejal ise või kolmandatel isikutel tuvastamiseks. Nagu asjade interneti puhul, tuleb siingi jõuda järeldusele, et andmete kombineerimine erinevatest allikatest võib kergesti luua isiku biomeetrilise jäljendi. Turul on mitmeid *online* käitumise põhiseid analüütika programme erinevate eesmärkide täitmiseks, mis töötlevad korraga kümneid või ka sadu inimese kognitiivseid ja psühholoogilisi parameetreid. Vastutavad töötlejad peaksid jälgima, et nad ei looks klientidest detailseid biomeetriliste jäljendite kogusid, mida saaks kasutada isiku universaalseks tuvastamiseks teistes süsteemides. Seetõttu peab vastutav töötleja sobiva analüütika programmi valimisel hindama ka juba kasutuses olevate programmide ja uue programmi koosmõju ja tagajärgi andmesubjektile.

Online käitumise põhine profiili loomine on Määruse mõistes profiilianalüüs ja vastutav töötleja peaks lähtuma artiklist 22. Küll aga võib sõltuvalt kogutavate andmete hulgast ja viisist olla üheaegselt tegu ka biomeetriliste andmete töötlemisega. Sellisel juhul tuleb ikkagi lähtuda artiklist 22. Kui aga profiilianalüüsi viisi tõttu selgub, et töödeldakse eriliigilisi biomeetrilisi andmeid, siis on töötlemise õiguslikeks alusteks vaid andmesubjekti selgesõnaline nõusolek või avalik huvi.

Autor leidis vastuse ka küsimusele millistele tingimustele peab vastama andmesubjekti selgesõnaline nõusolek biomeetriliste andmete töötlemiseks. Andmesubjekti nõusolek on vabatahtlik, konkreetne, teadlik ja ühemõtteline tahteavaldus. Selleks, et eriliigiliste biomeetriliste andmete töötlemiseks antud nõusolek oleks vabatahtlik peab tuvastamiseks salvestama seadmes vaid biomeetrilise jäljendi, mitte originaalkujutist. Kasutatav tehnoloogia peab võimaldama ühest füüsilisest või käitumuslikust omadusest luua mitu erinevat biomeetrilist jäljendit ja biomeetrilisele tuvastustehnoloogiale tuleb anda alternatiive, mis oleks sama turvalised, näiteks PIN kood. Nõusolek on konkreetne ja teadlik, kui kasutatav biomeetrilise tuvastamise meetod vastab andmesubjekti ootustele, ehk andmesubjekti teavitatakse süsteemi veamäärast, süsteem on piisavalt täpne isiku tuvastamiseks ja tuvastamiseks valitud käitumuslikud või füüsilised tunnused ei diskrimineeri süsteemi kasutajat.

Magistritöö lõpetuseks kinnitab autor magistritöö alguses esitatud hüpoteesi tõele vastavust. Magistritöö hüpotees oli, et Eesti õiguses on vaja sätestada Määrusest täpsem regulatsioon eriliigiliste biomeetriliste isikuandmete töötlemiseks. Määrus ei ole saavutanud harmoniseerimise eesmärki biomeetriliste isikuandmete vallas ega andmesubjektide piisavat kaitset. Samas annab Määrus liikmesriikidele mitu võimalust näha ette Määrusest erinevaid

eeskirju ja õigusakte biomeetriliste andmete kontekstis. Autor esitas ettepanekud millega alustada Eestis biomeetriliste andmete erasektoris töötlemise kontekstis inimeste põhiõiguste kaitse tagamist. Eelkõige õigust eraelu kaitsele, inimväärikusele, autonoomsust teha enda kohta otsuseid ja õigust informatsioonilisele enesemääramisele.

Andmete minimaalsuse põhimõttest ja isikuandmete turvalisusest lähtudes tuleks imperatiivse normiga sätestada:

a. Biomeetriliste andmete kasutamine tuvastustehnoloogiates on lubatud ainult biomeetrilise jäljendi abil.
b. Biomeetrilised tuvastustehnoloogiad peavad võimaldama luua mitu erinevat jäljendit ühest ja samast isiku füüsilisest või käitumuslikust omadusest.

Autor on ka arvamusel, et tööandja vara kaitseks või muude tööandja oluliste huvide kaitseks tuleks eriliigiliste biomeetriliste andmete töötlemiseks ette näha normatiivaktis üldine alusnorm biomeetrilise tuvastustehnoloogia kasutamiseks töökohas. Selline alusnorm peaks tagama järgmist:

a. Määratlema, millised on niivõrd olulised tööandja huvid, mis lubaksid tal töötajatelt biomeetrilist tuvastamist nõuda ja;
b. Tööandja peab läbi proportsionaalsuse testi suutma demonstreerida meetme vajalikkust ja tuvastamiseks valitud füüsilise või käitumusliku omaduse sobivust tuvastamiseks ja;
c. Biomeetrilise tuvastamise viis ei tohi kedagi töötajatest diskrimineerida.

Andmekaitse Inspektsiooni poolt tuleks luua biomeetriliste andmete töötlemise juhis, mis täpsustab nii nn tavaliste kui eriliigiliste biomeetriliste andmete definitsiooni. Täiendused juhendis on vajalikud, sest Määruse artiklid 4 ja 9 biomeetrilistest andmetest on liiga kitsad, et kaitsta andmesubjektide põhiõigusi uutest tehnoloogiatest tulenevate ohtude eest. Biomeetrilisteks andmeteks tuleb lugeda ka andmekogud, mis oma struktureerituse astmelt, andmete säilitamise ajaperioodilt ja teiste olemasolevate biomeetriliste andmebaasidega ühilduvuse poolest võimaldavad vastutaval töötlejal või kolmandatel isikutel füüsilisi isikuid vähese vaevaga tuvastada. *Online* analüütika tööriistade puhul peaks juhend täpsustama vahet kasutajakogemuse analüüsil ja biomeetrilisel tuvastamisel ning vastutava töötleja kohustust hinnata erinevate analüütika tööriistade koosmõju biomeetrilise tuvastamise perspektiivist.

Legal basis for processing special categories of biometric data in private relations

Abstract

Biometric technologies have made growth spun in recent years and gained a centre direction of development in many sectors. Biometric technologies enable to Access mobiile phones, authorise payments, identify access rights at workplace and create new analytics tools for marketers and product owners. With data protection reform biometric data was added *expressis verbis* to the list of special categories of data in the Regulation (EU) 2016/679 Article 9(1). at the same time the Regulation did not bring biometric data to the list of special categories of data in an absolute form, but divided biometric data into two: ordinary personal data and special categories of personal data. Processing of special categories of personal data is Under stricter rules regarding legal basis than ordinary personal data. However, the distinction between two types of personal data has been left open to interpretations and the final responsibility for the correct classification lies with data controller. Differentiating whether biometric data are ordinary or special categories of personal data is important for data controller when choosing the legal basis.

Therefore, the master's thesis researched how data controller should choose suitable legal basis for processing special categories of biometric data in private sector. More specifically, focus was on the choice of legal basis in the situation where data controller wishes to offer or use biometric identification voluntarily. The hypothesis of master's thesis was that Estonian law needs to prescribe more detailed regulation for processing special categories of biometric data that in the Regulation. Master's thesis searched answers for following questions:

1. What are the biometric data in the meaning of Regulation?
2. When are biometric data considered special categories of data and when not?
3. What are the potentially suitable legal basis for processing special categories of biometric data in different domains in the perspective of data controller?
4. Which conditions must satisfy the explicit consent of data subject for processing biometric data?
5. If and how should Estonian law be improved in the context of processing biometric data?

In the first part of the master' s thesis the author searched answer to the question, what are the biometric data in the meaning of Regulation. Therefore, the author analysed the four elements of definition of biometric data in the Article 4(14):

a. personal data;
b. personal data resulting from specific technical processing;
c. personal data relating to the physical, physiological or behavioural characteristics of a natural person;
d. personal data which allow or confirm the unique identification of that natural person.

For better understanding of Article 4 definition, the author put the meaning of biometric data in the Regulation into context with generally known characteristics of biometric data. The general characteristics of biometric data are universality, permanence and uniqueness. These characteristics are the reason behind risks associated with biometric data and the reason biometric data have found a place in the list of special categories of data. Universality means that the characteristic is present in a lot of people, so that comparing would be possible. Permanence means that the characteristic has to stay relatively unchanged in time, i.e. stable. To use in biometric systems, biometric data has to also be unique for each individual or at least distinctive. At the same time such characteristics leave traces, such as fingerprints on a glass, or they are easily accessible through photos on the Internet, which gives rise to the risk of identity theft. Also, biometric data contains information about person's genotype, race, ethnic origin and health which also increases the risk of discrimination.

In the following, the author reached to conclusion that person's physical and behavioural characteristics are personal data in the meaning of the Regulation. The second element of the definition of biometric data "personal data resulting from specific technical processing" is one of the most unclear parts of the definition. The Regulation does not specify what is meant by specific technical processing in the definition of biometric data, only to uniquely identify a person. Biometric data differ from other types of personal data in a way that their classification depends solely on the manner of processing and technical means used. Author reached a conclusion that by the condition of specific technical processing in the Regulation it is foremost meant to exclude ordinary and small scale processing, such as publishing photos on newspapers. Therefore, in the opinion of the author the condition of specific technical processing must be regarded satisfied if person's physical and behavioural characteristics are processed by technical means in a manner that biometric characteristic are made measurable and comparable. Also, the author considers specific technical processing situations where databases are created from biometric characteristics that with reasonable effort enable to separate a person from a group and which threatens to cause significant harm to data subject.

Third element of the definition “data relating to the physical, physiological or behavioural characteristics of a natural person” is a wide selection of measurable human characteristics. Behavioural characteristics are for example voice, signature, gait or strategy of activity performance. However, according to legal literature and Article 29 Working Party opinions, person’s physical and physiological characteristics may be used as synonyms.

“Personal data which allow or confirm the unique identification of that natural person” of Article 4 definition of the Regulation is a key criteria for qualifying biometric data as special categories of personal data. According to Article 9 (1) it is prohibited to process biometric data for the purposes of uniquely identifying a natural person. Term “uniquely identifying” is not explained in the Regulation and, thus, the author analysed what is meant by this term. In the opinion of the author it could be said that it is expected from a biometric system to separate a person from a group based on his/her biometric characteristics and that ability to separate is assessed in a context. On the other hand, biometric systems are known to be inaccurate and, therefore, no biometric system can guarantee to always uniquely identify. Author found that the technological neutrality of the regulation should be taken into consideration and, therefore, no biometric system should be pre-emptively excluded based on system performance. Also, it should be taken into consideration that biometric characteristics carry a certain link between the identity of a natural person and other databases. For example, a student organisation’s database of its members’ photos may be biometric data if the database is easily combined with a law enforcement recognition systems. In other words, it should be assessed how likely it is considering the nature of used technology that a person will be identified based on his/her biometeid data in the future when combined with other information which would not identify anyone independently automatically.

Then, the author found an answer to how to differentiate special categories and so called ordinaru biometeic data. Special categories of data are a group of personal data that needs a higher protection due to consequences its abuse would bring. Biometric data according to the Regulation are special categories of personal data only if they are used by specific technical means fo the purposes of uniquely identifying a natural person. In other words, the regulation differentiates between owning and using biometric data. Nevertheless, the court practice of European Court of Human Rights show how dangerous for private life the European Court of Hman Rights considers biometric databases regardless their possible uses. Data controller should take that into account when deciding whether biometric data it processes fall in the list of special categories of personal data of Article 9or not. It cannot be ignored that the authors

of the text of the Regulation have tried to differentiate Articles 4 and 9. Therefore, the author reached a conclusion that the Article 4 (14) biometric data may include a variety of ways to prepare biometric characteristics to identification and variety of biometric databases. Implementing Article 9 presumes that biometric data are directly used to identify a natural person or if the purpose is not identification, then data controller must find a line where the purpose of creating databases and the manner of use significantly infringe the private life of data subject.

When choosing a legal basis, it becomes problematic that mostly processing of biometric data is a grey area where the choice of legal basis in every single time mostly depends on the manner of processing and the purpose. Data controller may choose a legal basis for so called ordinary biometric data from Article 6, from Article 9 if it is special categories of biometric data and from Article 22 in case of profiling.

Then the author searched an answer to the question, what are the potentially suitable legal bases for processing special categories of biometric data in different domains in the perspective of data controller. Since the classification of biometric data depends on the context, the author looked at biometric processing in different domains to find common traits when personal data transforms into biometric data and from there to special categories of data. Specifically, author analysed biometric identification for financial services, at workplace, in the internet of things and in the online behavioural analytics tools. The author also brought up a comparison of legal bases in all of these domains.

Conformity of the Regulation and PSD2 was analysed in the finance sector. PSD2 obliges the financial service provider to use multifactor authentication for most electronic payments from which biometric identification is one of the steps. Author found that PSD2 and the Regulation both see explicit consent as a suitable legal basis, but the Regulation takes preference since it is a *lex generalis*. Also, if data controller wishes to offer client voluntarily an option of biometric identification then explicit consent from Article 9 (2)(a) must be asked from the client.

In the case of processing special categories of biometric data at workplace, the author found that it is practically not possible for the employer to use biometric identification at workplace, because the only legal basis for it could be the explicit consent of the employee. Proving the validity of employees' explicit consent for processing special categories of personal data is extremely difficult. The author established that Estonian law at the moment lacks a general

norm which would allow employer to use biometric identification technology for the purposes of protecting its assets or for other substantial reasons.

Biometric characteristics are easily caught via different sensors or they are widely accessible via the Internet. The Regulation prescribes as one of the legal basis for processing special categories of biometric data the fact that data subject has made his/her personal data manifestly public. For this reason. The author specified what are the data controller's possibilities to use biometric data made public by the data subject and when an explicit consent from data subject is needed for further processing of biometric data. In the context of biometric data made public by the data subject the author reached a conclusion based on Estonian and European Court of Human Rights and the Court of Justice of the European Union court practice that the basis of personal data made public by the data subject is very narrow. Data controller must take into account the level of structuring, change of context, intensity of processing and the fact of how foreseeable further processing in the planned way was for data subject at the moment of making his/her personal data public. In other words, if a detailed structured database is created based on data acquired from social media or other websites then data controller may no longer rely on the exemption of publishing personal data in the Regulation, but has to acquire an explicit consent from data subject.

In the context of internet of things, the author found that processing of person's physical or behavioural characteristics corresponds to the definition of biometric data of the Article 4(14) of the Regulation. Data controller must assume that any collection of or processing of biometric characteristics through the internet of things enables identification of an individual based on his/her physical and behavioural characteristics. The author found that the internet of things gives the processing of biometric data such context which turns them into special categories of personal data if they participate in big data or cloud computing processing as a structured database. The author also found that when assessing the impact of technology on the transformation of biometric data to special categories of personal data the following criteria from the court practice of European Court of Human Rights must be assessed: presence of universal and permanent outward signs of identification like voice or fingerprint; the time of keeping biometric data, e.g. foreseeability of the ways of processing; the level of structure, e.g. how little effort it takes to integrate with an identification system. Legal basis to process biometric data in the internet of things may come from the Regulation or the e-privacy directive which in Estonia has been taken over as ESS. The e-privacy directive prescribes a legal basis

as consent of the user of a device. The same conditions apply to the consent from the Regulation and from the e-privacy directive both.

In the context of internet behaviour surveillance the author analysed the difference between profiling and biometric identification based on behavioural biometric data. As previously concluded, it must be emphasised here as well that biometric data is transformed into special categories of personal data by the fact how easily data processor or third party may use them for identification. As in the case of the internet of things it must be concluded here that combining data from different sources might easily create a biometric template. There are many online behavioural analytics tools on the market for different purposes which process tens or even hundreds of person's cognitive and psychological parameters at the same time. Data controllers should be aware that they are not creating detailed databases of biometric templates which could be used to universally identify a person in other systems. Therefore, when choosing a suitable analytics tool, data controller must assess the impact on data subject of combining the new programme with programmes already in use.

Creating a profile based on online behaviour is profiling in the meaning of the Regulation and the data controller should act according to Article 22 of the regulation. However, depending on the amount and manner of data collected it could simultaneously constitute a biometric data processing. In such case Article 22 must still be taken as legal basis. If as a result of profiling it appears that special categories of biometric data are processed, then legal basis may only be explicit consent or public interest.

The author also found the answer to the question, which conditions must satisfy the explicit consent of data subject for processing biometric data. Data subject's consent is free, specific and informed act of will. In order for the consent for processing of special categories of biometric data to be free, only the biometric template may be recorded in the device, not the original source. The used technology must enable to create several biometric templates from one physical or behaviour characteristic and alternatives to the biometric identification technology must be given which would be as safe, e.g. PIN code. Consent is specific and informed if the used biometric identification method is in accordance with the expectations of the data subject, i.e. data subject is informed of system failure rate, system id precise enough to identify a person and the behavioural or physical characteristics chosen for identification do not discriminate the system user.

For the conclusion of the master's thesis the author confirms that the hypothesis is true. The hypothesis of the master's thesis was that the Estonian law needs to prescribe more detailed regulation for processing special categories of biometric data that in the Regulation. The regulation has not achieved its purpose to harmonise the member states' actions in the domain of biometric personal data and has accorded data subjects sufficient protection. At the same time the Regulation gives member states several options to prescribe rules and laws concerning biometric data that differ from the Regulation. The author suggested proposals which would commence the protection of peoples' fundamental rights in the context of processing biometric data in private sector. Foremost, the right to the protection of private life, dignity, autonomy to make decisions concerning one self and the right to informational self-determination.

According to the principle of data minimisation and the security of personal data it should be prescribed by imperative norm:

a. Use of biometric data in identification technologies should only be allowed based on biometric template.
b. Biometric identification technologies should enable to create several different biometric templates from the same physical or behavioural characteristic.

The author is also on the opinion that for the protection of employers assets or other substantial employer's interests there should be a norm in law that is a general basis for using biometric identification technology at workplace. Such norm should warrant the following:

a. determine which are the substantial employers' interests that would allow to ask biometric identification from employees and;
b. employer must be capable of proving the necessity and suitability of physical or behavioural characteristic chosen for identification through a proportionality test and;
c. the manner of biometric identification may not discriminate any employees.

Data protection supervisory authority should create guidelines on processing biometric data which specifies the definition of so called ordinary biometric data and special categories of biometric data. Specifications in the guidelines are necessary because Articles 4 and 9 of the Regulation are too narrow to protect the fundamental rights of the data subjects from threats coming from new technologies. Biometric data should also cover databases which based on their level of structure, time of recording data and ability to be integrated with other existing biometric databases enables the data controller or a third party to identify a natural person with little effort. In the case of online analytics tools the guidelines should specify the difference

between user experience analysis and biometric identification and the obligation of data controller to assess the combined impact of different analytics tools from the perspective of biometric identification.

Lühendid

1. CNIL - Commission Nationale de l'informatique et des Libertés
2. EL - Euroopa Liit
3. EK - Euroopa Kohtu
4. EIK - Euroopa Inimõiguste Kohus
5. ESS - elektroonilise side seadus
6. GIODO - Generalnego Inspektora Ochrony Danych Osobowych
7. Inimõiguste Konventsioon - Inimõiguste ja põhivabaduste kaitse konventsioon
8. ICO – Information Commissioner’s Office
9. IKS – isikuandmete kaitse seadus
10. IKS RakS - isikuandmete kaitse seaduse rakendamise seadus
11. STARR - Decision SupporT and self-mAnagement system for stRoke survivoRs
12. PSD2 - makseteenuste direktiiv (EL) 2015/2366
13. TLS - töölepingu seaduses

Kasutatud materjalid

Teaduskirjandus ja seaduseelnõud

1. Antonova, J. Isikuandmete kaitse kohtueelses kriminaalmenetluses Eestis. Magistritöö. Tartu Ülikool. Tartu 2015.
2. Barfield, W. Pagallo, U. (koost). Research Handbook on the Law of Artificial Intelligence. Cheltenham: Edward Elgar Publishing Limited 2018.
3. Edwards, L. Urquhart, L. Privacy in public spaces: what expectations of privacy do we have in social media intelligence? - International Journal of Law and Information Technology 2016, No 24, lk 279–310.
4. Goode, A. Biometrics for banking: best practices and barriers to adoption. - Biometric Technology Today 2018, No10.
5. Handbook on European Data Protection Law. Luxembourg: Publications Office of the European Union 2018.
6. Hert, P, de. Biometrics: legal issues and implications. Background paper for the Institute of Prospective Technological Studies, DG JRC – Sevilla, European Commission. Sevilla: European Communities 2005. Kättesaadav arvutivõrgus: https://pdfs.semanticscholar.org/226a/48e50f01b54b6b0e400a0a73f712877308b5.pdf. Viimati külastatud 18.04.2019.
7. Hert, P, de. Papakonstantinou, V. The new General Data Protection Regulation: Still a sound system for the protection of individuals? - Computer Law & Security Review 2016, Vol 32, No 2.
8. Hildebrandt, M. Gutwirth, S. (koost). Profiling the European Citizen. Cross-Disciplinary Perspectives. Dordrecht: Springer 2008.
9. Hoecke, M. V. (koost). Methodologies of Legal Research. Which Kind of Method for What Kind of Discipline? Oxford ja Portland, Oregon: Hart Publishing 2011.
10. Information Commissioner's Office. Big data, artificial intelligence, machine learning and data protection. *Sine loco* 2017. Kättesaadav arvutivõrgus: https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf. Viimati külastatud 18.04.2019.
11. Jasserand, C. Legal Nature of Biometric Data: From Generic Personal Data to Sensitive Data. - European Data Protection Law Review 2016/2.

12. Jones, M. L. Privacy without Screens & the Internet of Other People's Things. - Idaho Law Review 2015, Vol 51.
13. Kindt, E, J. Having yes, using no? About the new legal regime for biometric data. - Computer Law & Security Review. 2018/6, Vol 34, No 3, lk 523-538.
14. Kindt, E, J. Privacy and Data protection Issues of Biometric Applications. A Comparative Legal Analysis. Leuven: Springer 2013.
15. Kindt, E, J. The Processing of Biometric Data. A Comparative Legal Analysis with a focus on the Proportionality Principle and recommendations for a legal framework. Doctoral thesis. Leuven: Katholieke Universiteit 2012.
16. Kotsios, A. Privacy in an Augmented Reality. - International Journal of Law and Information Technology 2015, No 23, lk 157-185.
17. Krausova, A. Online Behavior Recognition: Can We Consider It Biometric Data under GDPR. - Masaryk University Journal of Law and Technology 2018, Vol 12.
18. Liu, Y. Identifying Legal Concerns in the Biometric Context. - Journal of International Commercial Law and Technology 2008, Vol 3, No 1.
19. Männiko. M. Õigus privaatsusele ja andmekaitse. Tallinn: Juura 2011.
20. Pato, J. N. Millet, L. I. (koost). Biometric Recognition. Challenges and opportunities. Whither Biometrics Committee. Washington, D. C: The National Academies Press 2010. Kättesaadav arvutivõrgus: https://dataprivacylab.org/TIP/2011sept/Biometric.pdf. Viimati külastatud 18.04.2019.
21. Pichierri, F. Dimitrova, D. Smart environments in the health context, self-management and data protection in the STARR project. - International Review of Law, Computers & Technology 2018, Vol 32:1, lk 174-189.
22. Piiskop, M.-L. Andmesubjekti isikuandmete töötlemine nõusoleku alusel. Tartu Ülikool. Magistritöö. Tallinn 2018.
23. Sanchez-Reillo, R. jt. How to implement EU data protection regulation for R&D in biometrics. - Computer Standards & Interfaces 2019, Vol 61.
24. Sedenberg, E. Wong, R. Chuang, J. A window into the soul: Biosensing in public. Surveillance, Privacy and Public Space. *Sine loco*, ArXiv 2017. Kättesaadav arvutivõrgus: https://arxiv.org/ftp/arxiv/papers/1702/1702.04235.pdf. Viimati külastatud 18.04.2019.
25. Seletuskiri isikuandmete kaitse seaduse rakendamise seaduse eelnõu juurde 778 SE. Justiitsministeerium 13.12.2018.
26. Solove, D. J. Privacy Self-Management and the Consent Dilemma. – Harvard Law Review 2013,Vol 126.

27. Velbri, S. Isikuandmete kaitse üldmäärusest tulenev nõusoleku vajadus ja selle tingimused isikuandmete töötlemisel äriühingute poolt. Tartu Ülikool. Magistritöö. Tallinn 2018.
28. Wang, L. Geng, X (koost). Behavioral Biometrics for Human Identification: Intelligent Applications. New York: Medical Information Science Reference 2009.

Õigusaktid

29. Euroopa Parlamendi ja Nõukogu määrus (EL) 2016/679, 27. aprill 2016, füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiiv 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus). – ELT L119, 04.05.2016, lk 1-88.
30. Euroopa Parlamendi ja Nõukogu direktiiv 95/46/EÜ, 24.oktoober 1995, üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta. - ELT L 281, 23.11.1995, lk 31-50.
31. Euroopa Parlamendi ja nõukogu direktiiv (EL) 2016/680, 27. aprill 2016, mis käsitleb füüsiliste isikute kaitset seoses pädevates asutustes isikuandmete töötlemisega süütegude tõkestamise, uurimise, avastamise ja nende eest vastutusele võtmise või kriminaalkaristuste täitmisele pööramise eesmärgil ning selliste andmete vaba liikumist ning millega tunnistatakse kehtetuks nõukogu raamotsus 2008/977/JSK. – ELT L 119, 04.05.2016, lk 89–131.
32. Euroopa Parlamendi ja nõukogu direktiiv (EL) 2015/2366, 25. november 2015, makseteenuste kohta siseturul, direktiivide 2002/65/EÜ, 2009/110/EÜ ning 2013/36/EL ja määruse (EL) nr 1093/2010 muutmise ning direktiivi 2007/64/EÜ kehtetuks tunnistamise kohta (EMPs kohaldatav tekst). – ELT L 337, 23.12.2015, lk 35–127.
33. Euroopa Parlamendi ja nõukogu määrus (EÜ) nr 444/2009, 28. mai 2009 , millega muudetakse nõukogu määrust (EÜ) nr 2252/2004 liikmesriikide väljastatud passide ja reisidokumentide turvaelementide ja biomeetria standardite kohta. – ELT L 142, 06.06.2009.
34. Euroopa Parlamendi ja nõukogu määrus (EÜ) nr 1987/2006, 20. detsember 2006 , mis käsitleb teise põlvkonna Schengeni infosüsteemi (SIS II) loomist, toimimist ja kasutamist. - ELT L 381, 28.12.2006.
35. Euroopa Parlamendi ja nõukogu määrus (EÜ) nr 444/2009, 28. mai 2009 , millega muudetakse nõukogu määrust (EÜ) nr 2252/2004 liikmesriikide väljastatud passide ja reisidokumentide turvaelementide ja biomeetria standardite kohta. – ELT L 142, 6.6.2009.

36. Euroopa Parlamendi ja nõukogu direktiiv 2002/58/EÜ, 12. juuli 2002, milles käsitletakse isikuandmete töötlemist ja eraelu puutumatuse kaitset elektroonilise side sektoris (eraelu puutumatust ja elektroonilist sidet käsitlev direktiiv). – ELT L 201, 31.7.2002.
37. Euroopa Parlamendi ja nõukogu direktiiv 2009/136/EÜ, 25. november 2009 , millega muudetakse direktiivi 2002/22/EÜ universaalteenuse ning kasutajate õiguste kohta elektrooniliste sidevõrkude ja -teenuste puhul, direktiivi 2002/58/EÜ, milles käsitletakse isikuandmete töötlemist ja eraelu puutumatuse kaitset elektroonilise side sektoris, ning määrust (EÜ) nr 2006/2004 tarbijakaitseseaduse jõustamise eest vastutavate siseriiklike asutuste vahelise koostöö kohta (EMPs kohaldatav tekst). – ELT L 337, 18.12.2009.
38. Komisjoni delegeeritud määrus (EL) 2018/389 27. november 2017, millega täiendatakse Euroopa Parlamendi ja nõukogu direktiivi (EL) 2015/2366 regulatiivsete tehniliste standarditega, mis käsitlevad kliendi tugevat autentimist ning ühiseid ja turvalisi teabevahetuse avatud standardeid (EMPs kohaldatav tekst). – ELT L 69, 13.3.2018.
39. Nõukogu otsus 2007/533/JSK, 12.06.2007, mis käsitleb teise põlvkonna Schengeni infosüsteemi (SIS II) loomist, toimimist ja kasutamist. – ELT L 205, 7.8.2007, lk 63–84.
40. Euroopa Liidu põhiõiguste harta. - ELT C 326, 26.10.2012.
41. Inimõiguste ja põhivabaduste kaitse konventsioon. - RT II 2000, 11, 57.
42. Isikuandmete automatiseeritud töötlemisel isiku kaitse konventsioon. – RT II 2001, 1, 3.
43. Elektroonilise side seadus. - RT I 2004, 87, 593.
44. Isikuandmete kaitse seadus. – RT I 2007, 24, 127.
45. Isikuandmete kaitse seadus. - RT I, 04.01.2019, 11.
46. Isikuandmete kaitse seaduse rakendamise seadus. - RT I, 13.03.2019, 2.
47. Kaitseväeteenistuse seadus. - RT I, 10.07.2012, 1.
48. Töölepingu seadus. - RT I 2009, 5, 35.
49. Politseiametniku daktüloskopeerimise ja DNA-proovi võtmise ning daktüloskopeerimisel saadud andmete ja DNA-proovide edastamise kord. - RT I, 07.06.2013, 13.
50. Act 617/2009 on Strong Electronic Identification and Electronic Signatures. Soome 01.09.2009, tõlgitud 19.04.2010. Kättesaadav arvutivõrgus: https://www.finlex.fi/en/laki/kaannokset/2009/20090617. Viimati külastatud 21.04.2019.
51. Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Version consolidée au 28 août 2004. Kättesaadav arvutivõrgus: https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000006068624&dateTexte=20040828. Viimati külastatud 21.04.2019.

52. Délibération n° 2019-001du 10 janvier 2019 portant règlement type relatif à la mise en œuvre de dispositifs ayant pour finalité le contrôle d'accès par authentification biométrique aux locaux, aux appareils et aux applications informatiques sur les lieux de travail. 01.10.2019. Kättesaadav arvutivõrgus: https://www.cnil.fr/sites/default/files/atoms/files/deliberation-2019-001-10-01-2019-reglement-type-controle-dacces-biometrique.pdf. Viimati külastatud 21.04.2019.

Kohtupraktika

53. EIKo. 04.05.2000, 28341/95, *Rotaru v. Romania*.
54. EIKo. 25.09.2001, no. 44787/98, *P.G. and J.H. v. the United Kingdom.*
55. EIKo. 06.06.2006, 62332/00, *Segerstedt-Wiberg and Others v. Sweden.*
56. EIKo. 04.12.2008, 30562/04 ja 30566/04, *S and Marper v United Kingdom,*
57. EIKo. 18.04.2013, no.19522/09, *M.K. v. France.*
58. EKo. 13.05.2014, Case C-131/12, *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González,*
59. RKTKo 3-3-1-3-12
60. RKTKo 3-3-1-3-12
61. RKTKo 3-2-1-159-14

Liikmesriikide andmekaitse järelevalveasutused

62. Commission Nationale de l'informatique et des Libertés. Le contrôle d’accès biométrique sur les lieux de travail. 28.03.2019. Kättesaadav arvutivõrgus: https://www.cnil.fr/fr/le-controle-dacces-biometrique-sur-les-lieux-de-travail. Viimati külastatud 18.04.2019.
63. Commission Nationale de l'informatique et des Libertés. 21e rapport d’activité 2000. *Sine loco,* Pariis 2001. Kättesaadav arvutivõrgus: https://www.biometrie-online.net/images/stories/dossiers/generalites/droit/CNIL_Rapport-21.pdf. Viimati külastatud 18.04.2019.
64. Commission Nationale de l'informatique et des Libertés. Biométrie dans les smartphones des particuliers: application du cadre de protection des données. 24.07.2018. Kättesaadav arvutivõrgus: https://www.cnil.fr/fr/biometrie-dans-les-smartphones-des-particuliers-application-du-cadre-de-protection-des-donnees. Viimati külastatud 18.04.2019.

65. Commission Nationale de l'informatique et des Libertés.. Enceintes intelligentes : des assistants vocaux connectés à votre vie privée. 20.12.2018. Kättesaadav arvutivõrgus: https://www.cnil.fr/fr/enceintes-intelligentes-des-assistants-vocaux-connectes-votre-vie-privee. Viimati külastatud 21.04.2019.
66. Commission Nationale de l'informatique et des Libertés. Les dispositifs biométriques pour l'accès aux cantines scolaires. 23. 11.2015. Kättesaadav arvutivõrgus: https://www.cnil.fr/fr/les-dispositifs-biometriques-pour-lacces-aux-cantines-scolaires. Viimati külastatud 21.04.2019.
67. Information Commisioner's Office. Freedom of Information Act 2000 (Section 50). Decision Notice 28.02.2011. Kättesaadav arvutivõrgus: https://ico.org.uk/media/action-weve-taken/decision-notices/2011/590086/fs_50320566.pdf. Viimati külastatud 18.04.2019. Viimati külastatud 21.04.2019.
68. Data Protection Commission. Advice on Connected Toys and Devices. 04.12.2018. Kättesaadav arvutivõrgus: https://www.dataprotection.ie/en/guidance-landing/data-protection-commission-advice-connected-toys-and-devices. Viimati külastatud 18.04.2019.
69. Bundesnetzagentur. Bundesnetzagentur removes children's doll "Cayla" from the market. Press release 2017. Kättesaadav arvutivõrgus: https://www.bundesnetzagentur.de/SharedDocs/Pressemitteilungen/EN/2017/17022017_cayla.html. Viimati külastatud 21.04.2019.

Muu kasutatud materjal

70. Artikkel 29 Andmekaitse Töörühm. Opinion 3/2012 on developments in biometric technologies. 00720/12/EN. WP193. 27.04.2012. Kättsaadav arvutivõrgus: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf. Viimati külastatud 21.04.2019.
71. Artikkel 29 Andmekaitse Töörühm. Working Document on biometrics. 12168/02/NE, WP80, 01.08.2003. Kättesaadav arvutivõrgus: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp80_en.pdf. Viimati külastatud 21.04.2019.
72. Artikkel 29 Andmekaitse Töörühm. Opinion 4/2007 on the concept of personal data. 01248/07/NE, WP 136, 20.06.2007. Kättesaadav arvutivõrgus:

https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf. Viimati külastatud 21.04.2019.

73. Artikkel 29 Andmekaitse Töörühm. Guidelines on consent under Regulation 2016/679. 17/EN, WP259 rev.01. 10.04.2018. Kättesaadav arvutivõrgus: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051. Viimati külastatud 21.04.2019.
74. Artikkel 29 Andmekaitse Töörühm. Opinion 3/13 on purpose limitation. 00569/13/NE. WP 203. 02.04.2013. Kättesaadav arvutivõrgus: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf. Viimati külastatud 21.04.2019. Viimati külastatud 21.04.2019.
75. Artikkel 29 Andmekaitse Töörühm. Opinion 8/2014 on the on Recent Developments on the Internet of Things. 14/NE. WP223. 16.09.2014. Kättesaadav arvutivõrgust: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf. Viimati külastatud 21.04.2019.
76. Artikkel 29 Andmekaitse Töörühm. Opinion 02/2013 on apps on smart devices. 00461/13/NE. WP 202. 27.02.2013. Kättesaadav arvutivõrgus: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf. Viimati külastatud 21.04.2019.
77. Artikkel 29 Andmekaitse Töörühm. Opinion 01/2012 on the data protection reform proposals. 00530/12/EN WP 191. Brüssel, 2012. Kättesaadav arvutivõrgus: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp191_en.pdf. Viimati külastatud 21.04.2019.
78. Andmekaitse Inspektsioon. Kantavad seadmed ja privaatsus. Juhis organisatsioonidele ja kodukasutajale seaduse rakendamisel. 09.11.2015. Kättesaadav arvutivõrgus: https://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/Juhised/Juhis-kantavad%20seadmed%20ja%20privaatsus.pdf. Viimati külastatud 21.04.2019.
79. Andmekaitse Inspektsioon. Isikuandmete töötlemine töösuhtes. Abistav juhendmaterjal. Tallinn 2011, muudetud 23.05.2014. Kättesaadav arvutivõrgus: https://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/Isikuandmed%20t%C3%B6%C3%B6suhetes%20juhendmaterjal26%2005%202014_1.pdf. Viimati külastatud 21.04.2019.
80. Andmekaitse Inspektsioon. Andmekaitse Inspektsiooni arvamus isikuandmete kaitse seaduse rakendamise seaduse eelnõule. 16.04.2018. Kättesaadav arvutivõrgus:

https://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/eelnoule_arvamuse_avaldamine_-_iks_rs_eelnou.pdf. Viimati külastatud 21.04.2019.

81. Euroopa andmekaitseinspektor. Comments on the Communication of the Commission on interoperability of European databases. 10.03.2006. Kättesaadav arvutivõrgus: https://edps.europa.eu/sites/edp/files/publication/06-03-10_interoperability_en.pdf. Viimati külastatud 21.04.2019.
82. Euroopa andmekaitseinspektor. Opinion 4/2015. Towards a new digital ethics. Data, dignity and technology. 11.09.2015. Kättesaadav arvutivõrgus: https://edps.europa.eu/sites/edp/files/publication/15-09-11_data_ethics_en.pdf. Viimati külastatud 21.04.2019.
83. Euroopa andmekaitseinspektor. Opinion of the European Data Protection Supervisor on a research project funded by the European Union under the Seventh Framework Programme (FP7) for Research and Technology Development - Turbine (TrUsted Revocable Biometric IdeNtitiEs), 01.02.2011. Kättesaadav arvutivõrgus: https://edps.europa.eu/sites/edp/files/publication/11-02-01_fp7_en.pdf. Viimati külastatud 21.04.2019.
84. Euroopa Komisjon. Joint Research Centre. Technical report series. Biometrics at the Frontiers: Assessing the Impact on Society. For the European Parliament Committee on Citizens' Freedoms and Rights. Justice and Home Affairs (LIBE) 2005. Kättesaadav arvutivõrgus: http://www.statewatch.org/news/2005/mar/Report-IPTS-Biometrics-for-LIBE.pdf. Viimati külastatud 21.04.2019.
85. Euroopa Komisjon. Horizon 2020. Gait Biometrics 3 (Main goal of the project is to create a prototype of the software, which will be able to identify peoplejust based on the way how they walk). 31.07.2015. Kättesaadav arvutivõrgus: https://cordis.europa.eu/project/rcn/196201/factsheet/en. Viimati külastatud 21.04.2019.
86. Euroopa Komisjon. Research & Innovation in Internet of Things. Policy 2018. Kättesaadav arvutivõrgus: https://ec.europa.eu/digital-single-market/en/research-innovation-iot.
87. European Banking Authority. Final Guidelines on the security of internet payments. EBA/GL/2014/12_Rev1, 19.12.2014. Kättesaadav arvutivõrgus: https://eba.europa.eu/documents/10180/934179/EBA-GL-2014-12+%28Guidelines+on+the+security+of+internet+payments%29_Rev1. Viimati külastatud 21.04.2019.
88. International Working Group on Data Protection in Telecommunications. Working Paper on Biometrics in Online Authentication. 60th meeting, 22-23 November 2016, Berlin.

Kättesaadav arvutivõrgus: https://www.datenschutz-berlin.de/infothek-und-service/veroeffentlichungen/working-paper/. Viimati külastatud 18.04.2019.

89. Research Division. Internet: case-law of the European Court of Human Rights. *Sine loco*, European Court of Human Rights 2015. Kättesaadav arvutivõrgus: https://www.echr.coe.int/Documents/Research_report_internet_ENG.pdf. Viimati külastatud 21.04.2019.
90. Lenovo, Intel, and PayPal Team On Fingerprinting Tech For Online Payments. Fortune. 23.09.2016. Kättesaadav arvutivõrgus: http://fortune.com/2016/09/23/lenovo-intel-paypal-fingerprint-biometrics/. Viimati külastatud 21.04.2019.
91. Gannes, L. Eric *Schmidt: Welcome to "Age of Augmented Humanity." 0*7.09.2010. Kättesaadav arvutivõrgus: http://gigaom.com/2010/09/07/eric-schmidt-welcome-to-the-age-of-augmented-humanity/. Viimati külastatud 18.04.2019.
92. Cowley, S. Banks and Retailers Are Tracking How You Type, Swipe and Tap**. –** The New York Times 13.08.2018. Kättesaadav arvutivõrgus: https://www.nytimes.com/2018/08/13/business/behavioral-biometrics-banks-security.html. Viimati külastatud 18.04.2019.
93. Press release. Introducing Apple Card, a new kind of credit card created by Apple. 25.03.2019. Kättesaadav arvutivõrgus: https://www.apple.com/newsroom/2019/03/introducing-apple-card-a-new-kind-of-credit-card-created-by-apple/. Viimati külastatud 21.04.2019.
94. Collinnson, P. NatWest trials fingerprint debit cards to remove £30 limit. – The Guardian 11.03.2019. Kättesaadav arvutivõrgus: https://www.theguardian.com/money/2019/mar/11/natwest-trials-fingerprint-debit-cards-to-remove-30-limit. Viimati külastatud 21.04.2019.
95. Kald, I. Helmes käivitas näotuvastusega raamatulaenutuse. Äripäev. ITuudised 23.11.2018. Kättesaadav arvutivõrgus: https://www.ituudised.ee/uudised/2018/11/23/helmes-kaivitas-naotuvastusega-raamatulaenutuse. Viimati külastatud 21.04.2019.
96. Liive, R. Eestlaste idufirma Veriff lubab maailma kõige turvalisemat isikutuvastamise teenust. – Digigeenius 28.06.2016. Kättesaadav arvutivõrgus: https://digi.geenius.ee/rubriik/uudis/eestlaste-idufirma-veriff-lubab-maailma-koige-turvalisemat-isikutuvastamise-teenust/. Viimati külastatud 21.04.2019.
97. Lugeja küsib: kas tööandja tohib mult sõrmejälgi võtta? – Postimees. 04.07.2018. Kättesaadav arvutivõrgus: https://tarbija24.postimees.ee/4518093/lugeja-kusib-kas-tooandja-tohib-mult-sormejalgi-votta. Viimati külastatud 21.04.2019.

98. Vanian, J. Lenovo, Intel, and PayPal Team On Fingerprinting Tech For Online Payments. - Fortune. 23.09.2016. Kättesaadav arvutivõrgus: http://fortune.com/2016/09/23/lenovo-intel-paypal-fingerprint-biometrics/. Viimati külastatud 21.04.2019.
99. BioCatch. Kättesaadav arvutivõrgus: https://www.biocatch.com/.
100. BioCatch. What is behavioural biometric? Data Sheet. *Sine anno*. Kättesaadav arvutivõrgus: https://www.biocatch.com/hubfs/White%20Papers/What%20is%20Behavioral%20Biometrics.pdf?hsCtaTracking=07028355-5500-4d50-b976-f7be210efa8d%7C598e23f9-e463-49f2-a5d0-1e2eb83cb04b. Viimati külastatud 21.04.2019.
101. HotJar. Kättesaadav arvutivõrgus: https://www.hotjar.com/. Viimati külastatud 21.04.2019.

Lihtlitsents lõputöö reprodutseerimiseks ja lõputöö üldsusele kättesaadavaks tegemiseks

Mina, Marion Kallakas

1. annan Tartu Ülikoolile tasuta loa (lihtlitsentsi) enda loodud teose „Õiguslik alus eriliigiliste biomeetriliste andmete töötlemiseks eraõiguslikes suhetes," mille juhendaja on Helen Eenmaa-Dimitrieva ja kaasjuhendaja on Kärt Salumaa-Lepik ja

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, 30.04.2019