TARTU ÜLIKOOL

ÕIGUSTEADUSKOND

Avaliku õiguse osakond

Kea Kruuse

PRIVAATSUSE JA ISIKUANDMETE KAITSE MASINNÄGEMISE JA MASINÕPPE KASUTUSEL EUROOPA LIIDU ÕIGUSES EMOTSIOONITUVASTUSE JA EESTI KORRAKAITSE JÄLGIMISSEADMESTIKE NÄITEL

Magistritöö

Juhendaja

Dr. Carri Ginter

Tallinn

2019

SISUKORD

SISSEJUHATUS

Masinnägemisel[1] (ingl *computer vision*) ja masinõppel[2,3] (ingl *machine learning*) baseeruvate automatiseeritud emotsiooni- ja isikusamasuse tuvastuse ning neid tehnoloogiaid kasutavate jälgimisseadmestike abil on võimalik tõhusamalt seaduskuulekust tagada, kasumlikumalt äri ajada ning luua personaliseeritum ja turvalisem elukeskkond. Inimeste, eriti gruppide, suurem jälgimine masinnägemist ja masinõppe algoritme kasutades kujutab endast aga mitmeid ohte põhivabadustele ja -õigustele, eriti privaatsusele, isikuandmete kaitsele, võrdsele kohtlemisele ning sõna- ja ühinemisvabadusele.

Magistritöö uurimisprobleemiks on masinnägemise ja masinõppe ning nende rakenduste näotuvastuse (ingl *facial recognition*) ja emotsioonituvastuse (ingl *emotion detection and tracking; face coding; affect recognition; Emotion AI; emotion-tracking AI*) kui uute ja kiiresti levivate tehnoloogiate kasutamisega kaasnev oht privaatsusõigusele ja iskuandmete kaitse õigusele. On selgusetu, milliseid põhimõtteid ja raamistikku peab järgima emotsioonituvastuse puhul, kus isikut ei tuvastata, ning masinnägemise võimekusega jälgimisseadmestike ja isikusamasuse tuvastamisel Eesti korrakaitses.

Uurimisprobleemi käsitletakse Euroopa Liidu õiguslikus raamistikus. Põhiline raskuskese on põhiõiguste hartal ning Euroopa Liidu õiguse kahe olulise andmekaitset puudutava õigusakti - määruse 2016/679 ehk isikuandmete kaitse üldmääruse (edaspidi ka üldmäärus)[4] ja

---

[1] Masinnägemine ja masinõpe on tehisintellekti harud. Masinnägemine on interdistsiplinaarne teadusvaldkond, mille eesmärk on masinate abil digitaalsete piltide ja videote mõistmine ning tegevuste automatiseerimine sarnaselt inimnägemisele. Vt: M. Sonka jt. Image Processing, Analysis, and Machine Vision. Boston: Springer 2008.

[2] Masinõpe annab süsteemidele võime automaatselt õppida ja täiustuda läbi kogemuste ilma inimese sekkumiseta. Tehisintellekt on inimese mõtteprotsesside simulatsioon masinate, eelkõige arvutisüsteemide abil. Nende protsesside hulka kuuluvad õppimine (teabe hankimine ja selle kasutamine), põhjendamine (reeglite kasutamine jõudmaks ligikaudsete või kindlate järeldusteni) ja iseenda parandamine. Vt: M. Rouse. The Essential Guide to Managing HR Technology Trends: AI (artificial intelligence). – SearchEnterpriseAI. Kättesaadav: https://searchenterpriseai.techtarget.com/definition/AI-Artificial-Intelligence; (21.03.2019).

[3] Masinõpet kasutatakse näiteks internetis otsingutele vastete leidmisel, kõne tekstiks töötlemisel, näo tuvastamiseks piltidelt ja videolt. Sügavõpe on masinõppe klass, kus modelleeritakse sisendandmetes hierarhilisi abstraktsioone mitmete kihtide abil. Vt: B. Chandra, R. K. Sharma. Fast learning in Deep Neural Networks. – Neurocomputing, 2016/171, lk 1205–1215.

[4] Euroopa Parlamendi ja nõukogu määrus (EL) 2016/679, 27. aprill 2016, füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus). – Euroopa Liidu Teataja, 4.05.2016, L 119.

direktiivi 2016/680 ehk õiguskaitseasutuste andmekaitse direktiivi (edaspidi ka direktiiv)[5] analüüsil.

Töö esimene eesmärk on välja selgitada, kas masinõppe tehnoloogiate leviku valguses on Euroopa Liidu (EL) andmekaitse regulatsioonis vajalik gruppide tõhusam kaitse võrreldes praegusega.

Töö teine eesmärk on välja selgitada, kas andmekaitse üldmäärus laieneb emotsioonituvastusele, kui isikut ei tuvastata.

Töö kolmas eesmärk on välja selgitada, milliseid andmekaitsenõudeid tuleb järgida masinnägemise võimekusega jälgimisseadmestike kasutamisel ja automatiseeritud isikusamasuse tuvastamisel Eesti korrakaitses ja süüteomenetluses ning tuvastada võimalikud probleemid korrakaitses jälgimisseadmestike kasutusel andmekaitsenõuete täitmisega.

Magistritöö esimeseks hüpoteesiks on, et emotsioonide tuvastamine ja jälgimine pole andmekaitse üldmäärusega reguleeritud vaid juhul, kui töötletavate andmete põhjal pole võimalik andmesubjekti tuvastada, kuid ka sellisel juhul riivab emotsioonituvastus privaatsusõigust.

Magistritöö teiseks hüpoteesiks on, et õiguskaitseasutuste andmekaitsedirektiivi materiaalses kohaldamisalas on nii riiklik järelevalvemenetlus kui ka süüteomenetlus, kuni tegevus on EL õiguse kohaldamisalas.

Magistri kolmandaks hüpoteesiks on, et Eesti korrakaitses peab jälgimisseadmestike kasutus olema vajalik ja proportsionaalne ning proportsionaalsust mõjutab jälgimisseadmestiku asukoht ja seadme tehniline võimekus.

Magistritöö teema on uudne, sest Eesti õiguskirjanduses isikuandmete kaitset emotsioonituvastuse ja korrakaitses masinnägemise kasutuse valguses uuritud pole. Välismaises teaduskirjanduses on biomeetriliste tuvastussüsteemide ja emotsioonituvastuse kohta ilmunud mitmeid raamatuid ja teadusartikleid. Uuritud on isikuandmete kaitset

[5] Euroopa Parlamendi ja nõukogu direktiiv (EL) 2016/680, 27. aprill 2016. Õiguskaitseasutuste direktiivis sätestatud õigusnormid käsitlevad füüsiliste isikute kaitset isikuandmete töötlemisel pädevate asutuste poolt süütegude tõkestamiseks, uurimiseks, avastamiseks, nende eest vastutusele võtmiseks või kriminaalkaristuste täitmisele pööramiseks, sealhulgas avalikku julgeolekut ähvardavate ohtude eest kaitsmiseks ja nende ennetamiseks. – Euroopa Liidu Teataja, 27.04.2016, L 119/89.

näotuvastuse rakenduses töösuhetes, digiallkirjastamisel ja kaubanduses[6,7], ent arvestades teema olulisust ja relevantsust on probleemi EL andmekaitse perspektiivist vähe uuritud.

Teema on relevantne, sest tehisintellektil põhinevad tehnoloogiad nagu masinnägemine ja masinõpe võimaldavad kiiremat ja efektiivsemat automatiseeritud objekti, olukorra, isiku- ja emotsioonituvastust kui kunagi varem. Olulised on arengud masinõppe, matemaatiliste närvivõrkude ja isikute prognoositava käitumise valdkonnas, mis võimaldavad oluliselt täpsemat pildi- ja videotuvastust[8]. Varem oli suure rahva hulgast ühe konkreetse inimese isikusamasuse tuvastamiseks vaja mitukümmend politseiniku. Tänapäevase tehnoloogia juures teeb selle töö ära üks rahva sekka suunatud kaamera[9], mis kasutab masinnägemist ja masinõpet ning millel on ligipääs biomeetrilisele andmebaasile.

Isikusamasuse tuvastamiseks on erinevaid meetode, näiteks näoanalüüs, kõnnakuanalüüs, keha suuruse/kuju/proportsioonide tuvastus, hääle, kõrguse, tooni, keele, dialekti, aktsendi tuvastus, keemiline/bioloogiline/meditsiiniline analüüs (nt hingeõhu koostis, hingamise sagedus, pulss, vererõhk, elektro-galvaanilised naha omadused), eritunnused (nt armid, vigastused, tatoveering, kõrvaaugud), parandus-, abitehnoloogia (nt prillid, läätsed, kuulmisabi, tulevikus ka implantaadid), biomeetriline identifitseerimine (nt võrkkesta mustrid, sõrmejäljed, näokujutis, DNA).[10]

„Targad“ sensorid, mille andmeid analüüsivad masinõppe algoritmid, võimaldavad nii isiku identiteeti kinnitada (nn üks ühele kontroll) kui ka inimese identiteeti tuvastada (nn üks mitmele kontroll). Hea videokvaliteedi ja uusimate algoritmide puhul on isikutuvastussüsteemide veaprotsent vaid 0,2[11], kuigi kehvemate algusfaasis algoritmide ja kehva videokvaliteedi puhul

[6] K. Güven. Facial Recognition Technology: Lawfulness of Processing under the GDPR in Employment, Digital Signage and Retail Context. Magistritöö. Tilburg: Tilburg University 2019.

[7] P. Lewinski jt. Face and Emotion Recognition on Commercial Property under EU Data Protection. – Psychology & Marketing, Wiley Periodicals, 2016/33, No 9, lk 729-746.

[8] Valge Raamat: Identiteedihaldus ja isikut tõendavad dokumendid 1.0. – Riigi Infosüsteemi Amet 2018.

[9] NEC tarkvaraarendajate sõnul suudab NEC näotuvastussüsteem identifitseerida kuni 5 000 inimest rahvamassist. NeoFace Watch: High Performance Face Recognition. Brožüür. NEC Corporation, 2016. Kättesaadav: https://www.nec.com/en/global/solutions/safety/face_recognition/PDF/Face_Recognition_NeoFace_Watch_Brochure.pdf (10.02.2019)

[10] V. Grout. No More Privacy Any More? – Information, 2019/10, No 1, lk 19.

[11] Ameerikas tegutsev National Institute of Standards and Technology's (NIST) hinnangul on aastate 2014-2018 vahemikus näotuvastussüsteemid muutunud 20 korda täpsemaks ning praeguseks on parimate algoritmide veaprotsent vaid 0.2. Veaks loetakse seda, kui algoritm ei tuvasta andmebaasis olevat inimest. J. Grother jt. Ongoing Face Recognition Vendor Test (FRVT) Part 2: Identification. National Institute of Standards and Technology Interagency/Internal Report 8238, 2018.

on veanäitajad palju suuremad, üle 90%[12]. Tänapäevased masinõppesüsteemid suudavad tuvastada kuni 69% meeleavaldajatest, kes kannavad mütse ja salle näo varjamiseks[13].

Automatiseeritud isikusamasuse tuvastamise süsteemid lisavad julgeolekuorganitele efektiivsust turvalisuse tagamisel ning kuritegevuse vastu võitlemisel, mistõttu on neid inimeste tuvastamiseks ja jälgimiseks kasutusele võtnud õiguskaitseasutused mitmel pool maailmas[14]. Hiinas on praeguseks umbes 170 miljonit avaliku sektori jälgimiskaamerat ning 400 miljonit kaamerat on kavas lisada järgmisel neljal aastal (2018. aasta andmetel). Paljud nendest kaameratest kasutavad automatiseeritud näotuvastustehnoloogiat. Tehnoloogia võimekust illustreerib fakt, et Hiina politsei tabas näotuvastustehnoloogiat kasutades 50 000 kontserdikülastaja seast majanduskuriteos kahtlustatava. Hiina valitsus töötab selle nimel, et ühendada rohkem kui 170 miljonit valvekaamerat masinnägemise ja masinõppe tehnoloogiaga, loomaks senisest tõhusamat jälgimisühiskonda, et iga eksimus ning kuritegu avastataks[15]. USA-s on jälgimiskaamerate arv umbes neli korda väiksem[16]. Indias on biomeetrilises andmebaasis umbes 1,1 miljardit inimest India 1,3 miljardist elanikust[17], kelle biomeetrilised andmed (sh näokujutis, iirise kujutis, sõrmejäljed) on seotud paljude avalike teenustega, sh kasutatakse neid isikusamasuse tuvastamiseks. Moskva lisas 2018. aastal linna üle 7000 kaamera ning nüüd on linnas kokku üle 167 000 jälgimiskaamera. Linnapea leiab, et „see on suurepärane. Kriminaalid hoiavad Moskvast eemale ning ei ole ühtegi kohta, kus nad saaksid end siin peita.“[18]

[12] Näiteks Suurbritannia politsei alustas näotuvastussüsteemide testimisega juunis 2017 ning testimisjärgus algoritmide veaprotsendid olid politsei andmetel esialgu isegi kuni 92%. Vt: Police defend facial recognition technology that wrongly identified 2,000 people as potential criminals. – The Telegraph, 5.05.2018; Hilisemal testimisel oli veaprotsent ca 20%. Vt: P. Nilsson. How UK Police Are Using Facial Recognition Software. – Financial Times, 12.10.2018.

[13] A. Singh jt. Disguised Face Identification (DFI) with Facial KeyPoints using Spatial Fusion Convolutional Network. Veneetsia: IEEE International Conference on Computer Vision Workshops 2017.

[14] Globaalne videojälgimistehnoloogiate turg kasvab prognooside kohaselt 2023. aastaks 77,21 miljardi dollarini. 2017. aastal oli turuväärtus 32 miljardit dollarit. Vt: Global Video Surveillance Market: Focus on Ecosystem (Camera, Monitor, Storage, Software, Services), Applications, and Emerging Trends - Analysis and Forecast: 2018-2023. BIS Research 2018. Kättesaadav: https://bisresearch.com/industry-report/video-surveillance-market.html (11.03.2019).

[15] Hiina „suur vend” näeb arvatust halvemini – Digi, 01.08.2018.

[16] Chinese Man Caught By Facial Recognition at Pop Concert - BBC News, 13.04.2018; P. Mozur. Inside China’s Dystopian Dreams: A.I., Shame and Lots of Cameras. - The New York Times, 08.07.2018.

[17] V. Goel. ‘Big Brother’ in India Requires Fingerprint Scans for Food, Phones and Finances. - The New York Times, 07.04.2018.

[18] C. Burt. Moscow to Expand Facial Biometrics to More of Massive Surveillance Camera Network in 2019. - Biometric Update, 19.01.2019.

Euroopas on suurimat kõlapinda saanud näotuvastussüsteemide kasutamine Suurbritannias, kuid tehnoloogiat kasutatakse ka näiteks Saksamaal ja Prantsusmaal, kuigi viimases rangemate regulatsioonide tõttu vähem[19]. Eestil on aastateks 2019-2020 eesmärk luua uudsed automatiseeritud tuvastusvõimalused. Aastaks 2021 on eesmärk arendada biograafiliste andmete võrdlemise ja näobiomeetria üks-mitmele-võrdlemise tehnoloogilist lahendust (ABIS) ning aastateks 2019-2022 eesmärk kasutada nii avalik-õiguslikes kui ka eraõiguslikes suhetes laialdaselt biomeetrilistel andmetel põhinevat isikutuvastuse ja isikusamasuse kontrollimise võimalust.[20] Ettevõtetel võimaldataks ABIS-t kasutada, kuid neil ei tekiks õigust biomeetriliste andmete säilitamiseks, vaid neid kontrollitaks vastu riigi vastavat tehnilist lahendust ning päringu vastuseks saadaks jah/ei tüüpi vastus.[21] Eesti Politsei- ja Piirivalveamet (edaspidi ka PPA) töötab koostöös Tallinna Tehnikaülikooliga välja näotuvastussüsteemi, millel on võimekus tuvastada ka emotsioone[22].

Näotuvastustehnoloogiate kiiret levikut näitab ka see, et kõikidest maailma tehisintellekti idufirmadest on kaks kõige paremini rahastatud ettevõtet just näotuvastusettevõtted (SenseTime ja Face++) ning kõikidest tehisintellektil põhinevatest tarkvaradest on kõige tulusamad videojälgimistarkvara müüvad ettevõtted[23].

Suurim kriitika õiguskaitseasutuste automaatsete näotuvastussüsteemide kasutamisele on privaatsuse ja isikuandmete kaitse riive, kuna identifitseerimine toimub ilma nõusolekuta[24], ning kardetakse massilise jälgimise ohtu ja saadud andmete väärkasutust[25]. Samuti on kritiseeritud automaatsete näotuvastussüsteemide kasutuse läbipaistmatust ja järelvalve puudulikkust, tehnoloogia kallutatust ja diskrimineerimist, kuna tehnoloogia veaprotsendid erinevad sõltuvalt rassist ja soost[26]. On oht, et õiguse ei suuda tehnoloogia arenguga sammu

[19] M. Jacob. Facial Recognition Gains Grounds in Europe, Among Big-Brother Fears. – EURACTIV, 20.10.2017.

[20] Usaldusväärne ja turvaline identiteedihaldus aastateks 2019-2022. Siseministri käskkirja „„Siseturvalisuse arengukava 2015–2020“ 2018–2021 programmide kinnitamine“ lisa 7, lk 10, 14.

[21] A. Pau. Revolutsioon isikutuvastuses: Eesti asub looma sõrmejälgede hiigelandmebaasi – Postimees, 7.08.2018.

[22] K. Õim. Learning and recognition of facial expression with decision trees. Magistritöö. Tallinn: TTÜ 2018.

[23] Artificial Intelligence Deployments Have Expanded to Include 258 Unique Use Cases Across Enterprise, Consumer, and Government Markets. – Tractica, 19.12.2018.

[24] Draft Ethics Guidelines for Trustworthy AI. Working Document for stakeholders' consultation. Brüssel: The European Commission's AI HLEG, 2018, lk 18. Kättesaadav: https://www.euractiv.com/wp-content/uploads/sites/2/2018/12/AIHLEGDraftAIEthicsGuidelinespdf.pdf (10.03.2019).

[25] ÜRO Inimõiguste Kõrge Esindaja on aastal 2016 öelnud, et massiline salajane jälgimine ei ole inimõigustega kooskõlas, kuna jälgimise otsuse peaks tegema igal konkreetsel juhul kasutades proportsionaalsuse analüüsi. Vt: Report on Best Practices and Lessons Learned on How Protecting and Promoting Human Rights Contribute to Preventing and Countering Violent Extremism. ÜRO dokument A/HRC/33/29. – UN High Commissioner for Human Rights, 21.07.2016.

[26] Näotuvastussüsteemid põhinevad masinõppe algoritmidel, mis õpivad andmete abil inimesi tuvastama. Kui andmed, mille põhjal süsteem õpib, on kallutatud, põhinedes näiteks enamuses valge nahavärviga inimeste piltidel,

pidada. Olukorrale lisab keerukust tõsiasi, et infoühiskonna probleemid on interdistsiplinaarsed ja nõuavad juristidelt orienteerumist ka kommunikatsiooniteoorias, infotehnoloogia arengus ja ühiskonnauuringutes.[27] Ühendkuningriigi (edaspidi ka UK) õiguskaitseasutuste automatiseeritud näotuvastussüsteemide vastu pöörduti 2018. aastal ka kohtusse. Kaebaja väidab, et automatiseeritud näotuvastussüsteemid rikuvad üldsuse õigust privaatsusele, riivavad sõna- ja ühinemisvabadust, diskrimineerivad naisi ja vähemusrahvusi ning rikuvad andmekaitseõigust, kuna näotuvastuse kasutus pole riiklikus õiguses detailselt reguleeritud.[28]

Automaatne biomeetriline ja biosensoorne tuvastus ei ole piiratud ainult isiku identiteedi tuvastamise ja kinnitamisega, mille jaoks on vaja lisaks videole või pildile ka biomeetrilisi andmeid koondavat andmebaasi või isikutunnistust. Lisaks isikutuvastusele saab masinõppe ja biomeetriliste või biosensoorsete sensorite abil tuvastada ka inimeste arvu, kehaliigutusi, üldisi biograafilisi andmeid (nt sugu, vanus, rass) ning emotsioone.

Vaieldamatult on emotsioonituvastusel positiivseid rakendusi ning kasu paljudes valdkondades, mistõttu on ettevõtlus ja teadustegevus emotsioonituvastuse lahenduste pakkumisel ja arendamisel hoogustunud. Emotsioonituvastust pakkuvad ettevõtted väidavad[29], et suudavad tehnoloogia abil tuvastada emotsioone nagu ebakindlus, viha, üllatus, heaolutunne, enesekindlus ja vaimse tervise häired. Gartner prognoosib, et aastaks 2022 teavad tehnoloogiaseadmed inimeste emotsionaalse elu kohta rohkem kui nende oma perekond[30]. Emotsioonituvastust kasutatakse näiteks avalikus ruumis turunduses, kus videokaamerate abil tuvastatakse reaalajas inimeste reageeringuid reklaamidele ja muudetakse vastavalt reklaame; emotsioone jälgitakse sotsiaalmeedias (Facebook), tööl ja tööintervjuul, laenu küsimisel ja uniste autojuhtide üles äratamiseks autoroolis (Ford, Nissan, Toyota, Audi)[31].

hakkab algoritm kallutatud otsuseid tegema. Näiteks on süsteemid kategoriseerinud mitte-valgeid inimesi gorilladeks, loomadeks või ahvideks (Google, Flickr), öelnud asiaadile, et tema silmad on foto tegemisel suletud, kuigi tegelikult ei olnud (Nikon) ning tuvastanud valgenahalisi nägusid, kuid mitte mustanahalisi nägusid (HP). Kuna eksimusprotsent on osade rasside puhul suurem, on näiteks mustanahalistel inimestel suurem risk, et neid ekslikult tuvastatakse kui kriminaali.Vt: S. Lohr. Facial Recognition Is Accurate, If You're a White Guy. - The New York Times, 02.09.2018.

[27] E. Tikk, A. Nõmper. Informatsioon ja õigus. Tallinn: Juura 2007, lk 25-26.

[28] O. Bowcott. Police Face Legal Action over Use of Facial Recognition Cameras. – The Guardian, 14.06.2018; Cardiff Resident Launches First UK Legal Challenge to Police Use of Facial Recognition Technology in Public Spaces. – Liberty, 13.06.2018.

[29] Nt DeepEyes tehnoloogiaettevõte, mis pakub masinõppel põhinevaid biomeetrilisi ja biosensoorseid tuvastus- ja jälgimissüsteeme. Koduleht kättesaadav: https://www.deepeyes.co/video-based-a-i/ (03.03.2019)

[30] L. Goasduff. Emotion AI Will Personalize Interactions. – Gartner, 22.01.2018.

[31] A. McStay. The Right to Privacy in the Age of Emotional AI. Bangor: Bangor University 2018, lk 2.

Õiguskaitseasutustel võib olla kasulik emotsioone tuvastada näiteks vihaste või võimalikku ohtu kujutavate inimeste tuvastamiseks avalikes kohtades või isikute ülekuulamistel.

On väidetud, et emotsioonituvastus võib riivata eraelu puutumatust ja avalikes kohtades jälgimisvahendina kasutades ka sõna-, kogunemis- ja ühinemisvabadust. Emotsioonituvastuse abil on võimalik osavalt manipuleerida ja inimesi profileerimise kaudu diskrimineerida. Lisaks on kritiseeritud, et emotsioonituvastus pole täpne ning sisaldab pseudoteadust.[32]

Magistritöö esimene peatükk käsitleb küsimust, kas ja kuidas on kehtivas Euroopa Liidu andmekaitse regulatioonis kaitstud gruppide privaatsus ning milliseid muudatusi võiks kaaluda masinnägemise ja masinõppe tehnoloogiate leviku valguses.

Magistritöö teine peatükk keskendub emotsioonituvastuse regulatsioonile Euroopa Liidu õiguses, eelkõige andmesubjekti tuvastatavuse küsimusele, millest sõltub üldmääruse kohaldamine. Peatükis analüüsitakse võimalikku vajadust luua uus isikuandmete kategooria intiimsetest andmetest nagu emotsionaalne informatsioon ning alternatiive, kuidas mentaalset puutumatust avalikus ruumis kaitsta. Samuti uuritakse, kuidas sisustada „ilmselgelt avalikuks tehtud“ andmeid emotsioonituvastuse kontekstis, mis on töötlemisel alus andmesubjekti nõusoleku küsimata jätmisele.

Magistritöö kolmas peatükk käsitleb üldmääruse ja õiguskaitseasutuste direktiivi kohaldamisalasid riikliku järelevalve ja süüteomenetluse kontekstis ning vastavalt EL õigusest tulenevaid andmekaitse tingimusi jälgimisseadmestike ja automatiseeritud isikusamasuse tuvastamisele. Näotuvastuse reguleerimise ja kasutuse printsiipide osas tuuakse näiteid UK-st, kus planeeritakse näotuvastuse kasutust seadusega reguleerida. Magistritöö on piiritletud EL õigusega, mistõttu EL õiguse kohaldamisalast väljaspoole jääva riikliku julgeoleku tagamisele ei keskenduta[33].

Magistritöös kasutatakse andmekogumismeetodit ja tõlgendamismeetodit, samuti analüütilist ja väiksemas mahus empiirilist meetodit. Andmekogumismeetodit, tõlgendamismeetodit ja analüütilist meetodit kasutatakse kõigis peatükkides. Empiirilist meetodit kasutatakse peamiselt korrakaitse kontekstis analüüsides jälgimisseadmestike osas avalikkusele antud kogemuslikke tähelepanekuid, sh intervjuusid ja kommentaare.

[32] M. Whittaker jt. AI Now Report 2018. New York: AI Now Institute at New York University, 2018.

[33] Riikliku julgeoleku ja salajase jälgimise teemal vt nt: T. Wetzling, K. Vieth. Upping the Ante on Bulk Surveillance An International Compendium of Good Legal Safeguards and Oversight Innovations. – Heinrich Böll Stiftung Democracy, 2018/50.

Töö peamisteks allikateks on teaduskirjandus, mille puhul autoritest võib olulisematena välja tuua L. Taylor, B. van der Sloot, S. Wachter, A. McStay; samuti EL õigusaktid ja nende tõlgendused Artikkel 29 töörühma poolt ning EK ja EIK kohtupraktika. Lisaks on kasutatud EL asutuste juhisdokumente, analüüse ning tehnoloogia- ja õigusalaseid uudiseid ja artikleid.

Märksõnad: Euroopa Liidu õigus, privaatsus, andmekaitse, andmetöötlus, intellektitehnika, raalnägemine, tehisõpe, biomeetriline tuvastamine, näotuvastus, avalik kord.

1. PRIVAATSUSÕIGUS JA ISIKUANDMETE KAITSE ÕIGUS MASINÕPPE ALGORITMIDE LEVIKU VALGUSES

Põhiõigus eraelu puutumatusele ehk privaatsusõigus kaitseb inimese autonoomiat ning seisneb kontrollis oma eraelu üle ja võimaluses takistada põhjendamatut sekkumist eraellu[34]. Privaatsusõigust kaitsevad ÜRO inimõiguste ülddeklaratsioon[35], kodaniku- ja poliitiliste õiguste rahvusvaheline pakt[36], inimõiguste ja põhivabaduste kaitse konventsioon (edaspidi EIÕK)[37], Euroopa Liidu põhiõiguste harta (edaspidi harta)[38] ning ka Eesti Vabariigi põhiseadus (PS § 26)[39].

Õiguse loojad ja kohaldajad Eestis peavad otsuste tegemisel võtma arvesse kolme põhiõigusi sisaldavat dokumenti – põhiseadust, EIÕK-d ning hartat – ning neid tõlgendavate kohtute otsuseid. Neile lisanduvad Eesti õiguskorra osadeks olevad ÜRO inimõiguste kaitse instrumendid ja rahvusvahelised lepingud.[40]

[34] Privaatsusõiguse olemuse osas vt nt K. Sehver. Privaatsusõiguse riive proportsionaalsuse hindamise kriteeriumid euroopa liidu õiguses elektroonilise side andmete kaitse valdkonna näitel. Magistritöö. Tallinn: TÜ 2017, lk 11-21.

[35] ÜRO Inimõiguste Ülddeklaratsioon. Tegemist ei ole õiguslikult siduva dokumendiga, kuid sellelel on olnud suur mõju, kuna tegemist on esimese rahvusvahelise dokumendiga, mis keskendus ainult inimõigustele. See avas tee hilisematele õiguslikult siduvatele õigusaktidele. Vt nt: Mart Nutt. ÜRO inimõiguste ülddeklaratsioon 70. – Diplomaatia, 2018/184.

[36] Paktiga liitus Eesti 1991. aastal. Artikkel 17 lõige 1 kohaselt ei tohi kellegi isiklikku või perekonnaellu meelevaldselt või ebaseaduslikult vahele segada, kellegi korteripuutumatusele, kirjavahetuse saladusele, aule ja reputatsioonile ei tohi meelevaldselt või ebaseaduslikult kallale kippuda. Lõike 2 kohaselt on igal inimesel õigus seaduse kaitsele selliste vahelesegamiste ja kallalekippumiste eest. Kodaniku- ja poliitiliste õiguste rahvusvaheline pakt - RT II 1994, 10, 11.

[37] ELL artikli 6 lõige 3 kohaselt on konventsiooniga tagatud ja liikmesriikide ühistest põhiseaduslikest tavadest tulenevad põhiõigused Euroopa Liidu üldpõhimõtted. EIK eeldab harta vähemalt võrdväärset põhiõiguste kaitset EIÕK-ga ning kontrollib EL põhiõiguste kaitset üksnes siis, kui konkreetsel juhul esineb põhiõiguste kaitses „ilmselge puudus". Inimõiguste ja põhivabaduste kaitse konventsioon. - RT II 2000, 11, 57; EIKo 30.07.2005, 45036/98, *Bosphorus vs. Iirimaa.*

[38] Euroopa Liidu põhiõiguste harta. - ELT C 326, 26.10.2012.

[39] Eraelu puutumatus on põhiõigus ka Eesti Vabariigi põhiseaduse (edaspidi PS) kohaselt.

[40] U. Lõhmus. Põhiõiguste kaitse kolmnurgas riik - Euroopa Nõukogu - Euroopa Liit. – Juridica 2010/5.

EL aluslepingud ja harta sätestavad printsiibid, mida EL liikmesriigid ja institutsioonid peavad EL õiguse kohaldumisalas järgima[41,42,43]. Harta on õiguslikult siduv ja omab aluslepingutega sama jõudu tulenevalt EL lepingu (edaspidi ka ELL) artiklist 6(1). Harta ja aluslepingud väljapoole EL õiguse kohaldumise piire ei rakendu (harta artikkel 51).[44] EIÕK[45] kohaldamisala on hartast laiem. EIÕK-ga liitunud riigid, kelle seas on kõik EL liikmesriigid, on kohustatud EIÕK esimeses osas sätestatud õigused ja vabadused tagama igaühele oma jurisdiktsioonis. Seega peavad liikmesriigid[46] arvestama kogu oma tegevusalas EIÕK-s sätestatu (EIÕK artikkel 1)[47] ja EIK praktikaga ning lisaks EL õiguse kohaldamisalas[48] EL õigusega, sh harta ja EK

[41] EKo 24.04.2012, C-571/10, *Servet Kamberaj v Istituto per l'Edilizia sociale della Provincia autonoma di Bolzano (IPES) et al*; EKo 7.05.2013, C-617/10, *Åkerberg Fransson*; EKo 6.03.2014, C-206/13, *Cruciano Siragusa v Regione Sicilia*; EKo 29.01.2013, C-396/11, *Ciprian Vasile Radu*.

[42] Harta õiguslikust siduvusest ja EL õiguse kohaldamise ülimuslikkuse põhimõttest tulenevalt peavad siseriiklikud kohtud EL õiguse kohaldamisalas otsuseid tehes hartat kohaldama. Vt EKo 22.10.1998, ühendatud kohtuasjad C-10/97 kuni C-22/97, *Ministero delle Finanze vs. IN.CO.GE.'90*.

[43] Menetlusautonoomia põhimõtte kohaselt tuleb liikmesriikidel kehtestada oma sisemises õiguskorras menetlusnormid isikutele EL õigusest tulenevate õiguste, sh hartast tulenevate õiguste, kaitsmiseks. Need normid ei tohi olla ebasoodsamad normidest, millega reguleeritakse sarnaseid siseriiklikke olukordi (võrdväärsuse põhimõte) ega muuta EL õiguskorra alusel antud õiguste kasutamist praktiliselt võimatuks või ülemäära raskeks (tõhususe põhimõte). Vt RKo 3-3-1-79-08, p 20; EKo 14.12.1995, ühendatud kohtuasjad C-430/93 ja C-431/93, *Van Schijndel v Stichting Pensioenfonds voor Fysiotherapeuten*, p 17; EKo 07.09.2006, C-53/04, *Marrosu v Sardino*, p 52; EKo 18.06.2008, C-1/06, *Bonn Fleisch Ex- ja Import GmbH vs. Hauptzollamt Hamburg-Jonas*.

[44] EL õigus on siseriikliku õiguse suhtes ülimuslik. EL ainupädevuses või EL-ga jagatud pädevuses olevates valdkondades kohaldatakse Eesti seaduste, ka PS vastuolu korral EL õigusega EL õigust. Vt: *Åkerberg Fransson*, para 17-23, 36-37; EKo 6.03.2014, C-206/13, *Siragusa*, para 6, 25-26; RKPJKa 3-4-1-3-06.

[45] 1950. aastal Euroopa Nõukogu allkirjastatud EIÕK on rahvusvaheline leping inimõiguste ja põhivabaduste kaitsmiseks. EIÕK-ga on liitunud kõik 47 Euroopa Nõukogu liikmesriiki, kellest 28 on ELi liikmed. Euroopa Nõukogu koduleht. Kättesaadav: https://www.coe.int/en/web/human-rights-convention/

[46] EL ei ole konventsiooni liige. Euroopa Liidu Lepingu artikli 6 kohaselt liitub EL konventsiooniga, ent Euroopa Kohus liitumisele heakskiitu andnud ei ole, peamiselt seetõttu, et liitumine kahjustaks EL autonoomsust. Vt: EK 18.12.2014, C-2/13, arvamus; Euroopa Parlament ja Komisjon on rõhutanud vajadust konventsiooniga liituda. Vt: R. Manko. EU Accession to the European Convention on Human Rights (ECHR). Briifing. – European Parliamentary Research Service (EPRS), 07.2017; Olukord on "skisofreeniline", kuna EIK võib liikmesriiki karistada EL õiguse kohaldamise eest, kuid EL-i mitte. Hetkel puudub väline kontroll EL-i üle, s.t võimalus esitada EL tegevuse peale kaebus EIK-sse. Samuti on raskusi EIK otsuste täitmisega siis, kui EL liikmesriigi rikkumine tulenes sisuliselt EL õigusest. Vt: C. Salignat. The Impact of the Emergence of the European Union as a Human Rights Actor on the Council of Europe. – Baltic Yearbook of International Law 2014/4, lk 72.

[47]Arvestada tuleb, et vastavalt EIÕK artiklile 57 konventsiooniga liitumine on võimalik reservatsioonidega. Vt: Reservations and Declarations for Treaty No.005 - Convention for the Protection of Human Rights and Fundamental Freedoms – Euroopa Nõukogu. Kättesaadav: https://www.coe.int/en/web/conventions/search-on-treaties/-/conventions/treaty/005/declarations (02.03.2019).

[48] "Liidu õiguse kohaldamine" harta artikli 51 tähenduses eeldab teatava tihedusega seose olemasolu, mis ulatub kaugemale sellest, et asjaomaste valdkondade puhul on tegemist naabervaldkondadega või et üks neist valdkondadest avaldab teisele kaudset mõju. Teiste tegurite hulgas tuleb hinnata, kas asjaomaste riigisiseste õigusnormide eesmärk on liidu õiguse sätte kohaldamine, milline on nende riigisiseste õigusnormide iseloom ja kas need järgivad teistsuguseid eesmärke kui liidu õigus, isegi kui need riigisisesed õigusnormid võivad mõjutada liidu õigust vaid kaudselt, ning seda, kas selles valdkonnas on olemas liidu õiguse erinormid või normid, mis võivad seda valdkonda mõjutada (punktid 24 ja 25). EK ülevaate harta kohaldumisala osas vt: *Siragusa*; Euroopa Liidu põhiõiguste harta kohaldamisala. Temaatiline ülevaade. – EK, 12.2017. Kättesaadav:

praktikaga.[49] Lisaks olenevalt riigist kohalduvad ka muud rahvusvahelised lepingud, millega riik on liitunud.

Euroopa Nõukogu sai 2018. aastal valmis moderniseeritud konventsiooni 108, kus on uuendatud andmekaitse põhimõtteid võrreldes varasema konventsioon 108-ga. Moderniseeritud konventsioon on harmoniseeritud EL isikuandmete kaitse üldmääruse ja õiguskaitseasutuste direktiiviga pakkudes nendega samal tasemel kaitset. Euroopa Ülemkogu on andnud loa EL liikmesriikidele moderniseeritud konventsiooni 108-ga liituda. Loodetakse, et uuenud konventsiooni abil lihtsustub andmevahetus EL liikmesriikide ja teiste konventsiooni osaliste vahel.[50]

Isikuandmete kaitse on seotud privaatsusõigusega, kuid on õigusena eraldi sätestatud harta artiklis 8(1) ja EL toimimise lepingu artiklis 16(1). Küsimuses, kas isikuandmete kaitse on eraldiseisev põhiõigus, ollakse eri seisukohtadel. Õiguskirjanduses on argumenteeritud, et tegu on põhiõigusega, kuna isikuandmete kaitse õigusel on võrreldes privaatsusõigusega laiem kohaldamisala ning sellel on teatavad lisandväärtused nt õiglase töötlemise põhimõte[51]. Samuti takistaks käsitlemine hübriidõigusena isikuandmete kaitse õiguse täieulatusliku potentsiaali ärakasutamist[52]. Samas on argumenteeritud, et isikuandmete kaitset peaks vaatlema kui tarbija õigust mitte kui põhiõigust, kuna isikuandmete kaitse regulatsiooni olemus on pigem turgu reguleeriv kui inimõiguste riivete eest kaitsev[53]. Hartas on isikuandmete kaitse õigus toodud eraldi artiklina kui põhiõigus. Ka EK on viidanud[54] harta artiklis 8 sisalduvale isikuandmete kaitse õigusele kui põhiõigusele. Võib järeldada, et kuigi sel teemal on eriarvamusi, on

https://curia.europa.eu/jcms/upload/docs/application/pdf/2018-05/fiche_thematique_-_charte_-_et.pdf (27.03.2019).

[49] EU Charter of Fundamental Rights: When Does It Apply and Where to Go in Case of Violation? Skeem. – Euroopa Komisjon, *sine loco, sine anno*. Kättesaadav: https://ec.europa.eu/info/sites/info/files/charter-application_en.pdf (04.03.2019).

[50] Vt ka G. Greenleaf. 'Modernised' Data Protection Convention 108 and the GDPR. Sidney: UNSW Law, 2018; Võrdlust vana 2018.a konventsiooni ja moderniseeritud konventsiooni 108 osas vt: Convention for the Protection of Individuals with Regard to the Processing of Personal Data (CETS 108). Tabel. – Euroopa Nõukogu, 2018. Kättesaadav: https://rm.coe.int/cahdata-convention-108-table-e-april2018/16808ac958 (16.02.2019).

[51] Sehver, lk 19.

[52] *Ibid*; C. Docksey. Four Fundamental Rights: Finding the Balance. – International Data Privacy Law, 2016/6, No 3, lk 202; P. K. Tupay. Õigusest eraelule kuni andmekaitse üldmääruseni ehk tundmatu õigus isikuandmete kaitsele. - Juridica 2016/IV, lk 234, 236; O. Lynskey. Deconstruction Data Protection: The „Added Value" of a Right to Data Protection in the EU Legal Order. – International & Comparative Law Quarterly 2014/63 No 3, lk 573 jj.

[53] B. van der Sloot. Legal Fundamentalism: Is Data Protection Really a Fundamental Right? – Law, Governance and Technology Series, 2017/36, lk 3-30.

[54] Näiteks EK suurkoda: „harta artiklites 7 ja 8 toodud põhiõiguste" ja „riivab ka harta artikliga 8 tagatud põhiõigust isikuandmete kaitsele". Vt: EKo 16.11.2018, C-207/16, M*inisterio Fiscal*, p 58 ja 51.

vähemalt EL õiguse raames privaatsusõigus ja isikuandmete kaitse õigus eraldi põhiõigused, mis on omavahel tihedalt seotud.[55] EIÕK-s on isikuandmete kaitse osa põhiõigusest era- ja perekonnaelu puutumatusele.

Isikuandmete kaitse õigus on tihedalt seotud lisaks privaatsusõigusele ka mõtte- ja sõnavabaduse, usuvabaduse, diskrimineerimise keelu, efektiivse õiguskaitse ja õiglase kohtupidamisega. Harta artiklist 8 tulenevalt on isikuandmete kaitsel mitu iseloomulikku elementi: isikuandmete asjakohane töötlemine, töötlemine kindlaksmääratud eesmärkidel ja asjaomase isiku nõusolekul või muul seaduses ettenähtud õiguslikul alusel; õigus enda kohta kogutud andmetega tutvuda ja nõuda nende parandamist ning sõltumatu asutuse kontroll.[56]

Nii üldmäärus kui ka õiguskaitseasutuste direktiiv on võetud vastu kiire tehnoloogilise arengu ja üleilmastumise taustal eesmärgiga tugevdada ja ühtlustada andmekaitseraamistikku ning tagada selle tõhus täitmine (üldmääruse preambuli p 6-7, õiguskaitseasutuste direktiivi preambuli p 3-4).

1.1. Tehnoloogiline areng

Uute tehnoloogiate tõttu on muutunud viis, kuidas andmed tekivad. Aina enam tekivad andmed tehnoloogia tavapärase kasutuse käigus, kus kogutakse andmeid sageli inimese enda sekkumiseta. Näiteks sensorid võivad inimese teadmata koguda tema isiku ja käitumise kohta andmeid kohtades ja olukordades, kus varem andmeid ei kogutud, näiteks kodus, magamise ajal, poes või tänaval jalutades. Sellise andmekogumise üks eesmärke on inimese vajadusi ennustada ja nendele vastada.[57] Õiguskaitseasutuste andmekogumise eesmärk võib olla näiteks ohtude ennetamine või süüteomenetluse tõhustamine.

Suurenenud on digitaliseerimine ja andmestumine. Tehnoloogia arengu tõttu pole enam piire andmete hulgale, mida saaks salvestada, pole ka piire valdkondadele, mida saaks jälgida, ning jälgimise teel saadud informatsiooni on võimalik talletada väga kaua.[58] Dekaad tagasi ei eksisteerinud veel mitmeid andmeliike, näiteks genoomiline informatsioon, kasutati vähem

[55] IKS 2019. a seletuskirjas nimetatakse isikuandmete kaitset põhiõiguseks. Seletuskiri isikuandmete kaitse seaduse eelnõu juurde. – RT I, 04.01.2019, 11 – jõust. 15.01.2019, lk 2.

[56] Privaatsuse põhiväärtustest ja andmekaitse õiguse kujunemisloo osas vt ka Y. McDermott. Conceptualising the Right to Data Protection in an Era of Big Data. – Big Data & Society, 2017.

[57] S. Wachter. Data Protection in the Age of Big Data. – Nature Electronics, 2019/2, lk 6-7.

[58] *Ibidem.*

digitaalseid sotsiaalvõrgustikke ja analüüsimeetodeid nagu pilvandmetöötlus, vähem kasutati masinõpet ja algoritmilisi automaatotsuseid.[59]

Laienenud on andmete kättesaamine virutaalmaailmast n-ö pärismaailma (horisontaalne laienemine) ehk sensorite abil on hakatud koguma infot inimeste käitumise, omaduste, kogemuste jms kohta. Andmeid kogutakse vereringest, voodist, hommikusöögi ajal räägitust, teekonnast koju ja kooli, trennist, külmikust, parkimisest, elukohast ja elunditest. Samuti kogutakse uute tehnoloogiate abil aina intiimsemat infot (vertikaalne laienemine). Andmeid on võimalik koguda näo- ja emotsioonituvastustehnoloogia abil analüüsides häält, kõnnakut, rühti, teksti ning järeldusi tehakse isiku, meeleolu, emotsioonide, tõe ja vale ning isiksuse nõrkade kohtade osas. Sensorid on võimelised mõõtma hingetõmbeid, silmapilgutusi, lihastõmbeid, väiksemaid silmaliigutusi.[60]

2018. aasta maikuu seisuga luuakse iga päev 2,5 kvintiljonit ($2,5 \times 10^{18}$) baiti andmeid. Maailma suurimat sotsiaalmeediaplatvormi, Facebooki kasutab 2 miljardit inimest, kellest 1,5 miljardit on aktiivsed iga päev. Iga minut jagavad pool miljonit Snapchati kasutajat oma fotosid, laetakse Instagrami 50 tuhat fotot ning tehakse pool miljonit säutsu.[61] Asjade interneti areng tõstab samuti andmete loomise tempot. Internetiga ühendatud seadmeid on maailmas üle 17 miljardi, millest asjade interneti seadmeid on 7 miljardit, mis ei sisalda nutitelefone, tahvleid, sülearvuteid ega liinitelefone. Prognoositakse, et asjade interneti seadmete arv kasvab 7 miljardilt 10 miljardini aastaks 2020 ning 22 miljardini aastaks 2025.[62]

Uued jälgimise praktikad ning suurenud andmete kogumine ja töötlemine suurtes mahtudes nii era- kui ka avalikus sektoris kujutab endast väljakutset privaatsusele ja andmekaitsele. Jälgimist on keeruline vältida, sest jälgivaid seadmeid on aina enam. Näiteks võib olla keeruline jälgimiskaameraid vältida, kui neid on maailmas üle 350 miljoni (2016.a seisuga)[63].

Jälgimist on kolme tüüpi: klassikaline jälgimine (*surveillance*), kus inimest jälgib keegi teine (kõrgemalt); enese jälgimine (*sousveillance*), kui inimene end ise jälgib näiteks pulsikella abil; üksteise jälgimine (*co-veillance* või *mutual watching*), mis on seotud eelkõige

[59] L. Taylor jt. Group Privacy: New Challenges of Data Technologies. – Philosophical Studies Series, 2017/126, lk 3-4.

[60] S. Zuboff. Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. New York: Public Affairs, 2019.

[61] C. Piovesan. How Privacy Laws Are Changing To Protect Personal Information – Forbes, 05.04.2019.

[62] K. L. Lueth. State of the IoT 2018: Number of IoT devices now at 7B - Market accelerating – IOT Analytics, 08.08.2019.

[63] Rise of Surveillance Camera Installed Base Slows. – SDM, 5.05.2016.

sotsiaalmeediaga, kus inimesed üksteise elusid jälgivad.[64] Klassikaline jälgmine on olnud levinud praktika kaua aega ning selleks on varem kasutud fikseeritud asendis kaameraid. Tehnoloogiate arenguga on aga seadmed läinud väiksemaks ning arenenud on kinemaatiline jälgimine (*kineveillance*), kus kasutatakse kantavaid või liikuvaid seadmeid näiteks käekellasid, mobiilikaameraid ja droone.[65]

On nii positiivset (*bienveillance*) kui ka negatiivset jälgimist (*malveillance*).[66] Seirekapitalism pakub inimestele reaalseid väärtusi ning suurendab personaalsust, kuna suurem jälgimine võimaldab inimeste vajadusi ja soove täpsemalt tabada. Internetiplatvormid ja teenused teevad elu mugavamaks, efektiivsemaks ning annavad võimalusi sotsialiseerumiseks. Vastutasuks lubavad inimesed end jälgida.[67] Jälgimisvahendite abil on võimalik muuta elu mugavamaks ja loodussõbralikumaks, näiteks tualetis automatiseeritud vee laskmine või automatiseeritud tulede kustutamine. Jälgimine võib aidata vähendada ja tõkestada kuritegevust ning tõsta turvalisust. Valitsustel ja õiguskaitseasutustel on võimalus ka eraettevõtetelt isikute kohta andmeid välja nõuda, mis tähendab, et suur hulk andmeid, mida eraettevõtted koguvad, võivad sattuda õiguskaitseasutuste kätte. Seda fenomeni, kus üksteise jälgimisest kogutud andmed jõuavad korportatiivsete kanalite kaudu riigiasutustesse, on nimetatud fraasiga "*veillant panoptic assemblage*".[68]

Suurenenud jälgimistehnoloogiate kasutus tähendab riski liigseks võimu kogunemiseks valitsuste kätesse, eriti riikides, kus demokraatlikke järelvalvesüsteeme ja kodanikeorganisatsioone on vähem.[69] Riikides, kus demokraatia ei ole tugev, on näo- ja emotsioonituvastuse kasutamisel risk süsteemsete ja laialdaste inimõiguste, eriti vähemuste õiguste, rikkumisteks, kuna tehnoloogia võib võtta üle inimeste eelarvamused, kui tehnoloogia

[64] S. Mann. Surveillance (Oversight), Sousveillance (Undersight), and Metaveillance (Seeing Sight Itself). Workshop paper. The IEEE Conference on Computer Vision and Pattern Recognition (CVPR) Workshops, 2016.

[65] A. Rouvroy, Y. Poullet. The Right to Informational Self-Determination and the Value of Self-development: Reassessing the Importance of Privacy for Democracy. Dordrecht: Springer, 2009, lk 45–76.

[66] S. Mann.

[67] J. Szalai. O.K., Google: How Much Money Have I Made for You Today. – The New York Times, 16.01.2019.

[68] V. Bakir. Veillant Panoptic Assemblage: Mutual Watching and Resistance to Mass Surveillance after Snowden. – Media and Communication 2015/3, No 3, lk 12-25.

[69] K. P. Donovan, C. Nyst. Privacy for the Other 5 Billion. – Slate, 17.05.2013.

neutraalsusele eraldi tähelepanu ei pöörata.[70] Mõnes kultuuris on ka teatud biomeetrilised tuvastussüsteemid ebasobilikud ning teatud juhtudel inimestele ebamugavad või hirmutavad.[71]

Jälgimise suurenemist toetavad kiiresti kasvavad valdkonnad nagu käitumis- ja andmeteadus. Käitumisanalüüs võib paljastada tegevusvõimalusi segmentide, individuaalsete väljavaadete ja klientide kohta. Käitumisanalüüsi põhjal on võimalik saada mitmesugust infot, millest on huvitatud eelkõige eraettevõtted, näiteks individuaalsed isiklikud eelistused ja toote või sisu huvid; kus isik ostutsüklis või klient nn elutsüklis asub; millal on isik vastuvõtlikum, et teda veenda, ostma ajendada või talle lisatooteid müüa; millal tuleb isiku mõjutamiseks tegutseda; millised pakkumised on kõige asjakohasemad ja veenvamad; kui palju on inimene valmis kulutama.[72]

Andmed ja nende abil inimeste mõjutamine pakuvad huvi mitmetele alates reklaamiärist kuni poliitiliste organisatsioonide ja õiguskaitseorganiteni. On prognoositud, et asjade internet võib võimaldada minna ärimudelilt, kus on garanteeritud sooritus, üle ärimudelini, kus on garanteeritud tulem[73]. Võib olla ahvatlev teatud summa eest saada garanteeritud partei reitingu kasv või garanteeritud kasum toodete müügist, mis saavutatakse kogutud andmete põhjal inimeste mõjutamise tulemusena. Siiski on kritiseeritud, et ärimudel, mis kategoriseerib iga liigutuse, emotsiooni, sõna ja soovi on liiga radikaalne ning seda ei tohiks kergelt võtta.[74]

Üks näide varjatud manipulatsioonist emotsioonidega tuleb välja Facebooki eksperimentidest[75]. Facebooki töötajad leidsid, et inimeste emotsionaalseid seisundeid on võimalik mõjutada, kuna emotsioonid on n-ö nakkavad, ning seda mõjutamist on võimalik teha ilma nende teadmata. Facebooki rakendust kasutades muutunud emotsioonid kanduvad aga edasi ka ülejäänud ellu väljaspool rakendust.[76]

Privaatsusotsuseid tehakse aina enam nö seirekapitalismi eesmärke teenides. Näiteks mitmete tehnoloogiaettevõtete nagu Google'i ja Facebooki edu sõltub andmete kogumisest ning nende ettevõtete edulooga on kaasnenud teadmiste assümeetria süvenemine seirekapitalistide

[70] R. Gellman. Privacy and Biometric ID Systems: An Approach Using Fair Information Practices for Developing Countries. Washington DC: Center for Global Development, 2013/28, lk 10.

[71] *Ibid*, lk 23.

[72] Oh Behave! How Behavioral Analytucs Fuels More Personalized Marketing. White Paper. IBM Corporation, 2013.

[73] C. Pettey. Treating Information as an Asset. – Gartner, 17.02 2016.

[74] J. Szalai.

[75] A. D. I. Kramer jt. Experimental Evidence of Massive-Scale Emotional Contagion through Social Networks. – Proceedings of the National Academy of Sciences 2014/111, No. 24, pp 8788–8790.

[76] S. Zuboff.

kasuks.[77] See on üks probleemidest, mida EL-i andmekaitseregulatsioon adresseerib kehtestades nõuded andmesubjekti teavitamisele ja töötlemise läbipaistvusele, sh kohustuse isikuandmete töötlemise eesmärkide selgest teavitamisest (üldmääruse III peatükk ning peambuli p-d 39, 63).

Õigusfilosoofias on privaatsust vaadeldud kui autonoomsuse kaitset ning autonoomsust kui vabadust domineeriva võimu eest, mille üks vorme on informatsiooni valdamine. Sellest perspektiivist on privaatsus autonoomsuse eeldus, kuna võimaldab inimestel kontrollida, milleid andmeid enda kohta teistega jagada. Sellise privaatsuseta on võimatu iseenda üle valitsemine.[78] Iseenda üle valitsemine tähendab, et inimene saab elada oma ettenägemise ja põhjenduste kohaselt[79]. Kuna seirekapitalismi eesmärk on andmete abil inimeste otsuseid mõjutada, kujutab seirekapitalismi areng ohtu inimeste autonoomiale. See pole murekoht mitte ainult individuaalsel tasemel, vaid ka ühiskondlikult ja poliitiliselt, kuna privaatsus ja autonoomia on ühiskondlikud väärtused[80] ning vajalikud demokraatliku ühiskonna toimimiseks[81].

2016. aastal vastuvõetud EL andmekaitse pakett võttis eesmärgiks uuendada andmekaitsereegleid, et need oleksid sobilikud tehnoloogilise arengu valguses (üldmääruse preambuli p 6-7) ning reeglid oleksid tehnoloogiliselt neutraalsed ja sõltumatud konkreetsetest meetoditest (üldmääruse preambuli p 15). Seetõttu on EL andmekaitsereeglid piisavalt abstraktsed ega pole esitatud kinnist tehnoloogiliste meetodite nimekirja, millele üldmäärus ja õiguskaitseasutuste direktiiv kohalduksid. Adresseeritud on ka automatiseeritud otsuseid, sh profiilianalüüsi, mida seirekapitalismis kasutatakse. Ometi on esitatud kriitikat, et reeglid pole piisavad, et kaitsta inimeste gruppe.

[77] *Ibid.*

[78] D. Mokrosinska. Privacy and Autonomy: on Some Misconceptions Concerning the Political Dimensions of Privacy. – Law and Philosophy 2018/37, lk 126.

[79] *Ibid*, lk 127.

[80] *Ibidem*.

[81] Surveillance Capitalism and the Challenge of Collective Action. – New Labor Forum, 01.2019. Kättesaadav: https://newlaborforum.cuny.edu/2019/01/22/surveillance-capitalism/ (27.02.2019).

1.2. Grupitunnuse põhjal andmete töötlemine

Tehnoloogia tase võimaldab koguda andmeid inimeste endi, nende käitumise ja harjumuste kohta nii, et andmed on küll anonüümsed, ent ütlevad palju inimeste kalduvuste, tüüpide ja kollektiivide kohta ning võimaldavad inimeste nö sorteerimist ja kategoriseerimist. [82] Lisaks on uuringute kohaselt avalike andmete kaevega saadud anonüümsed profiilid võimalik konkreetse isikuga siduda 84-87% täpsusega[83].

Uuete andmeanalüütika tehnoloogiate mõjusid on seni peamiselt adresseeritud vaid individuaalsel tasemel, kuigi profileerimine ja masinõpe on suunatud gruppidele. Seni on andmekaitse tähelepanu olnud suunatud andmete anonümiseerimisele, üksikisiku indentiteedi ja isikuandmete kaitsele ning grupist on mõeldud vaid üksikisikute kollektiivina, kus oluline on iga üksik indiviid oma privaatsusõiguse ja isikuandmete kaitse õigusega. Sellest ei pruugi andmeanalüütika tehnoloogia arenedes piisata, sest suurandmete ajastul on andmeanalüüs suunatud gruppidele ning indiviidil põhinev andmekaitse ei pruugi olla piisav.[84]

On pakutud, et selle asemel, et traditsioonilisse andmekaitsekäsitlusse kinni jääda, peaks pigem keskenduma tehnoloogilisele reaalsusele ja probleemidele, mis tehnoloogia arengu tõttu on tekkinud ja tekivad.[85] Vastasel juhul ei suuda õigus piisavalt kiiresti probleemide lahendamise ja põhiõiguste kaitsega toime tulla. Nii põhiõiguste kaitse diskussiooni kui ka vajadustel seaduste loomisesse või muutmisesse on vajalik kaasata tehnoloogiaeksperte, sest õigusteadlased, ametnikud ja poliitikud ei pruugi teada, kuidas täpselt andmeanalüütika ja masinõpe toimivad.

Andmestumise tõttu on lihtsam inimesi monitoorida ja jälgida erinevatel era- ja avaliku huvi eesmärkidel. Esiteks on võimalik tänu andmeanalüüsile inimesi ja trende paremini mõista. Teiseks on võimalik inimesi mõjutada ning see võimalus tekitab nii ärililist kui ka poliitilist huvi[86]. Mõjutamine leiab aset nii demograafilisel kui ka individuaalsel tasemel ning eesmärk võib olla mõjutada nii inimest kui ka gruppi või massi inimesi. Varem, kui andmete kogumine ja -analüüs oli kallim, koguti andmeid peamiselt üksikisiku või väikeste gruppide kohta.

[82] L. Taylor jt. Group Privacy: New Challenges of Data Technologies. – Philosophical Studies Series, 2017/126, lk 3-4.

[83] G. Neff. Why Big Data Won't Cure Us. – Big Data, 2013/1, No 3, lk 117-123; Y-A. Montjoye jt. Unique in the Shopping Mall: On the Reidentifiability of Credit Card Metadata. – Science, 2015/347, No 6221, lk 536-539.

[84] L. Taylor jt, lk 1-2.

[85] *Ibid*, lk 3.

[86] *Supra*, ptk 1.1.

Tänapäeval on andmete kogumine ja töötlemine palju odavam ja lihtsam. Andmeid analüüsitakse mustrite ja grupiprofiilide põhiselt. Andmeanalüüsi tulemusi kasutatakse laiemate otsuste tegemiseks ning rakendatakse suuremal skaalal. Üksikisik ei ole enam andmetöötluse puhul tsentraalse tähtsusega.[87]

Andmeanalüüsi tehnoloogiate puhul on oluline mõista gruppide olemust. Esiteks, grupid on dünaamilised. Neid on lõpmatutes eri suurustes ja eri komponentidega ning nad on muutlikud. Muutlikkuse metafooriline näide oleks, et tegu on justkui inimestega bussi peal, kus bussi peal olevad inimesed igas peatuses vahetuvad. Teiseks, tehnoloogiad määravad rühmad klastrite ja tüpiseerimise kaudu. Seega on eksitav mõelda kollektiivse privaatsuse rikkumisest kui millestki sellisest, mis juhtub grupiga, mis eksisteerib sõltumatult tehnoloogiast, mis selle rühma moodustas. Kollektiivset privaatsust on võimalik rikkuda ka nii, et grupis olevad isikud pole sellest teadlikud, sest nad on gruppi näiteks enda teadmata profileerimise teel sattunud.[88]

Grupiprivaatsusele on võimalik läheneda kahel viisil. Esimese viisi puhul nähakse gruppi kogumina selles grupis olevate isikute privaatsusõigustest (nö „nende“ privaatsus). Selle mõtlemise metafoorne näide on, et kogum on sinine, kui kõik kogumi liikmed on sinised. Teise viisi puhul on kollektiivne privaatsus grupil kui sellisel (nö „selle“ privaatsus). Metafoor sellele viisile oleks, et kogum on raske, kuigi kõik selle liikmed on kerged, sest kergete liikmete kokkupanemisel on tulemuseks raske kogum. [89]

EL andmekaitse regulatsioon põhineb füüsiliste isikute isikuandmete kaitsel. Andmekaitse üldmääruse kaitsealasse jäävad andmed, mis võimaldavad isikuid identifitseerida. Andmed, mis konkreetset inimest identifitseerida ei võimalda, jäävad kaitsealast välja. See lähenemine on mõistlik vanamoelise andmetöötluse puhul, ent suurandmete ajastul ei pruugi ainult üksikisiku privaatsuse kaitsest piisata. Võib olla vajalik kaitsta andmeid, mis võimaldavad identifitseerida inimeste kategooriat või gruppi.[90]

Üldmäärus ei keela inimeste üldiste demograafiliste näitajate kogumist nagu näiteks vanus, sugu, rass jne, eeldusel, et andmed üldistatakse grupi inimeste kohta ning nende põhjal pole võimalik konkreetset isikut tuvastada ega isiku identiteeti kinnitada. Tehnoloogia, mis sellisel moel üldiste demograafiliste näitajate kogumist gruppide kohta võimaldab, on olemas. Sellist

[87] L. Taylor, lk 4-6.

[88] *Ibid*, lk 7.

[89] L. Taylor, lk 7-8.

[90] *Ibid*, lk 5.

tehnoloogiat kasutades võib igaüks ilma kelleltki nõusolekut küsimata rahvakogunemistel või rahvarohkemates kohtades inimgruppe profileerida eeldusel, et isik ei ole kaudselt tuvastatav.

Senine andmekaitse keskendub individuaalsetele huvidele ja õigustele ning kahju tekitamisele üksikisikule. Kaitse all on individuaalne autonoomia, inimväärikus, personaalne vabadus, identiteet ja isiku huvi end arendada. Kuigi ka suurandmete puhul on võimalik kahjustada üksikisikut, tehakse siiski suurandmete analüüsil põhinevad otsused profiilide ja mustrite põhjal ning need otsused mõjutavad negatiivselt või positiivselt gruppe või inimeste kategooriaid. Samuti on üksikisikul aina keerulisem olla teadlik kõikidest andmetöötlustest, kus sisalduvad mingil määral tema andmed. Tavainimesel on keeruline hinnata, kas seda töötlust tehakse õiguspäraselt. On kritiseeritud, et praegune individuaalne andmete kontroll ja nõusoleku andmise põhimõte on kitsas ning lisanduma peaks laiem tõlgendus privaatsusest. Seetõttu on pakutud, et üksikisiku huvide kaitsele peaks lisanduma ka grupi huvide kaitse – näiteks küsimused, kas grupp saab autonoomselt käituda või kas gruppi koheldakse väärikalt. Pakutud on ka kahju tekitamise eest kaitse laiendamist grupi tasandile. [91]

On kritiseeritud[92], et instrumendid, mis on loodud kaitsma indiviide andmete väärkasutuse eest, ei ole selle probleemi lahendamisel abik, kuna rikkumine toimub grupi tasemel, üksikisikud jäävad anonüümseks ja seetõttu ei ole kohustust andmetöötlejal teada anda, et nende andmeid töödeldakse. Samuti on keeruline teada saada, kas andmete väärkasutus riivab konkreetset isikut, ning mitmed suurandmete kasutused, mis sisaldavad algoritmide abil moodustatud gruppe, lähevad andmekaitse reeglite erandite alla, näiteks töötlemine avalikes huvides toimuva arhiveerimise, teadus- või ajaloouuringute või statistilisel eesmärgi (üldmääruse artikkel 89).[93] Need põhjused, välja arvatud viimane, on tõesed vaid siis, kui töödeldakse anonüümseid andmeid, mille puhul isik ei ole otseselt ega kaudselt tuvastatav. Kui andmetöötluse eesmärgist tulenevalt või selle täitmise jaoks on vajalik isikute tuvastamine ja nende teatud viisil kohtlemine, võib eeldada, et on täidetud mõistlik tõenäosus isiku tuvastatavuseks, töödeldavad andmed on seotud tuvastatava isikuga ning sellisele andmetöötlusele peab kohaldama andmekaitsereegleid[94]. Seega selliste töötlemiste puhul, kus eesmärk on inimesi tuvastada ja

[91] *Ibid*, lk 6.

[92] *Ibid*, lk 27.

[93] *Ibidem*.

[94] Opinion 4/2007 on the Concept of Personal Data. - Article 29 Data Protection Working Party, 20.06.2007 lk 16. Kättesaadav: https://www.clinicalstudydatarequest.com/Documents/Privacy-European-guidance.pdf (22.03.2019).

teatud viisil kohelda, tuleb siiski andmekaitsereegleid kohaldada, isegi kui töötlemine toimub grupitunnuse alusel.

Algoritmide või mudelite teel loodud grupid annavad võimaluse mõjutada ja kahjustada inimeste gruppe. Profileerimise teel loodud grupp ei ole grupp tavapärases mõistes. Tegemist ei ole ise kokku tulnud inimestega, vaid grupp on loodud algoritmilisel teel ning selle eesmärk ei pruugi olla inimesi tuvastada. Sellised grupid on praktiliselt raskesti hoomatavad, aga samal ajal täpsed, kuna inimesed satuvad sinna teatud eelistuste või omaduste tõttu. Taolisele gruppidele kahjustamisele on näitena toodud Hollandi linnas Eindhovenis grupi loomine selle põhjal, kus piirkondades inimesed öösiti või teatud hetkedel viibisid (rahvarohked tänavad, baarid, klubid) ning neid mõjutati käitumist suunavate lõhnade, valguse ja värvidega. Seega sattusid inimesed sellesse gruppi minnes teatud ajal teatud kohta (öösel linna), kuid neid ei sihitud nende identiteedi tõttu.[95] Selline tegevus ei pruugi olla isikuandmete kaitse rikkumine, ent võib olla privaatsusõiguse riive EIÕK artikkel 8 tähenduses, kuna piiratakse inimese autonoomiat, tema õigust iseenda üle valitsemisele. EIÕK artiklis 8 sätestatud privaatsusõiguse kaitse all on sellised juhud, kui mõjutatakse inimese identiteeti, isiksust või enese potentsiaali realiseerimist[96]. Seejuures ulatub EIÕK artikkel 8 kaitseala ka avalikku ruumi[97]. Harta artikkel 52(3) kohaselt on hartas sisalduvate selliste õiguste, mis vastavad EIÕK-ga tagatud õigustele, tähendus ja ulatus samad, mis neile EIÕK-ga ette on nähtud. Harta artikkel 7 ja EIÕK artikkel 8 sätestavad mõlemad privaatsusõiguse ning harta artikli 7 sisu ja ulatus on vähemalt sama, kui EIK praktika EIÕK artikkel 8 ulatuse kohta[98]. Seega taolistel juhtumitel, kui isik ei ole mõistliku tõenäosusega kaudselt tuvastatav, st ei kohaldu EL isikuandmete kaitse regulatsioon, võib siiski olla tegu privaatsusõiguse riivega, mis on sätestatud EIÕK artiklis 8 ning harta artiklis 7.[99]

On argumenteeritud, et kuigi üksikisik ei ole tuvastatav, on võimalik temani siiski jõuda ning selle näitena toodud, et inimesi võimalik kaardistada liikumise ja asukoha järgi ning haiguspuhangute puhul on võimalik asukoha või isiku käitumise andmete põhjal inimesi nö sundgarantiini panna ehk nende liikumist limiteerida olenemata sellest, kas inimene on päriselt

[95] L. Taylor jt, lk 14-15.

[96] Euroopa Inimõiguste Komisjon 19.05.1976, 6959/75, *Brüggemann and Scheuten v. Germany*.

[97] EIKo 25.09.2001, 44787/98, *P.G. and J.H. v. the United Kingdom*, para 56-57.

[98] EKo 05.10.2010, C-400/10, *J. McB. v L. E.*, para 53; EKo 15.11.2011, C-256/11, *Murat Dereci and Others v Bundesministerium für Inneres*, para 70.

[99] *Infra*, ptk 2.3.

nakatunud või mitte.[100] EL andmekaitseregulatsiooni kohaldamisalas on need näited aga väärad, kuna kujutavad inimese tuvastatavuse kriteeriumit liiga kitsendavalt. Asukohaandmed on samuti isikuandmed ning kirjas ka üldmääruse ja õiguskaitseasutuste direktiivi isikuandmete definitsioonis (üldmääruse artikkel 4(1) ja direktiivi artikkel 3(1)). Asukohaandmete abil on võimalik inimene kaudselt tuvastada. Samuti, kui töödeldakse automatiseeritult inimeste liikumist, on tegu profiilianalüüsiga üldmääruse artikkel 4(4) tähenduses. Andmesubjektil on õigus, et tema kohta ei tehtaks otsust, mis põhineb üksnes automatiseeritud töötlusel, sh profiilianalüüsil, mis toob kaasa teda puudutavaid õiguslikke tagajärgi või avaldab talle märkimisväärset mõju vastavalt üldmääruse artiklile 22(1). Seega ei ole inimeste liikumise kaardistamise ja selle põhjal neid mõjutavate otsuste tegemine pole tegu seaduslüngaga, vaid selline töötlemine on EL andmekaitseregulatsiooni kohaldamisalas ning asukohaandmete töötlemisel tuleb EL õiguse kohaldamisalas andmekaitsereegleid järgida.

Algoritmilisel teel loodud gruppide ebaeetilisuse või kahjulikkuse näiteid väljaspoolt Euroopa Liitu on mitmeid - näiteks poliitilistest huvidest kannustatuna sihiti gruppe Keenias 2007-2008, Rwhanda genotsiidi ajal 1994 ja Kesk-Aafrika Vabariigis 2004. Ähvardavaid sõnumeid saadeti eesmärgiga külvata gruppide tasandil hirmu Ukrainas 2013 ja Egiptuses 2011.[101] Kuigi nende näidete puhul ei olnud oluline üksikisikute identiteet, oli andmete töötlemise eesmärk inimesi teatud mõjutada viisil, mis vajab nendeni jõudmist[102] – sõnumid saadeti grupitunnuse alusel kaudselt tuvastatavatele inimestele. Seega langeksid sellised näited Euroopa Liidus üldmääruse materiaalsesse kohaldamisalasse.

Üks näide isikuandmete manipulatiivsest töötlemisest on 2014. aastal Facebooki kasutajatega tehtud eksperiment, mis hõlmas u 155 000 inimest. Eksperimenteerijad muutsid inimeste Facebooki ajajoontel olevaid postitusi nende teadmata ja leidsid, et nii sai inimeste meeleolu muuta nii negatiivselt kui ka positiivselt.[103] Taoline tegevus on samuti üldmääruse ja õiguskaitseasutuste direktiivi materiaalses kohaldamisalas analoogiliselt eelnevatele näidetele. Inimesed olid tuvastatavad – u 155 000 andmesubjekti. Kui taolist eksperimenti tehtaks EL õiguse kohaldamisalas täna, oleks see üldmääruse rikkumine, kuna andmeid töödeldi ilma õigusliku aluseta, täitmata andmekaitse põhimõtteid (nt õiglane ja läbipaistev töötlemine,

[100] L. Taylor jt, lk 27-30; S. Barocas, H. Nissenbaum. Big Data's End Run around Anonymity and Consent. Cambridge: Cambridge University Press, 2014.

[101] L. Taylor jt, lk 29.

[102] Opinion 4/2007 on the Concept of Personal Data, lk 16.

[103] *Ibid*, lk 17-18,

eesmärgipärasus) ning järgimata andmesubjekti õigusi (nt õigus teabele, õigus mitte olla automatiseeritud töötluse objekt, kui see avaldab märkimisväärset mõju).

1.3. Grupiprivaatsuse kaitse ettepanekud

Ajaloolises vaates pole gruppide kaitse midagi uut ja kummalist, vaid põhiõiguste kaitse on suuresti olnud motiveeritud vähemuste kaitse vajadusest. Põhiõigusi võib vaadelda kui instituuti tasakaaluks demokraatiale, kus enamus otsustab. Seetõttu on põhiõigusi kutsutud ka vähemuste õigusteks. Mitmed inimõigustele keskendunud lepped ja rahvusvahelised õigusaktid nagu ÜRO inimõiguste deklaratsioon, EIÕK, kodaniku- ja poliitiliste õiguste rahvusvaheline sätestavad (sh vähemustele) minimaalsed vabadused, millest (demokraatlik) otsustaja ei saa mööda vaadata.[104]

On väidetud, et isegi kui kõik grupiliikmed on kaitstud soovimatu eraellu sekkumise ja sihtimise eest, ei tähenda see, et grupp tervikuna on kaitstud. Vahel aitab individuaalse privaatsuse tagamine tagada grupiprivaatsust. Isikuandmete kaitse üldmääruses on tugevamalt kaitstud isikuandmete eriliigid, mis võimaldavad isikut diskrimineerida tema grupikuuluvuse tõttu. Artikli 8(1) kohaselt on keelatud on töödelda isikuandmeid, mille põhjal on võimalik inimese diskrimineerimine, näiteks andmeid, millest ilmneb rassiline või etniline päritolu, poliitilised vaated, usulised või filosoofilised veendumused või ametiühingusse kuulumine, geneetilisi andmeid, füüsilise isiku kordumatuks tuvastamiseks kasutatavaid biomeetrilisi andmeid, terviseandmeid või andmeid füüsilise isiku seksuaalelu ja seksuaalse sättumuse kohta, välja arvatud teatud tingimustel, nt nõusolek (artikkel 8(2)). Selle sättega on püütud kaitsa nii individuaalseid õigusi kui ka (vähemus)gruppide õiguseid.

Siiski on leitud, et individuaalse privaatsuse ja gruppide privaatsuse kaitse puhul tegu kahe eraldi privaatsuse probleemiga[105]. Osaliselt võib selle kriitikaga nõustuda, kuna isikuandmete kaitse üldmäärus keskendub kahjule, mis võib tekkida tuvastatud või tuvastatavale üksikisikule, on võimalik inimesi kahjustada algoritmide või mudelite abil loodud gruppe sihtides ilma üksikisikute identiteeti teadmata. Samas on eeltoodud näidete ja kriitika taustal näha, et isiku tuvastatavuse aspekti nähakse liialt kitsana. Isikuandmed on sh igasugused andmed, mille puhul inimene on mõistliku tõenäosusega kaudselt tuvastatav võttes seejuures arvesse töötlemise

[104] *Ibid*, lk 8.

[105] L. Kammourieh jt. Group Privacy in the Age of Big Data. – Philosophical Studies Series, 2017/126, lk 52-53.

eesmärki, tehnoloogiat, kulukust jne. Ka siis kui andmete kombineerimisel muu või muude andmebaasidega, on isik tuvastatav (nt pseudonümiseeritud andmete puhul), on tegu isikuandmetega. Seega pole õige väita, et inimesed on grupitunnuste alusel mõjutamisel kaitseta. Selline väide oleks EL andmekaitseregulatsiooni kohaldamisala liialt kitsendav.

Arvatud on, et gruppide kahjustamise probleemi tõttu on vaja vaadata kaugemale individuaalsest tuvastatavusest ning adresseerida suuremat küsimust, milleks on vastutus andmete väärkasutamise eest. Pakutud on muuta eetilisi standardeid selliselt, et need oleksid kooskõlas tehnoloogilise reaalsusega. Samuti on leitud, et grupiprivaatsuse tunnustamine aitaks kaasa individuaalse privaatsuse ja teiste õiguste tagamisel.[106]

On leitud, et parema grupi privaatsuse tagamiseks on vajalik nii individuaalse privaatsuse tugevam kaitse ja kui ka grupiprivaatsuse kaitse ning need peavad käima käsikäes. See tähendab õigusnorme nii siseriiklikul kui ka rahvusvahelisel tasandil ning nende jõustamist nii era- kui ka avalike kanalite kaudu. Lisaks nö ülevalt alla seadusandlusele on pakutud rohkem kasutada ka tehnoloogilisi lahendusi turvalisuse, läbipaistvuse ja vastutuse tagamiseks ning tõsta inimeste seas teadlikkust ja andmekasutuse kompetentsi.[107] Rõhutatud on nö pehmeid meetodeid nagu juhendid ja koostööprojektid, et tõsta ettevõtete vastutustunnet. Näitena heast praktikast on toodud ÜRO Juhend Äri ja Inimõiguste kohta[108] ning vabatahtlik projekt „The Internet Jurisdiction Project“[109], kus eraettevõtted konsulteerivad rahvusvaheliste ekspertidega, kuidas kaitsta sõnavabadust. On pakutud, et samasuguseid formaate ehk juhendeid ja vabatahtlikke projekte võiks rakendada ka kollektiivse privaatsuse paremaks tagamiseks.[110] Privaatsuse ja andmekaitse osas teavitustöö ja muud pakutud pehmed meetodid on olulised ning tarvilikud. Üldmääruses ka soodustatakse määrusest tulenevate kohustuste selgitamist näiteks toimimisjuhenditega (artikkel 40) ja andmekaitsenõukogu loomisega (artikkel 60jj).

On seisukohti, et kollektiivse privaatsuse kaitset ei saa jätta ainult avalikule võimule ja ettevõtetele, vaid vaja on ka abistavat tehnoloogiat. Pakutud on kasutada rohkem õigustehnoloogiat, mis integreerituna isikuandmete süsteemidesse aitaks automaatselt kinnitada, kas andmetöötlus vastab kasutustingimustele. Näiteks openPDS tehnoloogia abil

[106] L. Taylor jt, lk 33.

[107] L. Kammourieh jt, lk 55-56.

[108] Guiding Principles on Business and Human Rights: Implementing the United Nations “Protect, Respect and Remedy” Framework. – United Nations Human Rights, Office of the High Commissioner. New York, Geneva: United Nations, 2011.

[109] Kättesaadav: https://www.internetjurisdiction.net/ (10.03.2019).

[110] L. Kammourieh jt, lk 58-59.

töödeldakse andmeid lokaalselt andmesubjekti serveris, mitte kolmanda poole serveris. Nõnda saavad teenusepakkujad ja rakendused näha vajadusel kasutaja andmeid, ent ei salvesta neid oma serveritesse ega omanda neid andmeid.[111] Samas on ka seisukohti, et rohkem peaks liikuma tehnoloogilistel lahendustel põhinevast privaatsusest ehk lõimitud andmekaitsest (ingl *privacy by design*)[112] vastutusel põhineva privaatsuse poole ehk rohkem demokraatlikkust ja vähem tehnokraatlikkust[113]. Isikuandmete tõhusaks kaitseks on vaja mõlemat – nii tehnoloogiasse sisse ehitatud privaatsust kui ka vastutust ehk karistust rikkumise eest. Mõlemad aspektid sisalduvad andmekaitse üldmääruses vastavalt artiklites 25 ja 82.

Privaatsusõiguse või isikuandmete kaitse rikkumist, rikkumise ohvrit ja ohvrile tekitatud kahju võib olla keeruline tuvastada, kui tegu on grupipõhise töötlemisega. EIÕK alusel saavad kohtusse oma õiguste kaitseks pöörduda lisaks üksikisikutele ka vabaühendused, isikurühmad ja riigid (konvensiooni artiklid 34 ja 35), ent EIÕK alusel on võimalik EIK-i kaebus esitada vaid riikide tegevuse kohta, mitte teiste füüsiliste isikute või ettevõtete tegevuse kohta. Kaebuse vastuvõetavuse kohta on EIK praktika ajas muutunud. Kaebuse vastuvõetavuse hindamisel on ohvri kriteerumi täitmise juurest liigutud selleni, et piisavaks on mõju tekitava seaduse või poliitika olemasolu[114]. Juhul kui inimene ei tea, kas ta oli riigi tegevuse ohver ning tal pole seda ka võimalik kindlaks teha, võib EIK lubada *in abstracto* kaebust[115,116].

Üldmääruse artikkel 80(1) alusel on õigus ühendustel andmekaitse rikkumise puhul liikmesriigi kohtusse pöörduda, kuid tegu on siiski andmesubjekti esindamisega ning andmesubjekt on vaid füüsiline isik, sest isikuandmed on üldmääruse kohaselt füüsilise isiku kohta käivad andmed. Üldmääruse artikkel 80(2) alusel on võimalik organisatsioonil ka ilma andmesubjekti volituseta kohtusse pöörduda, kui liikmesriik on selle õiguse organisatsioonile andnud, ning organisatsioon leiab, et andmesubjekti õigusi on rikutud. Seega õigus tuleneb siiski kellegi individuaalse privaatsuse riivamisest, mitte ei ole õigus grupil endal. Samas ei saa väita, et

---

[111] Y-A. Montjoye jt. On the Trusted Use of Large-Scale Personal Data. – IEEE Data Engineering Bulletin, 2012/35, lk 5-8; D. Greenwood jt. The New Deal on Data: A Framework for Institutional Controls. – Cambridge: Cambridge University Press, 2014; L. Kammourieh jt, lk 60-61.

[112] Tehniliste võimaluste kohta privaatsuse tagamisel vt nt K. Hao. A Little-known AI Method Can Train on Your Health Data without Threatening Your Privacy. – MIT Technology Review, 11.03.2019.

[113] L. Taylor jt. Conclusion: What Do We Know About Group Privacy? – Philosophical Studies Series 2017/126, lk 236.

[114] EIKo 06.11.1978, 5029/71, *Klass and others v. Germany*, para 36; EIKo 10.02.2009, 25198/02, *Lordachi and others v. Moldavia*, para 34; EIKo 01.07.2008, 58243/00, *Liberty v. Great Britain*, para 57.

[115] EIKo 12.01.2016, 37138/14, *Szabó and Vissy v Hungary*; EIKo 04.12.2015, 47143/06, *Roman Zakharov v Russia*.

[116] Vt sel teemal pikemalt B. van der Sloot. Editorial European Data Protection Law Review 2016_1. – European Data Protection Law Review 2016/1, 10 lk.

grupitunnuse alusel töötlemisel oleksid inimesed täiesti kaitseta – see väide oleks üldmääruse ja direktiivi kohaldamisala liialt kitsendav. Arvestades grupitunnuse alusel töötlemisel riive tuvastamise, nö ohvri leidmise ja kahju kindlakstegemise keerukust võiks üldmääruse artikli 80(2) kirjeldatud õigus organisatsioonidele andmesubjekti volituseta kohtusse pöördumine olla iga liikmesriigi õiguses sätestatud. Praegu on sellise võimaluse loomine liikmesriikidele vabatahtlik.

1.4. Andmesubjekti õigus mõistlikele järeldustele

Andmekaitse reguleerib nn sisendandmeid (ingl *input data*), ent mitte väljundandmeid (ingl *output data*) ehk andmesubjektil ei ole õigust mõjutada seda, kuidas teda kategoriseeritakse. Pole olemas ka kontrollmehhanismi, mis jälgiks, et inimesi õigesti kategoriseeritaks või hinnataks. Lahendusena võiks EK võtta rohkem üle EIK lähenemise ehk vaadata töötlemisel tehtud järelduste probleemi vähem isikuandmete kaitse ja rohkem identiteedi vaatenurgast. Pakutud on, et andmesubjekti õiguste hulka peaks lisanduma õigus mõjutada, kuidas andmesubjekti kategoriseeritakse või profileeritakse.[117]

Seni on EL õiguses üksikisikutele antud vähe kontrolli ja järelevalvet selle üle, kuidas nende isikuandmeid nende kohta järelduste tegemiseks kasutatakse. Andmesubjektidel on kontroll selle üle, kuidas isikuandmeid kogutakse ja töödeldakse, kuid väga vähe kontrolli selle üle, milliseid järeldusi nendest isikuandmetest tehakse. Seetõttu on pakutud, et lisanduma peaks õigus mõistlikele järeldustele (ingl *the right to reasonable inferences*). See tähendaks, et juhtudel, kus algoritmid teevad isiku kohta kõrge riskiga järeldusi, oleks nõutud andmetöötlejalt *ex-ante* põhjendus, miks järeldus oli mõistlik.[118]

Mõistlike järelduste õigusele on seni vähe tähelepanu pööratud. Isikuandmete kaitse üldmäärus, e-privaatsuse regulatsioon, digitaalse sisu direktiiv annavad andmesubjektidele vaid piiratud õigusi järelduste osas, mida nende andmete põhjal tehakse. Samal ajal hõlbustab EL autoriõiguse direktiiv andmete kaevandamist, andmesubjektide õiguse piiramist ja suurandmete analüüsi ning uus ärisaladuste direktiiv kujutab piirangut vastutusele, mis puudutab mudeleid, algoritme ja järeldusi.[119] Tähelepanu on juhitud andmete põhjal kalduvuste (ingl *propensities*) analüüsimisele, mida tehakse üksikisikute ja gruppide andmete põhjal. Üks selline kalduvuste

[117] S. Wachter, B. Mittelstadt. A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI. – Columbia Business Law Review, 2019, lk 4. (Käsikiri avaldamisel.)

[118] *Ibidem.*

[119] *Ibid*, lk 79.

analüüsi näide on ennetav politseijälgimine (ingl *predictive policing*[120]).[121] Sarnane probleem tõusetus ka grupiprivaatsuse analüüsil seoses seirekapitalismiga, kus kaevandatakse inimeste käitumuslikke andmeid, vajadusi ja soove ning tehakse nende andmete põhjal tegusid, mis võivad olla manipulatiivsed.[122] Näiteks võidakse tuvastada inimese kalduvus depressioonile ja vastavalt sellele talle teistsuguseid reklaame näidata. Ennetava politseijälgimise puhul tuvastatakse näiteks statistiliste näitajate põhjal inimese potentsiaalne kalduvus süüteo toimepanemiseks ja koheldakse teda seetõttu teistest erinevalt.

Pakutud on, et vähem tuleks andmekaitse puhul tähelepanu pöörata individuaalsele nõusolekule ning tähelepanu tuleks enam suunata järeldustele, mida on võimalik avalike andmetega teha[123]. Põhiprobleem on senine EK praktika. *Bavarian Lager*[124], *YS. and M. and S.*[125] ja *Nowak*[126] kohtuasjades ning kohtujuristi arvamustes kohtuasjades *YS. and M. ja S.*[127] ning *Nowak*[128] on selgitanud, et andmekaitse õiguse eesmärk ei ole tagada seda, et andmetel tehtud järeldused ja otsused oleksid õiged või põhjendatud. EK praktika kohaselt on andmekaitse regulatsioon vahend andmekaitse subjektidele, et tagada andmete saamise õiguspärasus ning töötlemise õiguslik alus, kuid mitte järelduste ja otsuste õigsus ja põhjendatus.[129] Tegu on iroonilise olukorraga, kuna on eluliselt ja praktiliselt oluline, et andmete põhjal tehtud otsused oleksid õiged[130].

Pakutud on laiendada andmekaitse regulatsiooni selliselt, et see hõlmaks ka automaatsete otsuste tegemise õigsust. Nii saaksid andmesubjektid tugevama kontrolli, kuidas automaatsed

---

[120] Ennetav politseijälgimine kasutab andmeanalüüsi, et ennustada ja ennetada süütegusid. Ennustusi tehakse selle kohta millal ja kus kohas võib süütegu aset leida ning ka selle kohta, kes võib olla tõenäoliselt süüteo toimepaneja või ohver. Vt: G. Ridgeway. Policing in the Era of Big Data. – Annual Review of Criminology, 2018/1, lk 401-419. Seonduvatets probleemidest vt ka S. Brayne. Big Data Surveillance: The Case of Policing. – American Sociological Review, 2017/82, No 5, lk 977-1008.

[121] V. Mayer-Schönberger, K. Cukier. Big Data. – Boston, NY: Mariner Books, 2014.

[122] *Supra*, lk 14-16.

[123] J-E. Mai. Big Data Privacy: the Datafication of Personal Information. – The Information Society, 2016/32, No 3, lk 192-199.

[124] EKo 29.06.2010, C-28/08 P, *Commission v Bavarian Lager*, para 49.

[125] EKo 17.07.2014, ühendatud kohtuasjad C-141/12 ja C-372/12, *YS v Minister voor Immigratie, Integratie en Asiel and Minister voor Immigratie, Integratie en Asiel v M and S*, para 45-47.

[126] EKo 20.12.2017, C-434/16, *Peter Nowak v Data Protection Commissioner*, para 54-55.

[127] EK 17.07.2014, ühendatud kohtuasjad C-141/12 ja C-372/12, *YS v Minister voor Immigratie, Integratie en Asiel and Minister voor Immigratie, Integratie en Asiel v M and S*. Kohtujurist Sharpston arvamus, para 32, 60.

[128] EK 20.12.2017, C-434/16, *Peter Nowak v Data Protection Commissioner*. Kohtujurist Kokott arvamus, para 54-55.

[129] S. Wachter, B. Mittelstadt, lk 79.

[130] *Ibid*, lk 81-85.

süsteemid neid näevad ja käsitlevad. Leitud on, et enam peaks keskenduma töötlemise eesmärkidele ja mõjule ning vähem andmeliikidele, kuna uute andmetöötlustehnoloogiate ajastul võivad ka anonüümsed või mitte-isiklikud andmed inimest mõjutada ja kahjustada. Seega primaarne peaks olema andmete kasutus ja mõju ning sekundaarne andmete saamise viis.[131] Rohkem töötlemise mõjule ja eesmärkidele keskendumine aitaks ka paremini kaitsta gruppe negatiivsete mõjude eest.

On ka seisukohti, et ei peaks keskenduma ainult tuvastatavusele, kuna see on väidetavalt tekitanud seaduslünga, mida ettevõtted kasutavad andmekaitse õiguste tagamisest mööda hiilimiseks ning mistõttu andmesubjektidel ei ole kaitset automaatseid järeldusi ja otsustusi tegevate analüütikatehnoloogiate eest. See ettepanek ei tähenda, et peaks olema õigus midagi nõuda, kui anonüümseid andmeid pole andmesubjekti vastu kasutatud, kuid peaks olema paremad õiguskaitsevahendid, kui kolmandatelt osapooltelt saadud andmete ja anonüümsete andmete abil on rakendatud isiku suhtes mudeleid, profiile või muid taustteadmisi, mida on seejärel rakendatud tuvastatavale isikule.[132]

On leitud, et töötlejatel peaks olema kohustus põhjendada andmeallikaid ja kavandatavaid järeldusi enne järeldusi loova analüütika laialdast kasutamist. Seejuures peaks tähelepanu pöörama privaatsuse riive intensiivsusele nende andmete kasutusel ja järelduste tegemiseks kasutatavad allikad peaks olema mõistlik, eriti näiteks klõpsamise-, sirvimiskäitumise või hiire jälgimise puhul. Järelduste tegemise eesmärk peaks privaatsuse riive seisukohast õigustatama kasutatavate andmete allikaid. Näiteks järeldus hasartmängude või alkoholisõltuvuse kohta, et kasutada selle kohast sihitud reklaami, võib olla andmesubjekti liigselt kahjustav. Samuti tuleks tähelepanu pöörata puhverserverite andmete kasutusele (nt postikood) ja mittetundlikest andmetest tundlike andmete tuletamisele (nt poliitilised vaated), lähteandmete ja järelduste asjakohasusele tööltemise eesmärgi osas, nt Facebooki profiilide ja sõprade võrgustike põhjal laenuotsuste tegemine ei pruugi olla asjakohane, ning kriitiline tuleks ka olla järelduste tegemiseks kasutatud meetodite statistilisele usaldusväärsuse osas.[133]

Teatud määral on järelduste nõuet ka rakendatud. Näiteks Prantsuse haldusõigus annab eraisikule õiguse selgitusele tema kohta tehtud (haldus-)algoritmiliste otsuste kohta. See säte

[131] *Ibidem.*

[132] *Ibidem.*

[133] *Ibidem.*

on ulatuslikum kui andmekaitse üldmääruse vastavad sätted automatiseeritud otsuste tegemise kohta, kuid seda kohaldatakse ainult haldusotsuste suhtes.[134]

Pakutud on, et tuleks anda võimalus pöörduda ebamõistlike järelduste osas kohtusse. Selle saavutamiseks tuleb andmekaitse regulatsiooni eesmärk uuesti määratleda nii, et selles sisalduks järelduste põhjendamise kohustus. Andmesubjekti positsiooni tugevdamine vastutavate töötlejate suhtes on vajalik, et leevendada automaatseid järeldusi tegevate analüütikatehnoloogiate riske.[135] Negatiivse aspektina võib selline kohustus kaasa tuua suurema bürokraatia ja ettevõtete halduskoormuse.

Andmekaitse üldmääruse eesmärk on privaatsuse ja isikuandmete tõhusam kaitse arvestades tehnoloogilist arengut. Isikuandmete töötlemine peaks olema mõeldud inimesi teenima (Üldmääruse preambuli pp 4-6). Ent regulatsioon kasutab ebaefektiivseid strateegiaid, nagu keskendumine sisendandmetele, et neid eesmärke saavutada. EK ei ole tunnustanud õigust mõistlikele järeldustele ning inimeste üle järelduste tegemisele, näiteks tööproduktiivsuse hinnang, finantsiline seis, eluea pikkuse prognoos jäävad väljaspoole andmekaitse üldmäärust ning üldmäärus on pigem keskendunud andmete kogumise faasile[136].

Eeltoodud ettepanekud, eelkõige õigus mõistlikele järeldustele ning suurem keskendumine sellele, mida andmetega tehakse, võivad olla lahenduseks mitmetele emotsiooni- ja näotuvastuse probleemidele, kuna ei ole mitte ühe tehnoloogia põhised, vaid adresseerivad kõiki selliseid andmeanalüütika tehnoloogiaid, mis on suunatud grupi tasandile. Liikmesriikidel on õigus kehtestada siseriiklikult rangemad andmekaitse nõuded, seega ei ole takistust gruppide paremaks kaitseks ja andmetöötluse järelduste *ex ante* põhjendamise osas rangemaid nõudeid kehtestada.

Eelneva analüüsi tulemusena võib teha järgnevad tähelepanekud: tuleks vältida üldmääruse ja direktiivi materiaalse kohaldumisala kitsendavat tõlgendamist – see et isikuandmeid töödeldakse grupitunnuse põhjal, ei pruugi tähendada, et tegevus on väljaspool üldmääruse ja direktiivi kohaldamisala, eriti, kui töötlemine mõjutab konkreetseid isikuid (nt sõnumite saatmine, sotsiaalmeedias postituste sihtimine konkreetsetele inimestele grupitunnuse põhjal). Isegi kui isikud ei ole tuvastatavad ning seetõttu andmekaitse regulatsioon ei kohaldu, võib tegu

[134] Privacy and Freedom of Expression in the Age of Artificial Intelligence. – Article 19, 04.2018, lk 23. Kättesaadav: https://privacyinternational.org/report/1752/privacy-and-freedom-expression-age-artificial-intelligence (4.03.2019).

[135] S. Wachter, B. Mittelstadt, lk 81-85.

[136] S. Wachter 2019, lk 2.

olla privaatsusõiguse riivega EIÕK artikkel 8 ja harta artikkel 7 mõttes, kuna mõjutatakse inimese autonoomsust (nt linnas valguse ja lõhnadega mõjutamine). Gruppide paremaks kaitseks võiks olla siseriiklikult võimalus organisatsioonidel, kellel on põhikirjaga võetud eesmärk tegeleda põhiõiguste kaitsega, minna isikuandmete kaitse õiguse või privaatsusõiguse kaitseks kohtusse ka siis, kui ohvrit või konkreetset kahju pole võimalik tuvastada. Hetkel on selle võimaluse loomine vabatahtlik. Gruppide privaatsust võib aidata edendada ka uute tehnoloogiliste võimaluste kasutamine, näiteks automaatne kontroll, kas andmekaitsetingimused vastavad EL õigusele. Samuti on oluline jätkata pehmete meetoditega nagu ettevõtetele juhendite loomine ja koostööprojektid, kus andmekaitseeksperdid ettevõtteid nõustavad. *Ex ante* järelduste mõistlikkuse põhjendamise kohustuse tunnustamine EK poolt ja selle sisse viimine üldmäärusesse aitaks tagada seda, et andmetöötlusel tehtud otsused on mõistlikud ning usaldusväärsed – see õigus aitaks praktiliselt efektiivsemalt aidata andmesubjekte ebamõistlike järelduste vaidlustamisel nagu näiteks laenuotsuse puhul, mis tehti vaid isiku Facebooki konto baasil.

2. AUTOMATISEERITUD EMOTSIOONITUVASTUS

Inimeste igapäevaelus ja otsuste tegemisel omavad emotsioonid ja tunded olulist rolli, mistõttu on nende vastu huvi nii ettevõtetel, õiguskaitseasutustel kui ka eri agendadega organisatsioonidel ja isikutel (näiteks erakondadel). Emotsioonituvastuse[137] eesmärk on automaatselt klassifitseerida inimese emotsionaalne seisund.

Emotsioone on võimalik algoritmide abil tuvastada mitmetel viisidel, näiteks video, pildi, hääle, füsioloogiliste andurite abil biosignaale mõõtes (ingl *biometric sensing*, näiteks vererõhk, pulsilöögid, kehatemperatuur, lihaste kokkutõmbed) ja standardsete sisendandurite abil (näiteks arvutiklaviatuur- ja hiir).[138] Seejuures võib olla andmesubjekt nii tuvastatud, tuvastatav kui ka anonüümne. Näiteks on võimalik sentimentaalse analüüsi ehk arvamuskaeve meetodite abil tuvastada sentimentaalsust teksti põhjal, mille autor on anonüümne ning teda pole võimalik ka kaudselt tuvastada[139]. Sellisel juhul tuvastatakse küll emotsioonid, ent mitte isik, kes teksti kirjutas.

Emotsioone näo mikroilmete põhjal tuvastavad kaamerad on juba kasutuses ning neid kasutatakse ka ärilistel eesmärkidel[140]. Emotsioonituvastust kasutavad ja müüvad näiteks Amazon, Microsoft ja IBM, samuti paljud väiksemad firmad nagu Kairos, Eyeris ja Affectiva[141]. A. McStay on koostanud kokkuvõtliku tabeli, millistes valdkondades ja millisel eesmärgil emotsioonituvastust kasutatakse[142] ning on täpsemalt emotsioonituvastuse kasutusvaldkonnad lahti kirjutanud 2018. aastal ilmunud raamatus „Emotional AI: The Rise of Empathic Media“, kust on võimalik huvi korral lisa lugeda.

---

[137] Emotsioonituvastuse tehnoloogilisest poolest vt nt M. Somers. Emotion AI, explained. Cambridge: MIT Sloan School of Management, 2019.

[138] J.M. Garcia-Garcia jt. Emotion Detection: a Technology Review. Conference Paper. NY: ACM, 2017.

[139] Sentimentaalse analüüsi kohta vt nt S-T. Marran. Sentimentaalne analüüs eestikeelse peavoolumeedia veebiartiklite kommentaaride baasil. Bakalaureusetöö. Tartu Ülikool: Tartu 2012.

[140] D. Thomas. The Cameras that Know if You're Happy – or a Threat. – BBC News, 17.07.2018.

[141] O. Schwartz. Don't Look Now: Why You Should Be Worried About Machines Reading Your Emotions. – The Guardian, 6.03.2019.

[142] Vt Lisa 1; A. McStay, lk 3.

2.1. Füüsilise isiku tuvastatavus ja anonüümsed andmed

Andmekaitse põhimõtteid tuleb kohaldada tuvastatud või tuvastatavat füüsilist isikut puudutava igasuguse teabe suhtes. Isikuandmete definitsioonis on sätestatud, et tuvastamine võib olla otsene või kaudne ning tuvastamine toimub eelkõige sellise identifitseerimistunnuse põhjal nagu nimi, isikukood, asukohateave, võrguidentifikaator või füüsilise isiku ühe või mitme füüsilise, füsioloogilise, geneetilise, vaimse, majandusliku, kultuurilise või sotsiaalse tunnuse põhjal (üldmääruse artikkel 4(1); direktiivi artikkel 3(1)).

Masinnägemisel ja masinõppel põhineva näovõrdluse puhul töödeldakse inimese biomeetrilisi andmeid, mis on EL õiguse kohaselt isikuandmete eriliik, mida on keelatud töödelda ilma andmesubjekti selgesõnalise nõusolekuta või nõusoleku puudumist lubava erandita (üldmääruse artiklid 4(1)(14), 4(1)(1), 9(2)). Biomeetria tuleneb kreeka keelest ning tähendab "elu mõõtmist". Biomeetria viitab unikaalsete ja eristatavate füüsiliste, bioloogiliste ja käitumuslike omaduste mõõtmisele, mille abil on võimalik inimest tuvastada.[143] Lisaks füüsiliste omaduste võrdlemisele (nt näovõrdlus) on võimalik võrrelda ka käitumuslikke omadusi (nt emotsioonivõrdlus), seega võib teoreetiliselt ka emotsioonituvastuse puhul olla tegu biomeetriliste andmete töötlemisega. Kas see nii on, oleneb konkreetsest emotsioonituvastuse kontektstist, sh töötlemise eesmärgist ja kasutatavast tehnoloogiast.

Üldmääruse ja õiguskaitseasutuste direktiivi materiaalsesse kohaldamisalasse kuuluvad ka pseudonümiseeritud andmed (üldmääruse artikkel (2)(5)), mida saaks füüsilise isikuga seostada täiendava teabe abil, näiteks viies kokku kaks erinevat andmebaasi. Anonüümse teabe suhtes andmekaitse põhimõtted ei rakendu. Anonüümne teave on teave, mis ei ole seotud tuvastatud või tuvastatava füüsilise isikuga, või isikuandmete suhtes, mis on muudetud anonüümseks sellisel viisil, et andmesubjekti ei ole võimalik tuvastada või ei ole enam võimalik tuvastada (üldmääruse preambuli p 26). Füüsilise isiku tuvastatavusel on seega andmekaitse üldmääruse ja õiguskaitseasutuste direktiivi materiaalse kohaldamisala piiritlemisel võtmeroll.

Anonümiseerimise eesmärk on vältida isiku tuvastust tagasipööramatult, kud siiski on anonümiseerimise puhul risk isiku teiste hulgast esiletoomiseks[144]. Esiletoomine tähendab ka võimalust eraldada osa või kõik andmed isiku kohta ülejäänud andmebaasist[145]. Andmekaitse

[143] S. Z. Li (toim). Encyclopedia of Biometrics. – Springer US, 2009.

[144] Opinion 5/2014 on Anonymization Technique. – Article 29 Data Protection Working Party, 10.04.2014.

[145] *Ibidem.*

üldmääruse kohaldamine ei eelda kõrget tuvastatavuse võimalikkust[146]. Näotuvastuse ja emotsioonituvastuse kontekstis ei tähenda see, et isikuid ei ole vaja tuvastada, seda, et tegu pole isikuandmete töötlemisega. Isikuandmete regulatsiooni kohaldamiseks piisab, kui isiku tuvastamine võimalik.[147]

Anonümiseerimine on abiks näotuvastuse õiguspärase kasutuse tagamisel, kuna andmete anonümiseerimine võib viia tegevuse väljaspoole üldmääruse ja direktiivi materiaalset kohaldamisala, vähendada mõju andmesubjektile ja sellega aidata kaasa privaatsuse riive proportsionaalsuse hindamisel, ning võib aidata täita võimalikult väheste andmete kogumise tingimust.[148] Teisest küljest on anonüümsete andmete temaatika problemaatiline, kuna de-identifitseeritud andmeid on võimalik teoreetiliselt tagasi identifitseeritavateks andmeteks muuta ning füüsilise isikuga seostada. Lisaks on võimalik isegi anonüümsete andmete põhjal profiile luua ning diskrimineerida ja inimeste privaatsust riivata ilma selleta, et konkreetset isikut tuvastataks.[149]

On arvamusi, et ka mitte-identifitseeriva emotsioonituvastuse kasutamisel peaksid andmekaitse regulatsioonid rakenduma, sest tuvastamine on alati võimalik. Näiteks hüpoteetiliselt võib olla olukord, kus inimene ootab üksinda bussi ja on bussipeatuses oleva emotsioonituvastustehnoloogiaga täiustatud reklaamitahvli mõjuväljas. Sellisel juhul pärineb reklaami sisendiks olev info ühelt isikult ja on unikaalne ning langeb seetõttu andmekaitse reguleerimisalasse. See peegeldab privaatsusalaste teemade spetsialistide arusaama, et andmete anonüümseks muutmine on keeruline probleem. Probleem peitub selles, et piisaval hulgal infot kombineerides on isiku identifitseerimine alati võimalik. Sellele seisukohale on ka vastu vaieldud, et „isegi juhul kui ainult ühe inimese andmed on reklaamilise seisendiks /---/ pole see seda tüüpi olukord, mille lahendamiseks üldmäärus loodi“ ning seetõttu on väidetavalt tulemuseks regulatiivne tühimik info kohta, mis on küll tundlik (emotsioonid), aga mitte ilmtingimata isikuandmed.[150] Näiteks UK teabevoliniku büroo seisukohal on, et töökohal kehtivad andmekaitse reeglid tuvastatavuse eeldusel. Kuigi töötajatel on nii õigustatud ootus eraelu puutumatusele kui ka (mõningasele) privaatsusele töökeskkonnas, rakendub

[146] Handbook on European Data Protection Law. Käsiraamat. – FRA. Luxemburg: Euroopa Liidu Väljaannete Talitus, 04.2018.

[147] J. Shi jt. How Effective Are Landmarks and their Geometry for Face Recognition? – Computer Vision and Image Understanding, 2006/102, No 2, lk 117–133.

[148] P. Lewinski jt. Face and Emotion Recognition on Commercial Property under EU Data Protection. – Psychology & Marketing, Wiley Periodicals 2016/33, No 9, lk 729-746.

[149] S. Wachter, lk 3.

[150] McStay 2018, lk 209-211.

andmekaitse regulatsioon ainult juhul, kui kogutavad andmed võimaldavad nende tuvastamist või muul viisil teistest eristamist. Kui andmed on piisavalt üldistatud kujul, siis on andmekaitse kohalduvus õiguslikult vaieldav. Ka erisätetega reguleeritud eriliigiline teave mentaalse ja füüsilise tervise kohta peab andmekaitse regulatsiooni rakendumiseks täitma eeldust, et teavet on võimalik siduda isiku või personaalsete andmetega.[151] Samas pole nendes seisukohtades arvestatud sellega, et andmekaitse regulatsiooni kohaldamiseks ei ole vaja tuvastatavuse kõrget taset ning tuleks arvesse võtta ka töötlemise eesmärki. Reklaamiplakatite puhul oleneb, kas inimese emotsionaalset informatsiooni kasutatakse selleks, et teda kuidagi mõjutada. Kui kasutatakse, peaks sellisele töötlemisele kohaldama ka isikuandmete kaitse reegleid.

Tuvastatavuse hindamine oleneb konkreetsest situatsioonist[152]. Tuvastatavuse kindlakstegemisel tuleb arvesse võtta kõiki vahendeid, mida vastutav töötleja või keegi muu võib füüsilise isiku otseseks või kaudseks tuvastamiseks mõistliku tõenäosusega kasutada, näiteks teiste hulgast esiletoomine. Arvesse tuleb võtta kõiki meetmeid, mida mõistliku tõenäosusega on võimalik tuvastamiseks kasutada. Meetmete mõistliku tõenäosuse hindamiseks tuleb arvesse võtta kõiki objektiivseid tegureid, näiteks tuvastamise maksumus ja selleks vajalik aeg, andmete töötlemise ajal kättesaadavat tehnoloogiat ja tehnoloogilisi arenguid (üldmääruse preambuli p 26). Õiguskirjanduses on tuvastatavuse hindamiseks näotuvastuse kontekstis pakutud nelja põhilist aspekti, mida hinnata tuleks: (1) tuvastamise maksumus, (2) andmesubjekti huvi, (3) tehniliste turvameetmete tase, (4) millistel eesmärkidel tehnoloogiat kasutatakse[153].

Andmekaitse regulatsiooni kohaldumiseks on piisav, kui tunnuste põhjal kedagi teiste hulgast esile tuuakse ning tuvastatakse selle isiku käitumine või isiksuse omadused, et tema suhtes teatud otsuseid rakendada. Isikuandmete definitsioonist tulenevalt võib see toimuda ka sotsiaal-majanduslikul, psühholoogilisel või muul taolisel kriteeriumil.[154] Isik on identifitseeritav, kui neid on võimalik teiste grupi liikmete seast eristada ning seeläbi teisiti kohelda. See võib tähendada nii isiku tuvastamist kui ka seda, et isikut koheldakse teistest erinevalt indentiteediga tüüpiliselt mitteseostuvate tunnuste alusel.

Otsustamisel, kas tegu on anonüümsete andmetega, mängib rolli töötlemise eesmärk. Kui andmetöötluse eesmärgist tulenevalt või selle täitmise jaoks on vajalik isikute tuvastamine ja

[151] *Ibidem*.

[152] Opinion 4/2007 on the Concept of Personal Data, lk 13.

[153] J. Trzaskowski jt. Introduction to EU Internet Law. Copenhagen: Ex Tuto Publishing, 2015.

[154] Opinion 4/2007 on the Concept of Personal Data, lk 13.

nende teatud viisil kohtlemine, võib eeldada, et on täidetud mõistlik tõenäosus isiku tuvastatavuseks, töödeldavad andmed on seotud tuvastatava isikuga ning sellisele andmetöötlusele peab kohaldama andmekaitsereegleid.[155] Kui töötlemise eesmärk ei ole isiku tuvastamine ja teatud viisil kohtlemine, võib sõltuda andmete suhtes rakendatud tehnoloogilistest turvameetmetest, kas tegu on isikuandmetega, kuna turvameetmed on üks kriteerium hindamaks, kas on mõistlik tõenäosus isikute tuvastamiseks.[156]

Samas on igasugune tehnoloogiline süsteem on haavatav ja rünnatav. Näiteks Eesti ID-kaarti ohustanud turvanõrkus puudutas üle maailma vähemalt miljardit kiipi, mis on käigus arvutite turvamoodulites, e-posti turbeks ja virtuaalse privaatvõrgu (VPN) juurdepääsuks kasutatavates krüptovahendites, riiklikes isikut tõendavates dokumentides ja maksekaartides.[157] Seega kui põhimõtteliselt on andmete põhjal võimalik isiku tuvastatavus, tuleb tehnoloogilistesse turvameetmetesse suhtuda äärmise tõsidusega. Ainult siis, kui andmete põhjal isiku tuvastatavus on võimatu, sh kaaludes kõiki võimalusi, on tegu kindlasti anonüümsete andmetega, millele andmekaitse reeglid ei kohaldu. Kui tuvastatavus pole võimatu, tuleb seega teha iga konkreetse olukorra osas läbi kaalumine, kas on mõistlik tõenäosus isiku tuvastatavuseks või mitte. Sarnaselt tuleb kaalumine läbi teha emotsioonituvastuse kontekstis võttes arvesse töötlemise eesmärki ning võimalikke otseseid ja kaudseid viise isiku tuvastamiseks. Teoreeriliselt võib seega olla emotsioonituvastus nii andmekaitse regulatsiooniga hõlmatud kui ka mitte hõlmatud – juhul, kui töödeldakse ainult tõeliselt anonüümseid andmeid, mille põhjal isiku tuvastamine on võimatu või väga ebatõenäoline arvestades kõiki objektiivseid tegureid.

Töötlemise eesmärk on seega tuvastatavuse hindamisel olulise rolliga. Kui emotsioonituvastuskaamera on näiteks tänaval eesmärgiga mööda mineja emotsiooni tuvastada ning vastavalt sellele tema suhtes reklaami muuta eesmärgiga emotsioonide subjekti mõjutada, tuleks lugeda sellist emotsioonituvastust isikuandmete töötlemiseks, millele rakenduvad isikuandmete kaitse üldmääruse nõuded.

Tuues paralleeli asukohaandmetega, mis on isikuandmete liik, on võimalik statsionaarse emotsioonituvastuse kasutamisel teoreetiliselt kokku viia isiku asukoht ning tema emotsionaalne seisund, mis võimaldaks seega isiku kaudset tuvastamist. Samuti on oluline märkida, et videovalve puhul eeldatakse, et töödeldakse isikuandmeid, kui videovalve eesmärk

[155] *Ibid*, lk 16.

[156] *Ibid*, lk 17.

[157] M. Maigre, K. Kaska. Küberkaitsest terviklikult. – Diplomaatia, 14.09.2018.

on teatud olukorras salvestisele või kaamerapilti jäänud isik tuvastada. Kogu videovalve puhul on tegu isikuandmete töötlemisega, isegi siis, kui osad inimesed videol ei ole praktiliselt tuvastatavad.[158] Seega videovalve, millele on lisaks rakendatud emotsioonituvastuse võimalus, on hõlmatud isikuandmete kaitse regulatsiooniga.

Kuigi teaduskirjanduses on väidetud[159], et füüsiliste isikute emotsioonide tuvastamine ja jälgimine ei ole üldmäärusega reguleeritud, kuna emotsioonituvastustehnoloogia kasutamiseks ei ole vajalik piltide või video salvestamine ega füüsilise isiku identiteediga seostamine, oleneb andmekaitse regulatsiooni kohaldamine siiski konkreetsest kontekstist ja seda tuleb hinnata igal konkreetsel juhul, sh võttes arvesse ka töötlemise eesmärki. Kuigi emotsioone on tehniliselt võimalik tuvastada ja jälgida nii, et kogutud andmete põhjal ei võimaldata füüsilise isiku identifitseerimist ega füüsilise isiku identiteedi kinnitamist[160], ei tähenda tehniline tase automaatselt, et tegu on anonüümsete andmetega, vaid tuleb hinnata ka kõiki muid objektiivseid tegureid, et leida, kas isik on mõistliku tõenäosusega tuvastatav, kas teda tuuakse teiste seast esile ning kas tema andmete põhjal avaldatakse talle mõju (nt suunatud reklaam).

Üldmäärus ei kohaldu seega anonüümse info töötlemisele, näiteks statistiliste või teadusuuringute kontekstis, ning ei rakendu, kui emotsioonituvastuses kasutatavad andmed on anonüümsed. Sel juhul ei rakendu ka eriliigiliste isikuandmete regulatsioon, sest kuigi keha ja emotsioonide kohta käivad andmed on tundlikud, ei pruugi need olla isikuandmed, kui isik pole (tema teadmata) püütud emotsioonide põhjal tuvastatav.

Kui isikuandmete kaitse regulatsioon kohaldub, tuleks hinnata ka seda, kas on tegu biomeetriliste andmete töötlemisega (nt juhul kui näotuvastust ja emotsioonituvastust kasutatakse koos). Biomeetriliste andmete töötlemist puudutavad reeglid rangemad, kuna tegemist on eriliigiliste andmetega, mis võimaldavad diskrimineerimist. Biomeetrilisi andmeid ei tohi kasutada isiku tuvastamiseks, kui need seostuvad tervise, seksuaalelu või seksuaalse orientatsiooniga. Kui sellist infot ikkagi vajatakse, tuleb selleks saada subjekti selge nõusolek.[161] Tüüpiliselt lahendatakse nõusoleku probleem paludes isikul tühja kastikesse linnuke teha. Sellist tüüpi nõusolekut on vaja, kui andmed puudutavad isiku rassi või päritolu, poliitilisi vaateid, religioosseid või filosoofilisi uskumusi või ametiühingutesse kuulumist.

[158] Opinion 4/2007 on the Concept of Personal Data, lk 16.

[159] Vt nt E. Sedenberg, J. Chuang. Smile for the Camera: Privacy and Policy Implications of Emotion AI Elaine Sedenberg. Berkeley: University of California, Berkeley, lk 10.

[160] *Ibidem*.

[161] R. Coseraru. Facial Recognition Systems and their Data Protection Risks Under the GDPR. Magistritöö. Tilburg: Tilburg University, 2017, lk 50-51. Identifitseeritavuse problemaatika kohta vaata *Ibid*, lk 48 jj.

Sama kehtib geneetiliste ja biomeetriliste andmete töötlemisele, kui selle eesmärgiks on isiku tervise, seksuaalse orientatsiooni või konkreetse füüsilise isiku tuvastamine. Kui isik pole otseselt ega kaudselt tuvastatav ega grupist eristatav, siis andmekaitsereeglid ei kohaldu ning organisatsioonid võivad biomeetrilisi ja emotsioonide püüdmise tehnoloogiad kasutada „andmekaitsereeglitest kammistamata".[162]

Puudub kohtupraktika mitteidentifitseeriva emotsioonipüüdmise kohta. Samuti pole emotsioonituvastusele kohaldatud teisi asjakohaseid õigusakte nagu tervise ja tööohutuse seadus töökohtades või tarbijakaitse seadus, mis eksitavaid ja kuritarvitavavaid praktikaid addresseerib.[163]

Mõistlike järelduste nõue[164] on relevantne ka emotsioonituvastuse kontekstis. Emotsioonituvastus arendeb pidevalt ning kasutatavaid andmekogusid ja algoritme parandatakse. Lisaks on emotsioonituvastuse puhul probleem teaduslik tõsiseltvõetavus Emotsioonid pole n-ö käegakatsutavad, vaid on sisemised. Emotsioonituvastustehnoloogia koosneb kolmest osast: (1) inimese emotsioonide mõõdetavate indikaatorite loomine, (2) subjektiivsete hinnangute kogumine emotsioonide kohta ja (3) indikaatorite ja inimeste endi andud hinnangute vahelise suhte modelleerimine, et teha isiku emotsionaalse seisundi kohta ennustusi, mis on meetodi tõttu tõenäosuslikud.[165] Kuna emotsioonituvastustehnoloogia võib olla ebatäpne, võidakse isiku kohta teha näiteks järeldus, et ta on vihane inimene, kuigi tema näoilme, mille põhjal selline järeldus tehti, on tema pere ja kultuuri kontekstis normaalne mittevihane näoilme. Mõistlike järelduste nõude puhul peaks töötleja põhjendama, miks emotsioonituvastusel põhinev järeldus on mõistlik, ning oleks võimalik sellistele andmete põhjal tehtud järeldustele vastu vaielda.

Üldmääruse peambuli p 15, mis pole õiguslikult siduv, selgitab, et normide täitmisest kõrvalehoidumise märkimisväärse ohu vältimiseks peaks füüsiliste isikute kaitse olema tehnoloogiliselt neutraalne ega tohiks sõltuda kasutatud meetoditest. Üldmääruse preambuli p 63 selgitab, et igal andmesubjektil peaks olema õigus teada eelkõige isikuandmete töötlemise eesmärke, võimaluse korral isikuandmete töötlemise ajavahemikku, isikuandmete vastuvõtjaid, isikuandmete automaatse töötlemise loogikat ja sellise töötlemise võimalikke tagajärgi (vähemalt juhul kui töötlemine põhineb profiilianalüüsil) ning saada eelneva kohta

[162] A. McStay, lk 208-209.

[163] *Ibidem.*

[164] *Supra*, ptk 1.4.

[165] K. Sharma jt. A Dataset of Continuous Affect Annotations and Physiological Signals for Emotion Analysis. Tööversioon. – Arxiv, 06.12.2018.

teade. Seega ei tohiks seetõttu, et emotsioonituvastus on uus tehnoloogia ning seda pole andmekaitse üldmääruses *expressis verbis* mainitud, jätta sellele tehnoloogiale andmekaitseregulatsioon kohaldamata.

Üldmääruse kohaselt ei ole eriliigiliste isikuandmete töötlemiseks vajalik küsida andmesubjekti nõusolekut, kui töödeldakse isikuandmeid, mille andmesubjekt on üldmääruse artikli 9(2)(e) kohaselt ilmselgelt avalikustanud (ingl *manifestly made public by the data subject*). Mitmed inimeste biomeetrilised ja biosensoorsed andmed on väljapoolesuunatuse mõttes avalikud. Näiteks tõstatatud küsimus, kas avalikul tänaval kõndiva inimese nägu või tema vihane või õnnelik näoilme, mida ta ei varja, on avalikustatud või samas olukorras pulsisagedus või nahatemperatuur[166]. Sellele küsimusele peab vastama eitavalt, sest üldmääruse artiklit 9(2)(e) tuleb tõlgendada rangelt[167]. Artiklile 9(2)(e) tuginemiseks peab andmesubjekt eesmärgistatult tegema oma andmed avalikuks. Näiteks valvekaameratesse või muudesse sensoritesse jäämine ei tähenda, et andmesubjekt on andmed ilmselgelt avalikustanud. Küll aga võib isik olla andmed ilmselgelt avalikustanud näiteks, kui laeb üles video või pildi avalikku veebilehele kõigile juurdepääsetavalt. Samuti on oluline meeles pidada, et kuigi biomeetrilised andmed võivad olla nö avalikud, st nähtavad teistele, säilib vastavalt EIK praktikale teatud eraelu puutumatus ka avalikus ruumis[168].

2.2. Automatiseeritud otsused

Andmekaitse mängib olulist rolli eraelu puutumatuse õiguse kaitsmisel, kuid see ei käsitle kõiki eraelu puutumatuse riive aspekte, mis tulenevad tehnisintellekti erinevatest rakendustest ja kasutustest. Andmekaitse piirdub tuvastatud või tuvastatava isikuga (sh kaudselt) seotud andmete kaitsega. See ei hõlma muid privaatsusalaseid rikkumisi, mis ei hõlma isikuandmeid.

Kuigi üldmääruses kajastatud profiilide koostamist ja automatiseeritud otsuste tegemist puudutavad sätted on olulised, mõjutavad need ainult mõningaid tehisintellekti kasutusviise automatiseeritud otsuste tegemisel[169] või profileerimisel[170]. Lisaks ei rakendu EL andmekaitseregulatsioon väljaspool EL õiguse kohaldamisala, mistõttu on inimeste õiguste

[166] A. McStay 2018.

[167] Handbook on European Data Protection Law, lk 162.

[168] EIKo 28.01.2003, 44647/98, *Peck v. United Kingdom*.

[169] F. Kaltheuner, E. Bietti. Data is Power: Towards Additional Guidance on Profiling and Automated Decision-Making in the GDPR. – Journal of Information Rights, Policy and Practice, 2018/2, No 2.

[170] M. Hildebrandt, B.J. Koops. The Challenges of Ambient Law and Legal Protection in the Profiling Era. – The Modern Law Review, 2010/73, No 3, lk 428-460.

kaitse osade oluliste privaatsust riivavate süsteemide rakendamisel piiratud, nt varjatud jälgimisel riikliku julgeoleku tagamiseks. Sellisel juhul kohaldub EL liikmesriikide puhul endiselt EIÕK.[171]

Emotsioonituvastuse puhul on tegu automatiseeritud töötlemisega ning eesmärk on füüsilise isikuga seotud isiklike aspektide hindamine, kuna emotsioonid on kahtlemata isiklikud. Juhul kui emotsioonituvastuse eesmärk pole isiku tuvastamine ning isik pole tuvastatud, otseselt ega kaudselt tuvastatav hinnates kõiki objektiivseid tegureid ja mõistlikku tuvastatavuse tõenäosust, ei ole tegu isikuandmete ning seega ka profiilianalüüsiga, mis oleks hõlmatud isikuandmete kaitse üldmäärusega.

Juhul, kui konkreetsel juhul on järeldatud, et emotsioonituvastusele kohaldub andmekaitseregulatsioon, tuleb kõne alla ka kaitse automatiseeritud otsuste puhul. Emotsioonituvastus toimub algoritmide abil ning algoritmid teevad isiku emotsioonide kohta järeldusi. Isikuandmete kaitse üldmäärus piirab teatud juhtudel automatiseeritud otsuste tegemise kasutamist ning nõuab, et üksikisikutele antaks teavet automatiseeritud otsuste tegemise, sellega seotud loogika ja töötluse olulisuse ning plaanitavate tagajärgede kohta subjektiks oleva isiku jaoks (üldmääruse artiklid 13, 14 ja 22).

Julgustamaks vähem invasiivsete süsteemide loomist, tuuakse üldmääruses välja mitmed sätted ja ettepanekud, millest nii mõnigi piirab tehisintellekti rakendamist. Andmekaitse elementide vaikimisi süsteemi lisamise kohustuse eesmärk on integreerida andmekaitse põhimõtted andmetöötlustoimingute disaini.[172] Organisatsioonide jaoks loodud vahendid eraelu puutumatuse riskide haldamiseks, so andmekaitse mõjuhinnangute koostamine on kohustuslik paljudele tehisintellekti ja masinõppe baasil toimivatele süsteemidele, mis on üldmääruse reguleerimisalas ja millega kaasnevad olulised eeldatavad riskid, nt eriliigiliste isikuandmete töötlemine.[173]

Üldmääruse artikli 4(4) kohaselt on profiilianalüüs: ”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.” Profiilianalüüsil on

[171] Privacy and Freedom of Expression in the Age of Artificial Intelligence, lk 23.

[172] R. Binns. Data Protection Impact Assessments: a Meta-Regulatory Approach. – International Data Privacy Law 2017/7, No 1, lk 22-35; L. Edwards, M. Veale. Enslaving the Algorithm: From a ‘Right to an Explanation’ to a ‘Right to Better Decisions’? – IEEE Security & Privacy, 2018/16, No 3, lk 46-54.

[173] Privacy and Freedom of Expression in the Age of Artificial Intelligence, lk 23.

seega kolm omadust[174]: (1) tegemist peab olema automatiseeritud töötlemisega, (3) seda tuleb teha isikuandmetega ning (3) profiilianalüüsi eesmärk peab olema füüsilise isikuga seotud isiklike aspektide hindamine. Selle definitsiooni kohaselt on masinõppe ja muid profileerimisviise kasutades uute isiklike andmete (järelduste) loomine võimalik. Kui emotsioonituvastus langeb isiku tuvastatavuse tõttu isikuandmete kaitse üldmääruse kohaldamisalasse, tuleb sellele kohaldada ka automatiseeritud otsuste kohta sätestatut, kuna emotsioonituvastuse puhul on täidetud profiilianalüüsi tingimused.

Üldmääruse preambuli p 71 selgitab, et automatiseeritud otsuste tegemine ja profiilianalüüs konkreetsete isikuandmete liikide põhjal peaks olema lubatud ainult eritingimustel. Üldmääruse artikkel 22(1) kehtestab täielikult automatiseeritud otsustele üldise keelu, kuid vaid sellistel otsuste puhul, millel on õiguslikud või muud olulised tagajärjed. Seega artikkel 22 kohaldamisalasse kuuluvad ainult sellised automatiseeritud otsused, millel on tugev mõju. On vaieldav, kas emotsioonipüüdmisel personaliseeritud teenused või reklaamid või muu mõjutamine on „muud olulised tagajärjed". Artikkel 29 töögrupp on selgitanud, et töötlemisel on muud olulised tagajärjed, kui otsusel on potentsiaal näiteks „mõjutada märkimisväärselt asjaomaste üksikisikute olukorda, käitumist või valikuid; avaldada andmesubjektile pikaajalist või püsivat mõju või tuua kõige äärmuslikumal juhul kaasa üksikisikute tõrjutuse või diskrimineerimise"[175]. Internetireklaami kontekstis ei avalda otsus edastada profiilianalüüsil põhinevat suunatud reklaam tüüpilistel juhtudel üksikisikutele samamoodi märkimisväärset mõju, näiteks tavalise veebipõhise ärireklaami puhul, milles lähtutakse lihtsast demograafilisest profiilist[176]. Märkimisväärne mõju on aga võimalik olenevalt juhtumi eripäradest, sealhulgas olenevalt profiilianalüüsi protsessi sekkuvast laadist, asjaomaste üksikisikute ootustest ja soovidest; reklaami esitamise viisist või sihtrühma kuuluvate andmesubjektide haavatavust puudutava teabe kasutamisest. Töötlemine, millel võib olla üldiselt väike mõju, võib märkimisväärselt mõjutada haavatavaid ühiskonnarühmi, nagu näiteks vähemused.[177] Seega tuleb emotsioonituvastuse puhul vaadata konkreetset olukorda, et hinnata, kas emotsioonituvastus avaldab märkimisväärset mõju. Kui emotsioonide põhjal tehakse isikute suhtes hinnaerinevusi või on tegu haavatavate gruppidega, siis artikkel 22(1) keeld suure tõenäosusega kohaldub.

[174] Suunised automatiseeritud töötlusel põhinevate üksikotsuste tegemise ja profiilianalüüsi kohta määruse 2016/679 kohaldamisel. – Artikli 29 alusel asutatud andmetekaitse töörühm, 06.02.2018.

[175] *Ibid*, lk 22.

[176] *Ibid*, lk 23.

[177] *Ibidem*.

Automatiseeritud otsuste tegemisega, sh profiilianalüüsiga seotud ohte ja mõju tuleb hinnata andmekaitsealases mõjuhinnangus. See on ka viis näitamiseks, et ohtudega tegelemiseks on võetud kasutusele asjakohased meetmed ning et järgitakse isikuandmete kaitse üldmäärust.[178] Artikkel 35(3)(a) kohaselt tuleb mõjuhinnang läbi viia, kui toimub füüsiliste isiklike aspektide süstemaatiline ja ulatuslik hindamine, mis põhineb automaatsel isikuandmete töötlemisel, sealhulgas profiilianalüüsil, ja millel põhinevad otsused, millel on füüsilise isiku jaoks õiguslikud tagajärjed või mis samaväärselt mõjutavad oluliselt füüsilist isikut. Säte kehtib ka sellise töötlemise puhul, kus töödeldakse andmeid osaliselt automaatselt, mitte täielikult automatiseeritult.[179] Emotsioonituvastuse puhul tasub viia läbi eelnev mõjuhinnang, kuna on oht inimeste privaatsuse riivele ning mõjuhinnangu käigus võib saada selgeks, kas on isikuid, keda töötlemine võib märkimisväärselt mõjutada, mis tähendaks, et töötlemine oleks keelatud, välja arvatud siis, kui on täidetud mõni erand.

Erandid keelule sätestab artikkel 22(2), mille järgi võib automatiseeritud otsuseid teha, kui see on vajalik andmesubjekti ja vastutava töötleja vahelise lepingu sõlmimiseks või täitmiseks, on lubatud vastutava töötleja suhtes kohaldatava liidu või liikmesriigi õigusega, milles on sätestatud ka asjakohased meetmed andmesubjekti õiguste ja vabaduste ning õigustatud huvide kaitsmiseks, või põhineb andmesubjekti selgesõnalisel nõusolekul. Automatiseeritud emotsioonituvastuse alus sõltub seega konkreetsest olukorrast. Näiteks avalikul tänaval või internetis inimeste emotsioonide põhjal neile sihitud reklaame näidates eesmärgiga neid mõjutada ja muutes vastavalt emotsioonidele toote või teenuse hinda, peaks töötlemise aluseks olema sõnaselge nõusolek.

Kui on tehtud läbi tuvastatavuse hinnang ning on selgunud, et konkreetsele emotsioonituvastusele rakendub andmekaitseregulatsioon, tuleb hinnata ka seda, kas emotsioonituvastus omab märkimisväärset mõju. Kui emotsioonituvastus märkimisväärset mõju ei oma, tuleb siiski järgida andmetöötluse põhimõtteid ja tagada andmesubjektidele üldmääruses sätestatud õigused. Kui emotsioonituvastusel on märkimisväärne mõju, on selline emotsioonituvastus üldjuhul keelatud, välja arvatud siis, kui on täidetud artiklis 22(2) sätestatud erand, näiteks selgesõnaline nõusolek. Märkimisväärse mõju olemasolul tuleks emotsioonituvastuse kasutamisel artikkel 14(2)(g) kohaselt esitada andmesubjektile ka

[178] *Ibid*, lk 30.

[179] Suunised, mis käsitlevad andmekaitsealast mõjuhinnangut ja selle kindlaksmääramist, kas isikuandmete töötlemise tulemusena „tekib tõenäoliselt suur oht“ vastavalt määrusele (EL) 2016/679. – Artikli 29 alusel asutatud andmekaitse töörühm, 04.04.2017.

vähemalt teave kasutatava loogika ja selle kohta, millised on sellise töötlemise tähtsus ja prognoositavad tagajärjed andmesubjekti jaoks.

2.3. Emotsionaalne informatsioon kui andmeliik

Isegi kui emotsioonituvastusele ei rakendu isikuandmete kaitse regulatsioon, võib selline emotsioonituvastus omada negatiivseid mõjusid. Mitteidentifitseeriva emotsioonituvastuse levik võib kaasa tuua mitmeid riske, näiteks inimestesse võidakse hakata suhtuda kui emotsionaalsetesse loomadesse, kelle bioloogiat tundma õppida, et nendega manipuleerida, inimesi võidakse näha kui objekte, mitte subjekte, inimesed võivad kaotada enda kohta kogutava tundliku info üle kontrolli, passiivse jälgimistegevusega võidakse koguda inimeste intiimseid andmeid ilma nõusolekuta, inimesed võivad lõpetada avalikes kohtades käimise, rohekm võib olla soovimatut tähelepanu käitumisele ja inimkehale, võivad lisanduda viisid tarbijate käitumise mõjutamiseks, rakendades käitumuslikke teaduseid, ning samuti võib mitteidentifitseeriv emotsioonituvastus riivata väärikust.[180] Mitmed eksperdid on olnud emotsioonituvastuse osas kriitilised öeldes, et algoritmid ei ole täpsed ning teevad kõrge riskiga otsuseid tuginedes pseodoteadusele.[181] Hüpoteetiliselt võivad olla algoritmid diskrimineerivad, sest ühe inimese naeratus võib olla viisakus, mitte õnnelikkus ning mossis nägu on tegelikult tema tavaline nägu ega tähenda negatiivsust.

Masinate võime inimeste emotsioone lugeda seostub ka "müksamise teooria" (ing.k *nudge theory*), freiminguteooria (ing.k *framing theory*) ja käitumusliku majandusteooria võimaliku väärkasutamisega, mis oli probleemiks ka grupiprivaatsuse aspektist[182]. Müksamine on käitumusliku majandusteooria tehnika, kus muudetakse inimese valiku arhitektuuri (internetis näiteks kasutajaliidest), selleks, et inimesed kalduksid teatud otsuste poole[183]. Füsioloogia ja emotsioonide mõistmine loob inimeste otsuste mõjutamiseks uusi võimalusi.[184]

Emotsioonide kaubaks muutumise ulatusse tuleb suhtuda ettevaatlikult, kuid eesmärk ei peaks olema emotsioonituvastustehnoloogiate keelustamine, vaid viisi leidmine, kuidas tehnoloogiat kasutada selliselt, et see austaks inimelu väärikust, suurendaks tehnoloogiast saadavat kasu ning

[180] A. McStay 2018, lk 6.

[181] O. Schwartz.

[182] *Supra*, ptk 1.1-1.3.

[183] K. Renaud, V. Zimmermann. Guidelines For Ethical Nudging in Password Authentication. – SAIEE African Research Journal 2018/109, No 2, lk 105.

[184] A. McStay 2018, lk 6.

teeniks, mitte ei kuritarvitaks inimesi.[185] Need majanduslikud, eetilised ja filosoofilised probleemid on olulised mõistmaks emotsioonituvastuse laiemat mõju, ent neil probleemidel siinkohal pikemalt ei peatuta.

Tugevamate salasõnade valimise poole müksamise kontektstis on pakutud 7 printsiipi, mis peavad olema täidetud, et müksamine oleks eetiline: (1) tagasihoidlik ehk inimesel peab olema vabadus teha ka valik, mis ei ole müksamise eesmärk, (2) inimese autonoomiat austav ehk inimesele peaks ütlema, et neid müksati, miks seda tehti, mis on müksamise eesmärk ja milline on sellise müksamise mõju inimestele; (3) läbipaistev ehk inimene peab olema teadlik müksamisest ja selle eesmärgist; (4) kaitstav ehk inimesel peab olema võimalus müksamise rakendajaga ühendust võtta ning küsimusi küsida; (5) õigustatud ehk peab olema selgitatud, miks on müksamine vajalik; (6) sobiv ehk müksata tuleks ainult sel määral, mis on vajalik ja kui on vajalik; (7) järelevalve all ehk müksamine ja selle võimalikud mõjud peaksid olema kontrollitud[186]. Need soovituslikud printsiibid kattuvad teatud määral harta ja üldmääruse põhimõtetega nagu üldmääruse artiklist 5 tulenevad põhimõtted: seaduslikkus, õiglus ja läbipaistvus; eesmärgipiirang; võimalikult väheste andmete kogumine; õigsus, säilitamise piirang; usaldusväärsus ja konfidentsiaalsus ning vastutus. Siiski on need 7 pakutud printsiipi vaid soovituslikud ning andmekaitse printsiibid kohaldub vaid siis, kui emotsioonituvastusega töödeldakse isikuandmeid mitte anonüümseid andmeid.

Pakutud on, et emotsionaalne informatsioon võiks andmekaitse regulatsioonis olla sätestatud kui eraldi informatsiooniliik, kuna on moraalselt vale, et inimeste emotsioone püütakse nende teadmata, emotsioonide alane informatsioon võib omada laiemat mõju ning pole selge, milline on andmesubjektide endi kasu emotsioonituvastuse kasutamisel avalikus ruumis.[187] Emotsioonituvastustehnoloogiate kasutuse kohta on viidud läbi ka küsitlusi. Aastatel 2015-2018 küsitleti Suurbritannias ca 2000 inimest, kellest pooled vastasid, et neile ei sobi emotsioonituvastus ühelgi juhul[188], mis viitab sellele, et inimesed peavad emotsioone enda eraelu osaks, millele laieneb eraelu puutumatuse kaitse põhimõte. Emotsioonituvastusega kaasnev problemaatika seostub S. Wachtersi kriitikaga, et andmekaitse regulatsioon on liialt keskendunud andmete kogumise hetkele ning liiga vähe on tähelepanu pööratud, sellele, mida

[185] A. McStay 2018, lk 6.

[186] K. Renaud, V. Zimmermann, lk 112-113.

[187] A. McStay, 2018.

[188] *Ibid*, lk 7.

nende andmetega tehakse[189]. Seos on ka grupiprivaatsuse temaatikaga[190], kuna kui emotsioonituvastus ei ole konkreetse isikuga seotud, on see tõenäoliselt seotud teatud grupiga ehk proovitakse mõjutada gruppe.

Emotsioonituvastuse täiendavaks reguleerimiseks on eri variante, võimalik on nii emotsionaalse informatsiooni kui eraldi andmeliigi andmekaitse regulatsiooni lisamine või näiteks tugevam grupiprivaatse kaitse. Kehtiva õiguse raamistikus on oluline, et isikuandmete kaitse üldmääruse materiaalset kohaldamisala meelevaldselt ei kitsendataks. Üldmääruse kohaldamisalast peaks olema väljaspool vaid selline emotsioonituvastus, mille põhjal isikut on võimatu tuvastada või pole tuvastamine mõistlikult tõenäoline võttes arvesse objektiivseid tegureid nagu tuvastamise hind, aeg, tehnoloogiline tase ning emotsioonituvastuse eesmärki. Kui eesmärk hõlmab isikute tuvastamist ja nende mõjutamist, siis peaks sellisele emotsioonituvastusele rakendama isikuandmete kaitse regulatsiooni ehk vastavalt üldmäärust või õiguskaitseasutuste direktiivi.

EIK praktika kohaselt hõlmab EIÕK artikkel 8 ka riikide positiivset kohustust kindlustada inimeste õigus oma füüsilise ja psühholoogilise väärikuse efektiivsele kaitsele[191]. See kohustus hõlmab ka meedete võtmist, et efektiivselt ja kättesaadavalt seda kaitset tagada[192]. Kuigi teatud emotsioonide püüdmine võib olla väljaspool isikuandmete kaitse regulatsiooni kohaldamisala, võib olla tegu inimese füüsilise ja psühholoogilise väärikuse riivamisega ehk privaatsusõiguse riivega EIK artikkel 8 ja harta artikkel 7 tähenduses. Mentaalse puutumatuse küsimuses on EIK näiteks leidnud, et ka vaimne tervis on privaatsusõiguse oluline osa ning seotud moraalse väärikusega[193]. Seega võib analoogia põhjal öelda, et isegi kui teatud emotsioonituvastus ei ole EL isikuandmete kaitse regulatsiooniga hõlmatud, võib emotsioonituvastus riivata inimese füüsilist ja psühholoogilist autonoomsust EIÕK artikli 8 ja harta artikli 7 tähenduses.

[189] *Supra*, ptk 1.4.

[190] *Supra*, ptk 1.3.

[191] EIKo 21.03.2002, 65653/01, *Nitecki v. Poland*; EIKo 08.07.2003, 27677/02, *Sentges v. the Netherlands*; EIKo 13.02.2003, *Odièvre v. France*, para 42; EIKo 09.03.2004, 61827/00, *Glass v. the United Kingdom*, para 74-83; EIKo 04.01.2005, 14462/03, *Pentiacova and Others v. Moldova*.

[192] EIKo 09.10.1979, 6289/73, *Airey v. Ireland*, para 33; EIKo 09.06.1998, 21825/93 ja 23414/94, *McGinley and Egan v. the United Kingdom*, para 101; EIKo 19.10.2005, 32555/96, *Roche v. the United Kingdom*, para 162.

[193] EIKo 06.02.2001, 44599/98, *Bensaid v. the United Kingdom,* para 47.

3. ANDMEKAITSENÕUDED MASINNÄGEMISE KASUTAMISEL EESTI KORRAKAITSES JA SÜÜTEOMENETLUSES

Eesti riigi eelarvestrateegias 2019-2022 on võetud siseturvalisuse valdkonnas eesmärgiks nutikate, optimaalsete ja mõjusate lahendustega elukeskkonna parandamine, ohu vähendamine elule, tervisele, varale ja põhiseaduslikule korrale ning kiire ja asjatundliku abi tagamine. Siseturvalisuse valdkonnas on eesmärkide seas plaan luua ja võtta kasutusele automaatne biomeetriline identifitseerimissüsteem (ABIS)[194,195] ning pakkuda õigusliku aluse olemasolul biomeetriliste andmete alusel isiku tuvastamist teenusena nii erasektori kui ka riigisektori esindajatele. Kriminaalpoliitika valdkonnas soovitakse aastaks 2030 olla teadmiste- ja analüüsipõhised, kasutades selleks andmeid ja tehnoloogiat[196]. Personali vähenemine[197] seab piirid politsei reageerimiskiirusele, süütegude menetluste läbiviimise kiirusele ja kvaliteedile. Uute tehnoloogiate kasutamine võimaldab ressursilünki kompenseerida, õiguskaitseasutuste ametnike tööd lihtsustada ning aidata kaasa süütegude ennetamisele ja avastamisele.[198]

3.1. Kaamerate ja masinnägemise rakendus korrakaitses ja süüteomenetluses

Üheks nutikaks, optimaalseks ja mõjusaks lahenduseks saab pidada masinnägemist. Masinnägemise rakendusviisid on näiteks automaatne näotuvastus ja autonumbri tuvastus[199]. Reaalajas reageerimiseks ilma masinnägemiseta kaamerate puhul on vajalik, et inimene

[194] ABIS võimaldaks biomeetrilisi andmeid töödelda ja kasutada senisest efektiivsemalt ja koordineeritumalt, kuna koondaks seni eri ministeeriumite haldusalas olevad siseriiklikud biomeetrilised andmebaasid üheks andmebaasiks. ABIS-e isikuandmete kaitse õiguslikust poolest vt M. Miidla jt. Euroopa Liidu ja rahvusvaheliste õigusaktide analüüs identiteedihalduse valdkonnas. – Sorainen, 03.12.2018.

[195] ABIS võimaldab sõrmejälgede ja näokujutiste automaatse võrdlemise teel isikuid tõsikindlalt tuvastada. „Arvestades biomeetria üha laialdasemat kasutamist, on ka selle mõju identiteedivaldkonna arengule järgneva kümne aasta jooksul määrav. Rakendatakse erinevaid tehnoloogiaid ning katsetatakse alternatiivseid biomeetrilisi tunnuseid.“ Valge Raamat: Identiteedihaldus ja isikut tõendavad dokumendid 1.0.

[196] Inimkeskne ja nutikas kriminaaljustiitssüsteem ja kuriteoennetus: Kriminaalpoliitika põhialused aastani 2030. Eelnõu seisuga 29.11 2018. – Justiitsministeerium.

[197] Politseinike arv on aastatega kahanenud ligi tuhande võrra – Lõuna-Eesti Postimees, 21.08.2018

[198] Siseministri käskkirja ”Siseturvalisuse arengukava 2015-2020” 2018-2021 programmide kinnitamine. Lisa 1 – Turvalisemad kogukonnad.

[199] H. Idrees jt. Enhancing Camera Surveillance Using Computer Vision: a Research Note. – Policing: An International Journal of Police Strategies & Management 2018/41, No 2, lk 292-307; Tehnilisest aspektist vt ka C. Guaragnella, T. D’Orazio. A Survey of Automatic Event Detection in Multi-Camera Third Generation Surveillance Systems. – International Journal of Pattern Recofnition and Artificial Intelligence, 2014/29, No 1.

videoedastust monitooriks ning videost ohukahtluse või õigusvastase teo tuvastamisel reageeriks. Masinnägemise puhul teevad tuvastamise osas töö ära masinõppe algoritmid, mistõttu on võimalik tõsta tuvastamise efektiivsust ja selle abil inimeste reageerimise kiirust. Lisaks inimressursi kokkuhoidmisele on masinnägemisel ka teisi eeliseid. Näiteks ei „vaata" algoritmid seda, mida neid pole programmeeritud vaatama[200], ei väsi ega ole hajameelsed, kuigi masinnägemisel on muid tehnilisi probleeme nagu näiteks vastete ebatäpsus[201]. Seega on võimalik masinnägemise abil efektiivsemalt avaliku korda kaitsta ja süüteomeneltust läbi viia. Riigid mitmel pool maailmas rakendavad jälgimisseadmestikke ja intelligentset videoanalüütikat, et avalikes kohtades inimesi jälgida[202]. Prognoositakse, et globaalne linnades kasutatavate jälgimistehnoloogiate turg kasvab võrreldes 2016. aastaga 2021. aastaks 14,6%[203]. Inglismaal ja Walesis on juba näotuvastustehnoloogiat rakendatud erinevate rahvakogunemiste jälgimiseks[204]. Sealjuures väidavad politseijõud, et nad on teadlikud võimalikest inimõiguste riivest ning olulisusest kasutada tehnoloogiat järgides seaduslikkuse ja proportsionaalsuse põhimõtet[205].

Masinnägemise abil on potentsiaalselt võimalik tuvastada objekte (nt relv), isikusamasust[206], teatud anomaalsusi[207], tegevusi või olukordi (nt vandalism, kaklus, tulekahju) ning erinevaid inimese tunnuseid, näiteks sugu[208] ja kahtlust äratavaid emotsioone[209]. Masinnägemine aitab lisaks reaalajas tuvastusele ka varasemalt salvestatud videolt leida vajalikku objekti, inimest või olukorda[210]. Masinnägemise rakendamine võib olla seega sisult erinev olenevalt sellest,

---

[200] Videoedastust monitoorivad inimesed näevad aga ka näiteks intiimseid tegevusi. Häirekeskuse päästekorraldaja teadis öelda, et Vana-Posti tänaval on ööklubi Hollywood, mille ees purskkaev, ning kaamerasilm on korduvalt fikseerinud, et inimesed kipuvad selles purskkaevus värskendust otsima ja mõned võtavad end paljaks. T. Herm. Teralised abilised mundris ja mundrita inimestele. – Virumaa Teataja, 06.04.2019.

[201] H. Idrees jt.

[202] IHS Markit andmetel kulutasid linnad 2017. aastal üle maailma jälgimistehnoloogiatele üle 3 miljardi dollari. J. E. Solsman. Cities Worldwide Spend Over $3 Billion Last Year to Peep on You. – CNET, 28.03.2018.

[203] *Ibidem.*

[204] M. Hughes. Three Arrested Using Facial Recognition Technology during Wales' Six Nations Opener. – WalesOnline, 06.02.2018.

[205] Introduction of Facial Recognition into South Wales Police. – South Wales Police, 2018.

[206] Näotuvastusel põhinevad isikutuvastust saab kasutada näiteks piirivalves. N. Soni. Piiriturvalisuse tagamine elektriaia ja näotuvastuse alusel. Magistritöö. Tallinn: TTÜ, 2017.

[207] Anomaalsuste osas masinnägemise ülevaade vt S. K. Kumaran jt. Anomaly Detection in Road Traffic Using Visual Surveillance: A Survey. Odisha: Indian Institute of Technology Bhubaneswar, 2019.

[208] S. E. Ezeoke. Näo emotsiooni ja soo tuvastus kasutades konvulutsioonilisi närvivõrke. Magistritöö. Tallinn: TTÜ, 2018.

[209] M. Sajjad jt. Raspberry Pi Assisted Facial Expression Recognition Framework for Smart Security in Law-Enforcement Services. – Information Sciences, 2019/479, lk 416-431.

[210] H. Idrees jt.

mida on algoritmid programmeeritud tuvastama - see omab tähtsust privaatsusõiguse ja isikuandmete kaitse õiguse riive ulatust ning meetme proportsionaalsust hinnates.

Üldiselt koosneb biomeetriline tuvastustehnoloogia kolmest astmest: biomeetriliste andmete hõive, võrdlus andmebaasis olevate andmetega ning otsus[211]. Masinnägemisel põhinev näotuvastus jaguneb tehniliselt neljaks astmeks: näotuvastus (ingl *face detection*), normaliseerimine (ingl *normalization*), tunnushõive (ingl *feature extraction*) ja isikutuvastus (ingl *recognition*)[212]. Isikutuvastuses[213] on masinad täpsemad kui inimesed ning masina õppimisvõime on kiirem[214].

Masinnägemist saab rakendada nii statsionaarsete kaamerate kui ka mobiilsete puhul nagu autokaamerad, droonikaamerad[215] ja kehakaamerad[216] ning neid on võimalik kasutada ühtse süsteemina. Näiteks kui statsionaarse kaamera isikutuvastustarkvara tuvastab isikusamasuse tagaotsitava inimesega, on võimalik politseinikul asukohta kohale minnes kehakaamera näotuvastuse abil teistkordselt isikusamasus tuvastada, et vähendada eksimise tõenäosust[217].

Eestis hindavad inimesed kodukoha turvalisust kõige suuremal määral tõstva tegurina valvekaameraid avalikes kohtades (53 protsenti)[218] ning kaamerad aitavad ka õiguskaitseasutusi oma ülesannete täitmisel[219], mistõttu on õiguskaitseasutustel motivatsioon neid juurde paigaldada. Põhja häirekeskuses jälgitakse ööpäevläbi ekraanidelt 2019. aasta aprilli seisuga üle saja Harjumaal asuva valvekaamera videot, kust tuvastatakse reaalajas nii taskuvargaid, külma ilmaga magama jäänud kodutuid, peksmisi kui ka võimalikke alkoholijoobes autojuhte

---

[211] Opinion 2/2012 on Facial Recognition in Online and Mobile Devices. – Article 29 Data Protection Working Party, 22.03.2012.

[212] B. Akinnuwesi, T. T. Agagu. Automated Students' Attendance Taking in Tertiary Institution Using Facial Recognition Algorithm. – Journal of Computer Science and Its Application 2012/19, No 2. Näotuvastuse tehnilise poole osas vt R. Coseraru, lk 17.

[213] Masinnägemise abil isikusamasuse tuvastamiseks võetakse riiklikust andmebaasist inimese näofoto, mis on näiteks ID-kaarti või passi taotledes tehtud, ja võrreldakse kaamerapildiga. Kui tarkvara ütleb, et pildid klapivad, on isikusamasus tuvastatud. H. Lõugas. Päris inimeste küsimused: mis asi see Elisa näotuvastus on ja kas ma peaks seda kartma? – Digigeenius, 10.09.2018.

[214] K. Kütt. Turvalise identiteedi tulevik. – Director, 01.04.2019.

[215] Mehitamata õhusõidukil masinnägemise kasutamise kohta vt P. Tänav. Reaalaja sardsüsteemil põhinev objekti detekteerimis- ja jälgimissüsteem. Magistritöö. Tallinn: TTÜ, 2018.

[216] Kehakaamerate abil näotuvastust on rakendatud näiteks UK-s, vt nt Z. Doffman. Facial Recognition Is Coming To Police Body-Worn Cameras In 2019. – Forbes, 10.01.2019.

[217] *Ibidem*.

[218] M. Kuul. Valdav osa Eesti elanikke peab Eestit turvaliseks riigiks – ERR uudisteportaal, 24.09.2018.

[219] Maanteeamet alustab Tallinnas keelava fooritule eiramise automaatkontrolli testperioodiga. – Maanteeamet, 18.02.2019; K. Virk. PPA hankis piiriturvalisuse tagamiseks militaardroonid. – Politsei- ja Piirivalveamet, 12.01.2018.

ning edastatakse info Päästeametile, Politsei- ja Piirivalveametile või kiirabile.[220] 2019. aasta suve keskpaigaks lisandub Rapla linna avalikku ruumi kümmekond valvekaamerat,[221] Kuressaare kesklinna lisandub kuude erinevasse kohta 16 valvekaamerat.[222] Läänemaal tänaval toimuvate kuritegude kergemaks avastamiseks soovib politsei „katta linna valvekaameratega", lisada numbrituvastusega liikluskaameraid ning kasutada kaameraid ka rulapargis alaealiste suitsetajate tabamiseks[223].

Tartusse on politsei ja omavalitsuse koostööna paigutatud linna avalikesse kohtadesse üle 30 valvekaamera. Lõuna prefektuuri operatiivjuhi sõnul uuenevad kaamerad kiiresti, polisei otsib pidevalt uusi positsioone ja kasutakse võimsat optiliste zuumidega kaameraid, kust isegi väiksemad detailid on hästi tuvastatavad.[224] Valvekaameraid paigaldatakse eelistatult mittenähtavasse kohta[225].

Masinnägemise tehnoloogia arendamisel ja levikul on soodne kasvulava arvestades, et riigi strateegilistes dokumentides kavandatakse siseturvalisuse ja õiguskorra valdkondades uute tehnoloogiate kasutuselevõttu, küsitluse kohaselt peavad Eesti inimesed kaameraid kodukoha turvalisuse tagamisel kõige olulisemaks, õiguskaitseasutused paigaldavad ülesannete täitmiseks kaameraid juurde ning masinnägemise abil kaamerate „nutikamaks tegemine" võimaldab tõhusamalt tagada avalikku korda ja läbi viia süüteomenetlust. Kaamerate paigaldamine ja kõrgema tehnoloogiaga tarkvara kasutamisel tuleb aga arvestada isikuandmete kaitse nõuetega, mis tulenevad Eestile nii siseriiklikust, EL-i õigusest kui ka rahvusvahelisest õigusest.

3.2. EL õiguse kohaldamisala korrakaitses ja süüteomenetluses

Isikuandmete töötlemist korrakaitses ja süüteomenetluses puudutavad lisaks siseriiklikule õigusele ka EL- i ja Euroopa Nõukogu õigusaktid, millest on ülevaate koos selgitustega teinud Fundamental Rights Agency (FRA)[226]. Euroopa Nõukogu moderniseeritud konventsioon 108 on harmoniseeritud EL-i isikuandmete kaitse üldmääruse ja õiguskaitseasutuste direktiiviga. Isikuandmete kaitse üldmäärust võib vaadelda kui *lex generalis* ning õiguskaitseasutuste

[220] T. Herm.

[221] V. Veski. Poolik lahendus tõi Karmani parklasse pooliku öörahu. – Raplamaa Sõnumid, 27.03.2019.

[222] K. Koovisk. Mida on tehtud, et Kuressaare kesklinnas turvalisem oleks? – Saaremaa Teataja, 07.02.2019.

[223] M-L. Raigla. Läänemaal on kuritegevus Eesti keskmine. – Lääne Elu, 01.04.2019; M-L. Raigla. Sel aastal tulevad Haapsalu sissesõitudele kaamerad. – Lääne Elu, 01.04.2019.

[224] J. Saluorg. Turvakaameraid võib isikuandmete töötlemiseks kasutada. – ERR uudisteportaal, 19.10.2018.

[225] K. Saarpuu. Vargad varastasid endale tegevusvabadust. – Järva Teataja, 18.10.2018.

[226] Handbook on European Data Protection Law, lk 271-272.

direktiivi kui *lex specialis*[227] nende omavahelises suhtes[228]. Erinevalt üldmäärusest ei ole direktiiv otsekohalduv, vaid tuleb võtta üle siseriiklikku õigusesse, mida Eesti tegi hilinemisega 2019. aasta alguses. Isikuandmete kaitse üldmäärusel ja õiguskaitseasutuste direktiivil[229] on erinevad kohaldamisalad ning olenevalt isikuandmete töötlejast ja tegevusest, mille raames isikuandmeid tööteldakse, võib kohalduda kas üks või teine või mitte kumbki.

3.2.1. Isikuandmete kaitse üldmääruse ja õiguskaitseasutuste direktiivi kohaldamisalad

Õiguskaitseasutuste direktiiv kohaldub vaid siis, kui on täidetud selle materiaalne ja isikuline kohaldamisala. Direktiivi kohaldamiseks peab töötlemine toimuma pädevate asutuste poolt (isikuline kohaldamisala) süütegude tõkestamiseks, uurimiseks, avastamiseks, nende eest vastutusele võtmiseks või kriminaalkaristuste täitmisele pööramiseks, sealhulgas avalikku julgeolekut ähvardavate ohtude eest kaitsmiseks ja nende ennetamiseks (materiaalne kohaldamisala, mis tuleneb artiklitest 1(1) ja 2(1)). Kui õiguskaitseasutus töötleb isikuandmeid muul eesmärgil, näiteks tulenevalt töösuhtest, kohaldub sellisele töötlusele üldmäärus, välja arvatud juhul, kui töötlemine on väljaspool EL õigust.

Direktiivi materiaalsele kohaldamisalale lisati „sealhulgas avalikku julgeolekut ähvardavate ohtude eest kaitsmiseks ja nende ennetamiseks“ („*or the safeguarding against and the prevention of threats to public security*“) 2015. aastal kolmepoolsete läbirääkimiste käigus.[230] Esialgses komisjoni ettepanekus oli direktiivi kohaldamisala kitsam. Samuti täiendati selgitusi direktiivi preambulis, lisades muuhulgas „*[t]he activities carried out by the police or other law enforcement authorities are mainly focused on the prevention, investigation, detection or prosecution of criminal offences including police activities without prior knowledge if an incident is a criminal offence or not. These can also include the exercise of authority by taking coercive measures such as police activities at demonstrations, major sporting events and riots. Those activities performed by the above-mentioned authorities also include maintaining law*

[227] B. Custers jt. EU Personal Data Protection in Policy and Practice. – Information Technology and Law Series, 2019/29, lk 217.

[228] Sarnaselt on ka e-privaatsuse direktiiv üldmääruse suhtes *lex specialis*. Vt: üldmääruse artikkel 95.

[229] Ajaloo kohta vt L. J. Pajunoja. The Data Protection Directive on Police Matters 2016/680 Protects Privacy - The Evolution of EU´s Data Protection Law and its Compatibility with the Right to Privacy. Magistritöö. Helsingi: Helsingi Ülikool, 2017.

[230] Proposal for a Directive of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data by Competent Authorities. Ülemkogu ettepanek. – Euroopa Ülemkogu, 02.10.2015. Kättesaadav: http://data.consilium.europa.eu/doc/document/ST-12555-2015-INIT/en/pdf (05.04.2019); vt ka M. Lauristin. Protecting Personal Data Processed for the Purposes of Police and Judicial Cooperation in Criminal Matters. – Legistlative Train Schedule, 20.03.2019.

and order as a task conferred on the police or other law enforcement authorities where necessary to safeguard against and prevent threats to public security, aimed at preventing human behaviour which may lead to threats to fundamental interests of the society protected by the law and which may lead to a criminal offence,"[231] mis vastu võetud direktiivi teksti jõudis väikeste sõnaliste muudatustega, mis sisu ei muutnud (preambuli p 12). Seega laiendati direktiivi kohaldamisala ning selgitati preambuli punktis 12, et „politsei või muude õiguskaitseasutuste tegevus, sealhulgas politsei toimingud juhul, kui eelnevalt pole teada, kas tegemist on süüteoga, keskenduvad peamiselt süütegude tõkestamisele, uurimisele, avastamisele või nende eest vastutusele võtmisele. Selline tegevus võib hõlmata ka avaliku võimu teostamist sunnimeetmete võtmisega, näiteks politsei tegevus demonstratsioonidel, suurtel spordiüritustel ja massirahutustel. Selline tegevus hõlmab ka avaliku korra säilitamist, mis on politseile või muule õiguskaitseasutusele antud ülesanne, et vajaduse korral kaitsta avalikku julgeolekut ja seadusega kaitstavaid ühiskonna põhihuve selliste ohtude eest ja hoida ära selliste ohtude teke avalikule julgeolekule ja seadusega kaitstavatele ühiskonna põhihuvidele, mis võivad viia süüteo toimepanemiseni. Liikmesriigid võivad anda pädevatele asutustele muid ülesandeid /---/ ning nii kuulub neil muudel eesmärkidel toimuv isikuandmete töötlemine niivõrd, kuivõrd see on liidu õiguse kohaldamisalas, määruse (EL) 2016/679 kohaldamisalasse." Preambulis kirjeldatakse sunnimeetmete võtmist väljaspool süüteomenetlust, mis on omane korrakaitsele kui ohutõrjele ja sätestatud korrakaitseseaduses[232]. Samuti kirjeldatakse materiaalsesse kohaldamisalasse kuuluvana ohtude teket, mis võivad viia süüteo toimepanemiseni, mis on sarnane korrakaitseseaduse (edaspidi ka KorS) § 5 lg-tes 1 ja 2 sätestatuga (KorS 5. peatükk)[233]. Selgituses pole piiritletud materiaalset kohaldamisala süüteokahtluse olemasoluga, vaid hõlmatud on ka avaliku korra säilitamine ja ohtude tekke ärahoidmine. Seega on direktiivi materiaalses kohaldamisalas ka ohutõrje iseloomuga olukorrad, kus süüteomenetlus pole alanud[234] ja hoitakse ära ohtude teket avalikule julgeolekule ja ühiskonna põhihuvidele, mitte ainult süüteomenetlus.

Kolmepoolsetel läbirääkimistel materiaalse kohaldamisala laiendamist kritiseeriti põhjusel, et pole selge, millised tegevused on direktiivi laiendatud materiaalse kohaldamisalaga kaetud.

[231] *Ibidem.*

[232] Korrakaitseseaduse eelnõu - SEN Seletuskiri RT I, 22.03.2011, 4, jõust 01.07.2014, lk 101-102.

[233] Tuleb tähele panna, et korrarikkumine ja süütegu ei ole sünonüümid. Kõik korrarikkumised ei ole süüteod. Korrakaitseseaduse eelnõu, lk 21.

[234] Täpsemalt süüteomenetluse ja korrakaitse piiritlemisest on kirjutanud I. Pärnamägi. Põhiõigustesse sekkumise materiaalõiguslikud tingimused ning nende piiritlemine ohutõrjes ja süüteomenetluses. Tallinn: TTÜ, 2018.

Defineerimata on „criminal offence“[235], mis on Eesti õigusesse võetud üle kui süütegu. Samuti pole defineeritud „riiklik julgeolek (*national security*)“ ja „avalik julgeolek (*public security*)“ ning nende erinevus. Kuigi soovitati preambulit selles osas täiendada, seda ei tehtud.[236] Taoline ebaselgus võib tuua kaasa selle, et liikmesriigid mõistavad kohaldamisala erinevalt ning võtavad direktiivi erinevalt üle[237].

IKS seletuskirjas on direktiivi materiaalse kohaldamisala kohta öeldud: „Direktiiv 2016/680 kasutab kohaldamisala piiritlemisel süütegude tõkestamist (*prevention*), uurimist (*investigation*), avastamist (*detection*), vastutusele võtmist (*prosecution*) ja kriminaalkaristuste täitmisele pööramist (*execution of criminal penalties*).“ IKS seletuskirjas on direktiivi materiaalse kohaldamisala piiritlemisel aga välja jäetud „sealhulgas avalikku julgeolekut ähvardavate ohtude eest kaitsmiseks ja nende ennetamiseks“, mis direktiivile kolmepoolsetel läbirääkimistel saavutatud kokkuleppena lisati ning mille eesmärk oli direktiivi kohaldamisala laiendada. Seletuskirjas selgitatakse „Eesti õiguses on nii süütegude uurimine kui ka nende eest vastutusele võtmine direktiivi mõttes hõlmatud süütegude menetlemise mõistega, mistõttu kasutatakse terminit süütegude menetlemine,“[238] ent käsitlusest on välja jäänud süütegude tõkestamine ehk ennetamine[239], mis on osa korrakaitsest ehk riikliku järelevalve menetlusest (KorS § 5 lg 7)[240]. Seletuskirjas ollakse seisukohal, et riikliku järelevalve teostamine korrakaitseseaduse § 2 lõike tähenduses ei ole pädeva asutuse tegevus, mis seisneks süütegude ennetamises, avastamises, uurimises, süüdistuse esitamises või avaliku julgeoleku tagamises direktiivi kohaldamisala tähenduses[241]. See tõlgendus ei võta arvesse kolmepoolsetel läbirääkimistel laiendatud direktiivi kohaldamisala ega KorS § 5 lg-t 7, mille kohaselt on riikliku järelevalve meetod ka süütegude ennetamine. Direktiivi materiaalse kohaldamisala kitsendava tõlgenduse tõttu leitakse seletuskirjas, et isikuandmete töötlemisele riikliku järelevalve teostamisel tuleb kohaldada andmekaitse üldmäärust ning IKS 4. peatüki kohaldamine tuleb kõne alla siis, kui alustatakse väärteomenetlust[242]. Seetõttu on tõlgendatud

[235] J. Sajfert, T. Quintel. Data Protection Directive (EU) 2016/680 for Police and Criminal Justice Authorities. – Cole/Boehm GDPR Commentary, Edward Elgar Publishing 2019, lk 22. (Käsikiri avaldamisel.)

[236] D. Naranjo. Data Protection Directive on Law Enforecement: The Loopholes. – EDRi, 18.11.2015.

[237] J. Sajfert, T. Quintel, lk 4.

[238] Isikuandmete kaitse seaduse eelnõu seletuskiri - RT I, 04.01.2019, 11 – jõust. 15.01.2019, lk 19.

[239] Tõkestamise sünonüüm on EKI kohaselt ennetamine. Ka lõpetamata süüteo tõkestamise puhul on tegemist riikliku järelevalve menetlusega. Võimalik on ka süüteomenetluse ja riikliku järelevalve menetluse samaaegne kulgemine näiteks kui karistatav on ka süüteokatse. Vt ka I. Pärnamägi, lk 17, 19-20.

[240] Vt ka I. Pärnamägi, lk 17, 19-20.

[241] IKS seletuskiri lk 19

[242] *Ibidem*.

direktiivi kohaldamisala kitsendavalt ning ülevõtmisel otsustatud, et direktiiv kohaldub vaid süüteomenetlusele ning korrakaitsele kohaldub üldmäärus.

Seletuskirjas olev ebaselgus süütegude tõkestamise kategoriseerimisega leidub ka seaduses. IKS § 12 lg 1 järgi on 4. peatüki kohaldamisalas süütegude tõkestamine, mis sisuliselt on osa riiklikust järelevalvest, ja sama paragrahvi lg-s 2 on öeldud, et riiklikule järelevalvele peatükki ei kohaldata.

Kuigi direktiivi kohaldamisala on mõistetud kitsendavalt, ei ole korrakaitse allutamine üldmäärusele, kus on rangemad isikuandmete kaitse nõuded ja vähem paindlikkust võrreldes direktiiviga, otseselt vastuolus EL õigusega, kuna lubatud on kehtestada ka direktiivis sätestatust rangemaid nõudeid vastavalt direktiivi artiklile 1(3). Oluline on seejuures arvestada, et korrakaitses tuleb sel juhul lähtuda isikuandmete töötlemisel üldmäärusest, mis on otsekohalduv. Meeles tuleb pidada ka EL õiguse kohaldamise ülimuslikkust ehk siin kontekstis vastuolu korral siseriikliku õiguse ja üldmääruse vahel kohaldatakse üldmäärust.

PPA Põhja prefektuuri korrakaitse büroo liiklusjärelevalvekeskuse juht oli 10.09.2018 kirjas politseidroonide korrakaitses kasutamise osas seisukohal, et „direktiiv numbriga 2016/680 laieneb üksnes süüteomenetlusele, mitte korrakaitselisele tegevusele.“[243] 10.09.2018 ei olnud Eesti veel direktiivi üle võtnud, mistõttu on selline seisukoht vaieldav arvestades eeltoodud 2015. a direktiivi materiaalse kohaldamisala laiendamist ja lisatud selgitusi. IKS jõustumisega 15.01.2019 allutati korrakaitse ehk riiklik järelevalve üldmäärusele, mistõttu kohalduvad rangemad andmekaitse nõuded, kui oleks kohaldunud jättes korrakaitse direktiivi kohaldamisalasse. Liiklusjärelevalvekeskuse juht leidis 19.09.2018 kirja lõpetuseks, et „/---/ saab kokkuvõtvalt väita, et jälgimisseadmestiku kasutamine politsei poolt korrakaitselises tegevuses on reguleeritud KorS-ga.“[244] See väide pole isikuandmete kaitse õiguse kontekstis korrektne. Ka enne IKS vastuvõtmist oleks pidanud politsei esindaja järeldama, et korrakaitsele õiguskaitseasutuste direktiivi mittekohaldumisel tuleb kohaldada üldmäärust, välja arvatud siis, kui tegevus on väljaspool EL õiguse kohaldamisala. IKS vastuvõtmisega allutati riikliku järelevalve käigus isikuandmete töötlemine üldmääruse kohaldamisalasse. Seega tuleks isikuandmete töötlemisel korrakaitselises tegevuses ehk riiklikus järelevalves ehk ohutõrjes lähtuda eestkätt üldmääruses sätestatust ning KorS-i ja korrakaitset puudutavaid eriseadusi

[243] H. Kullamäe. Politsei ja Piirivalveameti vastus 2.1-3/23169-3 K. Käsperi (Eesti Inimõiguste Keskus) poolt esitatud arupärimisele droonide kasutamise kohta, 10.09.2018.

[244] *Ibidem*.

lugeda koos üldmäärusega. Süüteomenetluses, välja arvatud tegevus väljaspool EL õiguse kohaldamisala, tuleks kohaldada aga siseriiklikku õigust, kuhu on direktiiv üle võetud.

3.2.2. Isikuandmete töötlemine tegevuse käigus, mis ei kuulu EL õiguse kohaldamisalasse

Üldmäärust ega õiguskaitseasutuste direktiivi ei kohaldata sellise isikuandmete töötlemise tegevuse käigus, mis ei kuulu liidu õiguse kohaldamisalasse. ELL artikli 4(2) viimase lause kohaselt on riigi julgeolek iga liikmesriigi ainuvastutuses. Õiguskaitseasutuste direktiivi preambuli p 14 selgitab, et direktiivi kohaldamisalasse kuuluva tegevusena ei tohiks käsitada riikliku julgeolekuga seotud tegevust, riikliku julgeoleku küsimustega tegelevate asutuste või üksuste tegevust ning isikuandmete töötlemist liikmesriikide poolt ELL V jaotise 2. peatüki kohaldamisalasse kuuluva tegevuse käigus.

IKS seletuskirjas selgitatakse, et Eestis hõlmab see julgeolekuasutusi, kelle tegevuse eesmärk on julgeolekuasutuste seaduse (JAS) § 2 lõike 1 järgi tagada riigi julgeolek põhiseadusliku korra püsimisega mittesõjaliste ennetavate vahendite kasutamise abil ning koguda ja töödelda julgeolekupoliitika kujundamiseks ja riigikaitseks vajalikku teavet. Üldmäärus ega IKS 4. peatükk, millega võeti siseriiklikku õigusesse üle õiguskaitseasutuste direktiiv, ei kohaldu seega JASi alusel nimetatud julgeolekuasutustele riigi julgeoleku tagamisel (JAS § 5 kohaselt on julgeolekuasutused Kaitsepolitseiamet ja Välisluureamet). Küll aga kohaldub seletuskirja kohaselt IKS 4. peatükk Kaitsepolitseiameti poolt isikuandmete töötlemisele, kui seda ei tehta riigi julgeoleku tagamiseks, vaid JAS § 6 punkti 3 kohaselt kuritegude tõkestamisel ning JAS § 6 punkti 4 alusel kuritegude kohtueelsel uurimisel, kuna sel puhul on täidetud direktiivi materiaalne kohaldamisala.[245]

Kuna riikliku julgeolekuga seotud isikuandmete töötlemine jääb direktiivi kohaldamisalast välja, ei saa nõustuda Aleksei Ivanovi 2018. aastal Tallinna Tehnikaülikoolis kaitstud magistritöö 1. peatüki järeldusega, mida on korratud ka kokkuvõttes, et „*[j]ulgeoleku tagamine* peab toimuma kooskõlas andmesubjektide põhiõiguste ja –vabaduste järgimisega ning *tuginema direktiivis 2016/680 sätestatud isikuandmete töötlemise põhimõtetele*.“[246] Selline järeldus on ekslik, kuna annab direktiivile palju laiema kohaldamisala, hõlmates materiaalsesse kohaldamisalasse ka riikliku julgeoleku tagamise, mis on väljaspool EL õiguse kohaldamisala.

[245] IKS seletuskiri, lk 20.

[246] A. Ivanov. Füüsilise isiku kui andmesubjekti osaluse suurendamine isikuandmete kogumise ja töötlemise protsessis. Magistritöö. Tallinn: TTÜ, 2018, lk 46.

Samuti ei ole võimalik direktiivile otse tugineda, välja arvatud siis, kui direktiiv pole võetud üle õigel ajal või on võetud üle valesti, kuna direktiiv pole otsekohalduv erinevalt määrusest[247]. Vale järeldus võis tuleneda sellest, et järelduseni jõudmisel ei hinnatud direktiivi isikulist ega materiaalset kohaldamisala.

Üldmääruse ja direktiivi kohaldamisala näitlikustav tabel isikuandmete töötlemisel masinnägemise kasutamisel õiguskaitseasutuste poolt Eestis alates 15.01.2019. Tabel ei hõlma kõiki isikuandmete töötlust puudutavaid õigusakte, vaid on mõeldud Eesti korrakaitse ja süüteomentluse kontekstis selgitama, millal kohaldub üldmäärus.

	Riikliku järelevalve menetlus ehk ohutõrje, sh vahetu sunni ja süüteoennetuse puhul (IKS § 12 lg 2; KorS § 1 lg 1^1)	Süüteomenetlus (IKS § 12 lg 1)	Julgeolekuasutuste tegevus riigi julgeoleku tagamisel
EL õigus	Harta ja üldmäärus	Harta ja siseriiklik õigus, kuhu võeti üle õiguskaitseasutuste direktiiv, eestkätt IKS 4. peatükk	EL õigus ei kohaldu
EIÕK, konventsioon 108 (tulevikus moderniseeritud konventsioon 108)	Kohaldub	Kohaldub	Kohaldub

[247] Vt nt EKo 05.10.2004, C-3717/01, *Pfeiffer jt.*

3.2.3. Korrakaitse ja süüteomenetluse eristamine

Vastavalt eelnevalt leitule on Eesti otsustanud kohaldada korrakaitseliste tegevuste puhul kõrgendatud isikuandmete kaitse nõudeid sisaldavat üldmäärust ning süüteomenetluse puhul IKS 4. peatükki, millega on üle võetud õiguskaitseasutuste direktiiv. Kuna korrakaitse ja süüteomenetluse puhul on seadusandja otsustanud kohaldada erinevaid õigusnorme, on oluline neid kahte menetlust eristada.

Riikliku järelevalvemenetluse ja süüteomenetluse eristamisel tuleb esmaseks aluseks võtta meetme objektiivne eesmärk ja objektiivse eesmärgi ebaselguse korral tuleb eesmärgi sisustamisel võtta arvesse ametniku tahet ja selle avaldumist[248]. Kui meetme eesmärgi väljaselgitamine ei ole võimalik või kui meede teenis kaht eesmärki (preventiivne ja repressiivne), tuleks eelistada meetme adressaadi õiguste kaitse seisukohalt tema jaoks soodsamat lahendust[249].

Vastavalt KorS § 1 lg-le 4 määrab tegevuse õigusliku aluse valiku riikliku järelevalve menetluse või süüteomenetluse vahel meetme objektiivne eesmärk. Korrakaitse (riikliku järelevalve menetluse) eesmärk on KorS § 2 lg 1 kohaselt avalikku korda ähvardava ohu ennetamine, ohukahtluse korral ohu väljaselgitamine, ohu tõrjumine ja avaliku korra rikkumise kõrvaldamine. Riikliku järelevalve puhul alustatakse menetlust, kui see on otstarbekas. Korrakaitse puhul on keskne tähendus ohu või rikkumise kõrvaldamisel ning rikkuja süül ega süüvõimel pole tähtsust. Süüteomenetluse eesmärk vastavalt karistusseadustiku (KarS) 1 lg-le 1 on süüteo toimepannud isiku väljaselgitamine ja karistamine. Süüteomenetluse puhul alustatakse menetlust legaliteedist ning keskne tähendus on süüteo toime pannud isiku süül ja süüvõimel.[250]

Nende kahe menetluse eristamine on keeruline, kuna õiguskaitseasutus võib kanda nn topeltfunktsiooni (nt Politsei- ja Piirivalveamet) ning menetlused võivad teatud juhtudel kattuda[251]. On võimalik ka olukord, kus riikliku järelevalve menetlus ja süüteomenetlus

[248] C. Eljas jt. Järelevalve- ja süüteomenetluse piiritlemine. Sisekaitseakadeemia, 2018, lk 13; RKÜKo 3-3-1-75-11, p 16.

[249] *Ibid*, lk 15; M. Laaring jt. Korrakaitseseadus: kommenteeritud väljaanne. Komm vlj. Tallinn: Siseakadeemia 2017. para 1, lg 4, komm 4.

[250] C. Eljas jt, lk 10.

[251] I. Pärnamägi, lk 34 jj; M. Kärner. Mõned korrakaitseseadusega kaasnenud muudatused kriminaalmenetluses: järelevalve- ja süüteomenetluse piiritlemisprobleem. – Juridica 2014/6, lk 474; C. Eljas jt; M. Laaring. Eesti korrakaitseõigus ohuennetusõigusena. Doktoritöö. Tartu: TÜ, 2015.

toimuvad paralleelselt. Sellisel juhul tuleb järgida mõlema menetluse reegleid[252], sh andmekaitsereegleid.

3.3. Tingimused masinnägemise, sh näotuvastuse, kasutamisel korrakaitses

Andmekaitsereeglid kohalduvad, kui töödeldakse, sealhulgas kogutakse või säilitatakse, tuvastatud või tuvastatavat füüsilist isikut puudutat teavet, sh ka pseudonümiseeritud ja krüptitud teavet (üldmääruse artiklid 1(1), 4(1-2); direktiivi artiklid 1(1) ja 3(1-2)). Töötlemine on ka videosalvestamine või edastamine ehk jälgimisseadmestiku kasutamine KorS § 34 mõttes.

Üldmääruse ja direktiivi materiaalsest kohaldamisalast on väljaspool anonüümsete andmete töötlemine (üldmääruse preambuli p 26; direktiivi preambuli p 21), mis tähendab, et teabest on kaotatud kõik jäljed, mis võiksid viia tuvastatavate isikuteni ning see on olnud tagasipööramatu ehk lõplik umbisikustamine[253].

3.3.1. Jälgimisseadmestiku kasutamine korrakaitses vastavalt isikuandmete kaitse üldmäärusele

KorS eristab jälgimisseadmestiku kasutamist (§ 34), isikusamasuse tuvastamist (§ 32) ja isikusamasuse tuvastamist erilise meetmega (§ 33). Nii ilma kui ka masinnägemisega jälgimisseadmestike puhul kohalduvad andmekaitsereeglid, kuna töödeldakse isikuandmeid[254]. Politsei- ja piirivalveameti pressiesindaja sõnul võimaldavad tänapäevasete valvekaamerate ja -süsteemide salvestised isikuid kiiresti tuvastada[255], millest järeldub, et kaamerad võimaldavad isiku tuvastamist. Jälgimisseadmestiku kasutatamise puhul korrakaitselises tuleb kinni pidada isikuandmete kaitse üldmääruse nõuetest.

Üldmäärusest tulenevad üldised põhimõtted artikkel 5 kohaselt on: seaduslikkus, õiglus ja läbipaistvus; eesmärgi piirang; võimalikult väheste andmete kogumine; õigsus; säilitamise piirang; usaldusväärsus ja konfidentsiaalsus ning töötleja vastutus nende nõuete täitmise eest.

---

[252] I. Pärnamägi, lk 34 jj;

[253] Isikuandmete töötleja üldjuhend. – Andmekaitse Inspektsioon, 31.05.2018, lk 12. Kättesaadav: https://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/Juhised/2019%20juhised/Isikuandmete%20tootleja%20uldjuhend.pdf (10.03.2019).

[254] R. Coseraru, lk 55; P. Lundevall-Unger, T. Tranvik. IP Addresses – Just a Number? – International Journal of Law and Information Technology, 2010/19, No 1, lk 53-73.

[255] Kutsumata külalised purustasid külapoe akna ja varastasid sigarette. – Tartu Postimees, 20.03.2019.

Kaamera, sh statsionaarne kaamera ja kehakaamera, on jälgimisseadmestik, mille kasutamine on riikliku järelevalve erimeede (KorS § 34). Jälgimisseadmestikku võib kasutada üksnes siis, kui korrakaitseseadus või eriseadus seda ette näeb. KorS § 34 lg 1 kohaselt võib jälgimisseadmestikku kasutada ohu väljaselgitamiseks ja tõrjumiseks või korrarikkumise kõrvaldamiseks. See säte on kooskõlas üldmääruse artikli 6(1)(e), 6(2) ja 6(3)-ga ehk sätestab aluse isikuandmete töötlemiseks jälgimisseadmestikuga ning säte vastab tingimusele, et töötlemine on vajalik avalikes huvides oleva ülesande täitmiseks või vastutava töötleja avaliku võimu teostamiseks, milleks selle sätte puhul on korrakaitselised eesmärgid (ohutõrje).

Põhiõiguste, sh isikuandmete kaitse õiguse piiramisel peab lähtuma harta artiklist 52(1): isikuandmete kaitse õigust tohib piirata (1) ainult seadusega, (2) arvestades isikuandmete kaitse õiguse olemust, (3) piirang peab olema proportsionaalne ehk piiranguid tohib seada üksnes juhul, kui need on vajalikud ning vastavad tegelikult EL-i poolt tunnustatud üldist huvi pakkuvatele eesmärkidele või kui on vaja kaitsta teiste isikute õigusi ja vabadusi[256,257]. Proportsionaalsuse põhimõte on sätestatud ka KorS §-s 7.

Haapsalu politseijaoskonna piirkonnavanem kommenteeris Haapsallu liikluskaamerate lisamisel, et kaameratest ei hakata liiklusvoogu jälgima, sest „selleks pole politseil inimjõudu". Vallavanem kommenteeris liikluskaamerate lisamist: „ei näe, et kaamerate puudus teedel oleks suur probleem. Aga see ei tähenda, et me poleks sellega nõus tegelema."[258] Vallavanema kommentaarist nähtub, et kaamerate lisamine ei pruugi olla vajalik. Samuti ei tohiks kaameratest kõike jälgida, mitte seetõttu, et selleks pole võimekust, vaid seetõttu, et see pole igas olukorras vajalik ega proportsionaalne. Türi vallas asuvasse 175 elanikuga Taikse külla plaanitakse paigaldada seitse valvekaamerat, mille video jõuab ööpäevringselt Politsei- ja Piirivalveametisse, kus see ka salvestatakse. Külaseltsi juhatuse liikme sõnul on „Taikses üldiselt rahulik /---/ [a]ga kuna tehnika on arenenud ja tekkis turvakaamerate võimalus, siis miks mitte ajaga kaasas käia."[259] Sellest kommentaarist järeldub samuti, et kaamerate paigaldamine ei pruugi olla vajalik. Kui külas on üldiselt rahulik, ei pruugi olla proportsionaalne lisada sinna 7 kaamerat, millest ööpäevläbi mööduvaid inimesi ja objekte reaalajas seiratakse.

[256] Nende tingimuste sisustamisest andmete muul eesmärgil töötlemise kontekstis täpsemalt vt C. Jasserand. Subsequent Use of GDPR Data for a Law Enforcement Purpose: The Forgotten Principle of Purpose Limitation? – University of Groningen Faculty of Law Research Paper Series, 2018/26, lk 11 jj.

[257] EIK ja EK kohtupraktika ülevaadet nende tingimuste osas valvekaamerate kontekstis vt R. Buckley. L&RS Note: Data Privacy and Community CCTV Schemes. – Oirechtas Library & Research Service, 08.01.2019, lk 25 jj.

[258] U. Lauri. Politsei soovib Läänemaa valve alla panna. – Lääne Teataja, 07.03.2019.

[259] S. Ratt. Taikse küla sai endale turvakaamerad. – Järva Teataja, 04.04.2019.

Avalike alade ulatusliku süstemaatilise jälgimise puhul tuleb läbi viia *ex ante* andmekaitsealane mõjuhinnang vastavalt üldmääruse artiklile 35(3)(c)[260]. Samuti tuleb mõjuhinnang läbi viia, kui hakatakse asukohta jälgima reaalajas. Andmekaitse Inspektsioon (AKI) on koostanud mõjuhinnangu tegemise kontrollnimekirja ning selgitanud, mida seejuures hinnata[261]. Kui ole kindel, kas innovatiivse tehnilise lahenduse jaoks on vajalik mõjuhinnangu läbiviimine, tuleks seda teha.[262]

Põhjendatud peaks olema, miks on jälgimisseadmestiku kasutamine konkreetsel juhul vajalik, miks see on sobiv vahend eesmärgi saavutamiseks ja miks on see proportsionaalne saavutatava eesmärgi suhtes, st puudub vähem õigusi riivav alternatiiv. Jälgimisseadmestike kontekstis võiks kaamera paigaldamine olla vajalik näiteks kõrge õnnetuste või õigusrikkumiste arvuga alal. Proportsionaalsuse kaalumisel tuleks leida tasakaal avaliku huvi ja individuaalsete huvide vahel ning hinnata ka kaamera asukoha sobivust ja kaamera tehnilist võimekust. Tuleks põhjendada masinnägemisega nutikamaks tehtud kaamerate vajadust, sobivust ja proportsionaalsust kitsamas tähenduses. Samuti tuleb põhjendada kaamera asukohta – miks on üldiselt turvalise ilma suuremate probleemideta avaliku asukoha ööpäevringne reaalajas jälgimine vajalik.

Isikuandmete töötlemine peab artiklist 5(1)(b) tulenevalt olema üldjuhul eesmärgipärane. Ka harta artikkel 8(2) kohaselt tuleb isikuandmeid töödelda asjakohaselt ning kindlaksmääratud eesmärkidel. Üldmääruse preambuli p-s 50 on selgitatud, et isikuandmete töötlemine muudel eesmärgil kui need, milleks isikuandmed algselt koguti, peaks olema lubatud üksnes juhul, kui töötlemine on kooskõlas eesmärkidega, mille jaoks isikuandmed algselt koguti. Samas punktis on ka selgitatud, et võimalikest süütegudest või avalikku julgeolekut ähvardavatest ohtudest teatamine ning sama kuriteoga või avalikku julgeolekut ähvardavate ohtudega seotud üksikjuhtumi või mitme juhtumi korral asjakohaste isikuandmete edastamine pädevale asutusele on õigustatud. Seega on korrakaitselisel eesmärgil paigaldatud jälgimisseadmestikuga kogutud isikuandmete edasine töötlemine süüteomenetluses lubatud. Muul eesmärgil töötlemine peab olema töötleja pädevuse piires ning see töötlemine peab olema saavutatava muu eesmärgi suhtes vajalik ja proportsionaalne (üldmääruse artikkel 6(4))[263].

[260] Mõjuhinnangu kohta vt Isikuandmete töötleja üldjuhend, lk 23 jj.

[261] *Ibid*, lk 46, 50-51.

[262] Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing is "Likely to Result in a High Risk" for the Purposes of Regulation 2016/679. – Article 29 Data Protection Working Party, 04.04.2017.

[263] C. Jasserand, lk 8.

Väärteomenetluse seadustikust (VTMS) tulenevalt on väärteo tunnuste ilmnemisel kohtuväline menetleja kohustatud alustama ja läbi viima väärteomenetluse, kui tegu ei ole kohtuvälise menetleja veendumuse kohaselt vähetähtis või puuduvad väärteomenetluse seadustiku §-s 29 sätestatud väärteomenetlust välistavad asjaolud (VTMS § 31 lõige 1). Kuna kaamerate avalikesse kohtadesse lisamine ja väärteo tunnuste tuvastamine on võimalik masinnägemisel abil muuta efektiivsemaks, on oluline pidada kinni eesmärgi piirangu põhimõttest ning seada masinnägemise eesmärgiks tuvastada vaid sellised objektid, isikud või olukorrad, mis on eesmärgi saavutamiseks vajalikud.

KorS § 34 lg 3 kohustab jälgimisseadmestikust teavitama sildiga „VIDEOVALVE“, sõidukis jälgimisseadmestiku kasutamisel tuleb see paigutada kleebisega nähtavale kohale. Paragrahvis ei ole reguleeritud teavitamist juhuks, kui jälgimisseadmestik on politseiniku keha peal (kehakaamera) või näiteks drooni küljes. Analoogia alusel tuleks siiski ka sellistel puhkudel jälgimiseadmestikust teavitada. Vabariigi Valitsuse jälgimisseadmestiku kasutamisest avalikkuse teavitamise korra määruse[264] § 1 lg 1 kohaselt teavitatakse avalikkust jälgimisseadmestiku kasutamisest avalikku kohta paigutatud teabetahvli või korrakaitseorgani sõidukisse paigutatud kleebisega. See määratlus on liiga kitsas, kuna ei sisalda kehakaameraid, mille kasutamisest tuleks samuti teavitada. Sama paragrahvi lg 2 kohaselt võib lisada avalikku kohta paigutatavale teabetahvlile jälgimisseadmestikku kasutava korrakaitseorgani vapi kujutise, et anda informatsiooni isikuandmete töötleja kohta. See säte pole kooskõlas isikuandmete kaitse üldmäärusega, mis nõuab isikuandmete töötlemisel läbipaistvust. Süüteomenetluses on läbipaistvuse nõude ülatus väiksem ning on sätestatud IKS §-des 22 ja 23. Kuna korrakaitse eesmärgil töötlemine on allutatud isikuandmete kaitse üldmäärusele, tuleb korrakaitses jälgimisseadmestike kasutamise puhul täita üldmääruse nõudeid, sh läbipaistvuse nõuet. Läbipaistvuse nõude kohaselt tuleb inimesele, kui temalt andmeid kogutakse, anda andmetöötleja ja andmetöötluse kohta teavet. Olulisim andmekaitsetingimustest teavitamise puhul on see, et teave oleks kergesti arusaadav ja lihtsasti kättesaadav (üldmääruse preambuli p 39)[265]. Kui inimene ei tea, kelle jälgimisseadmestikuga tegu on, ega pole kirjas, kust leida sellekohast infot, ei saa pidada andmekaitsetingimustest teavitamist kergesti arusaadavaks ja lihtsasti kättesaadavaks (üldmääruse preambuli p 39). Muuhulgas peaks olema avalik informatsioon jälgimisseadmestiku tehnilise funktsionaalsuse kohta, sh kas kasutatakse

[264] Vabariigi Valitsuse jälgimisseadmestiku kasutamisest avalikkuse teavitamise korra määrus – RT I, 26.06.2014, 2.

[265] Vt ka Andmekaitse Inspektsioon. Isikuandmete töötleja üldjuhend, lk 43-45.

masinnägemist, kuidas ning millises ulatuses seda tehakse. Seda informatsiooni teadmata on andmesubjektil keeruline hinnata oma õiguste riivet.

Andmete säilitamise aeg peaks olema piiratud rangelt minimaalsega. Säilitamise piirang on sätestatud KorS § 34 lg-s 2, mis näeb ette, et videosalvestist peab säilitama vähemalt üks kuu, kuid mitte kauem kui aasta, välja arvatud siis, kui seadusega on sätestatud teisiti. Võrdluseks, et Iirimaal on korrakaitse videokaamera andmete säilitamise maksimaalne aeg 30 päeva[266], mistõttu on vaieldav, kas aasta aega video säilitamist on siiski rangelt minimaalne vajalik aeg.

Isikuandmetele ja neid töötlevatele seadmetele ei tohi olla loata ligipääsu (üldmääruse artikkel 1(1)(f), preambuli p 39). Kaamerapilti tohiks näha vaid töötaja, kellel on vaja seda tööülesannete täitmiseks vaadata. Häirekeskuse töötaja kirjeldas ajakirjanduses, kuidas „[k]ord olid häirekeskuses külas koolilapsed. Muu hulgas näidati neile kaamerate pilti reaalajas. Ja lapsi saatev õpetaja tundis ära vanalinnas jalutava õpilase, kes tegelikult pidi olema haigena kodus.“[267] Selline olukord on konfidentsiaalsuse nõude rikkumine, mida ei tohiks juhtuda. Andmekaitse Inspektsioon on selgitanud, et „[o]lenemata sellest, mis alusel kaameraid kasutatakse, tuleb isikuandmete kaitseks võtta kasutusele organisatsioonilised, füüsilised ja infotehnilised turvameetmed, et tagada andmete terviklikkus, käideldavus ja konfidentsiaalsus. Andmete turvalisuse tagamiseks peab vältima kõrvaliste isikute ligipääsu jälgimisseadmetele ning hoidma ära salvestiste omavolilise jälgimise, kopeerimise, muutmise, teisaldamise ja kustutamise. Tagantjärele peab olema võimalik kindlaks teha, millal ja milliseid andmeid vaadati, salvestati, muudeti või kustutati ning kes seda tegi. Selleks tuleb jälgimiseks kasutatavad vahendid seadistada selliselt, et igal kasutajal on süsteemi sisenemiseks oma kasutajanimi ja parool.“[268]

Jälgimisseadmestiku kasutamisel tuleb järgida andmesubjekti õigusi, sealhulgas teavitada andmesubjekti isikuandmetega seotud rikkumisest või teha sellekohane avalik teadaanne, kui isikute teavitamine on ebaproportsionaalselt raske (artikkel 34) ning väljastada andmesubjektile tema soovi korral tema kohta olemasolevad andmed (artikkel 15). Andmete väljastamisel andmesubjektile ei tohiks rikkuda teiste andmesubjektide õigusi ehk video puhul peaks olema

[266] Code of Practice for Community Based CCTV Systems. – Department of Justice and Equality. Kättesaadav: http://www.justice.ie/en/JELR/PD_001_Code_of_Practice.pdf/Files/PD_001_Code_of_Practice.pdf (10.04.2019).

[267] T. Herm.

[268] S. Biin. Ringkiri jälgimisseadmestiku kasutamisest kohalikes omavalitsustes. – Andmekaitse Inspektsioon, 24.03.2016. Kättesaadav: https://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/Ringkiri_jalgimisseadmestiku_kasutamisest.pdf (10.03.2019).

muudetud teised videos olevad inimesed tehniliste vahendite abil tundmatuks. Andmesubjektil on õigus olla unustatud ehk nõuda teda puudutavate andmete kustutamist teatud eranditega, näiteks ei pea andmeid kustutama, kui need on vajalikud avalikes huvides ülesande täitmiseks (üldmääruse 3. peatükk 3. jagu). Andmesubjekti õigusi võib piirata üldmääruse artiklis 23 toodud eranditega.

Järgida tuleb lõimitud andmekaitse ja vaikimisi andmekaitse põhimõtteid (üldmääruse artikkel 25). Tarkvara kasutusele võtmisele eelnevalt tuleb kindlaks teha, et see on turvaline. Nende põhimõtetega on seotud töötlemise vajalikkuse tingimus (üldmääruse artikkel 5). Tarkvara ei tohiks töödelda andmeid, mille töötlemine ei ole vajalik eesmärgi saavutamiseks. Tulenevalt üldmääruse artiklist 37(1)(c) peab jälgimisseadmestiku vastuval töötlejal olema määratud andmekaitseametnik.

Lisaks eeltood jälgimisseadmestike kasutamise üldistele andmekaitsepõhimõtetele tuleb arvestada, et eriliigiliste isikuandmete töötlemisele on kõrgemad isikuandmete kaitse nõuded (üldmääruse artikkel 9; direktiivi artikkel 10).

3.3.2. Isikusamasuse tuvastamine masinnägemise abil

Isikusamasuse tuvastamine on meede, mida võib kohaldada nii riikliku järelevalve menetluses kui ka väärteomenetluses (topeltfunktsiooniga). See meede on sätestatud nii korrakaitse- kui ka süüteomenetluse regulatsioonis – KorS § 32, KrMS § 140[1]. Väärteomenetluse seadustikus ei ole viidet KorS §-le 32 (isikusamasuse tuvastamine), kuid kriminaalmenetluses on lubatud isikusamasust tuvastada (KrMS § 140[1]). Kuna kriminaalmenetlus on n-ö juhtivaks menetluseks väärteomenetlusele, on lubatud tuvastada sama regulatsiooni järgi ka menetlusalune isik.[269] Erilise tuvastusmeetmega (KorS § 33) võib tuvastada vaid siis, kui KorS § 32 meetmega tuvastamine ei ole võimalik või on ebaproportsionaaselt raske. Sama on sätestatud ka KrMS §-s 140[1]. Masinnägemisega isikutuvastamine on eriline tuvastusmeede KorS § 33 tähenduses.

Eriliiki isikuandmed on kõrgema kaitse all ning nende töötlemine on üldmääruse järgi üldiselt keelatud teatud eranditega (üldmääruse artikkel 9) ning direktiivi järgi lubatud vaid siis, kui see on rangelt vajalik ning täidetud on teatud eeldused (direktiivi artikkel 10). Eriliiki isikuandmete alla kuuluvad biomeetrilised andmed (üldmääruse artiklid 4(14) ja 9; direktiivi artiklid 3(13) ja 10). Biomeetrilised isikuandmed on „konkreetse tehnilise töötlemise abil saadavad

[269] C. Eljas jt.

isikuandmed isiku füüsiliste, füsioloogiliste ja käitumuslike omaduste kohta, mis võimaldavad kõnealust füüsilist isikut kordumatult tuvastada või kinnitavad selle füüsilise isiku tuvastamist“ (üldmääruse artikkel 4(14); direktiivi artikkel 3(13)). Üldmääruse peambuli p 51 selgitab, et „[f]otode töötlemist ei peaks süstemaatiliselt käsitlema isikuandmete eriliikide töötlemisena, kuna need on hõlmatud üksnes biomeetriliste andmete määratlusega, kui neid töödeldakse konkreetsete tehniliste vahenditega, mis võimaldavad füüsilist isikut kordumatult tuvastada või autentida.“ Seega biomeetriliste andmete töötlemine ei hõlma igasugust fotode või video töötlemist, vaid konkreetse tehnilise vahendiga töötlemist, mis võimaldab isiku kordumatut tuvastamist või autentimist. Biomeetriliste andmete seas on mh näokujutis ja sõrmejäljed. Oluline on seega, milline on jälgimisseadmestiku tehniline võimekus. Kui kaamera tehniline võimekus on selline, et tuvastatakse biomeetrilisi andmeid, näiteks tuvastatakse videol olev näokujutis, võimaldab kaamera tehniline tase isiku kordumatut tuvastamist ning töödeldakse seega biomeetrilisi andmeid, mis on eriliigilised isikuandmed. Kaamerate tehnilise võimekuse tõstmisel võib seega muutuda isikuandmete kaitse õiguse riive ulatus, mis mõjutab omakorda töötlemise proportsionaalsust. Seetõttu tuleb kaamera (või muu sensori) tehnilisele tasemele tähelepanu pöörata, kui hinnatakse seda, kas kaamera kasutamine vastab andmekaitsereeglitele.

Isikusamasuse tuvastamine erilise meetmega hõlmab seega biomeetriliste andmete töötlemist. Üldmääruse artikkel 9(1) kohaselt on üldjuhul keelatud eriliigilisi isikuandmeid töödelda. Artiklit 9(2) sätestab juhud, kui artiklit 9(1) ei kohaldata. Korrakaitse ja näotuvastust võimaldavate avalikesse kohtadesse paigutatud kaamerate kontekstis on sobiv alus artikkel 9(2)(g), mis annab erandi, kui töötlemine on vajalik olulise avaliku huviga seotud põhjustel liidu või liikmesriigi õiguse alusel ning on proportsionaalne saavutatava eesmärgiga, austab isikuandmete kaitse õiguse olemust ja tagatud on sobivad ja konkreetsed meetmed andmesubjekti põhiõiguste ja huvide kaitseks. Need tingimused peavad olema täidetud kumulatiivselt.

Süüteomenetluses eriliigiliste isikuandmete töötlemise üldist keeldu ei ole. Direktiivi artikkel 10(a-c) kohaselt on eriliigilist andmete töötlemine lubatud üksnes siis, kui see on rangelt vajalik, sellele kohaldatakse andmesubjekti õiguste ja vabaduste kaitsmiseks asjakohaseid kaitsemeetmeid ning üksnes järgmistel juhtudel: see on lubatud liidu või liikmesriigi õigusega või et kaitsta andmesubjekti või teise füüsilise isiku elulisi huve või selliselt töödeldakse isikuandmeid, mille andmesubjekt on ilmselgelt avalikustanud. Tegemist on alternatiivsete alustega, millest näotuvastuse kontekstis on relevantsed esimesed kaks.[270]

[270] Nende eelduste sisustamise osas vt M. Miidla, lk 23 jj; Süüteomenetluses biomeetriliste andmete töötlemise tingimustest vt *Ibid,* lk 78 jj; Ristkasutuse kohta *Ibid,* lk 83 jj; Isikusamasuse tuvastamisest *Ibid,* lk 91 jj.

Õiguskaitseasutuste direktiivi preambuli p 26 selgitab, et õiguskaitseasutustel ei ole iseenesest selliste tegevused nagu varjatud jälitustoimingud või videovalve keelatud. Sellised toimingud on lubatud süütegude tõkestamise, uurimise, avastamise ja nende eest vastutusele võtmise või kriminaalkaristuste täitmisele pööramise, sealhulgas avalikku julgeolekut ähvardavate ohtude eest kaitsmise ja nende ennetamise eesmärgil, kui need on õigusaktis ette nähtud ning kujutavad endast demokraatlikus ühiskonnas vajalikku ja proportsionaalset meedet ning nende puhul arvestatakse nõuetekohaselt asjaomase füüsilise isiku õigustatud huve. Isikuandmeid tuleks töödelda üksnes juhul, kui nende töötlemise eesmärki ei ole mõistlikult võimalik saavutada muude vahendite abil (proportsionaalsus kitsas tähenduses).

Kuna masinnägemise abil isikusamasuse tuvastamine on isikuandmete kaitse õigust tugevalt riivav, peab selle kasutamine olema õigustatud ning läbi tuleb viia *ex ante* hinnang, kas selle rakendamise tingimused on täidetud. Proportsionaalsuse hindamisel tuleb arvesse võtta kaamera tehnilist võimekust ja funktsionaalsust, kuna see mõjutab oluliselt isikandmete kaitse riivet. ÜRO privaatsuse eriraportööri[271] hinnangul peab automatiseeritud näotuvastuse kasutamiseks olema tugev õigustus, näiteks terrorirünnaku risk või raskete kuritööde risk. Avalikku kohta, kus aeg-ajalt pannakse toime kergemaid süütegusid, võib olla õigustatud teatud juhtudel jälgimisseadmestiku paigaldamine, ent mitte automatiseeritud isikutuvastuse võimekusega seadme paigaldamine[272]. Näiteks Malta valitsus planeeris 2019. aasta eelarvesse näotuvastustehnoloogia paigaldamise tänavatele, kuid pärast avalikku kriitikat meetme ebaproportsionaalsuse osas otsustati ringi, et videokaameratele näotuvastustehnoloogiat ei lisata[273].

Avalik võim tohib sekkuda põhiõigustesse üksnes seadusega kindlaksmääratud tingimustel ja ulatuses[274]. Seadusereservatsiooni nõudest tulenevalt peab põhiõigusi puudutavates küsimustes kõik põhiõiguste realiseerimise seisukohalt olulised otsused langetama seadusandja[275], eriti kui täitevvõimu tegevus kohustab isikuid või piirab nende õigusi[276]. Mida intensiivsem on isikute põhiõiguste piiramine, seda üksikasjalikumalt peab see olema sätestatud seaduses.

---

[271] Legal Clarifications on Facial Recognition. – SZA Blog, 02.04.2019. Kättesaadav: http://blog.szalawfirm.com/legal-clarifications-on-facial-recognition/ (01.04.2019).

[272] *Ibidem*.

[273] *Ibidem*.

[274] RKHKo 3-3-1-41-00.

[275] RKÜKo 3-3-1-41-06, p 21; RKÜKo 3-4-1-19-07, p 25.

[276] RKÜKo 3-4-1-10-00, p 28.

KorS § 33 lg 5 kohaselt kehtestab erilise tuvastusmeetme kohaldamise korra kehtestab valdkonna eest vastutav minister määrusega[277], mille § 3 lg 8 kohaselt võib isiku või tema kehaosa fotod, mida andmebaasis olevate biomeetriliste andmetega võrreldakse, valmistada ka filmisalvestise üksikutest kaadritest. Täpsemalt masinnägemise abil isikutuvastuse kasutamise tehnilist poolt ja laadi sätestatud pole. Märksa sisukamalt on aga näiteks kirjeldatud DNA ja käekirjaproovi võtmist. Seaduslikkus tähendab EIK kohtupraktika[278] kohaselt seda, et piirangul on olemas õiguslik alus, seadus peab olema adevkaatselt kättesaadav ja ettenähtav, piisava täpsusastmega, et inimene saakse selle kohaselt oma käitumist reguleerida. EIK kohtupraktika kohaselt sõltub seaduse detailsuse nõutav aste konkreetsest meetmest, valdkonnast ja adressaatide arvust[279]. Seaduslikkus on seotud laiemalt ka sellega, kas riive on demokraatlikus riigis vajalik[280], mis tähendab, et sekkuv meede peab vastama "tungivale sotsiaalsele vajadusele" ja olema „proportsionaalne võrreldes taotletava õiguspärase eesmärgiga".[281] Arvestades masinnägemise abil isikutuvastuse kasutamisel isikuandmete kaitse riive intensiivsust, peaks olema selle tehnoloogia kasutamise tingimused ja tehnilised nõuded täpsemalt sätestatud.

Kaamerate kasutamine ei ole õigustatud vähese tähtsusega õigusrikkumiste tuvastamiseks[282]. Ühetaolist ja üldist lähenemist tuleb vältida ning valida ja paigaldada kaamerad vastuseks konkreetsele ja reaalsele turvariskile[283]. Ainult inimese grupilise kuuluvuse põhjal, nt osalemise tõttu kogunemisel või üritusel, ei tohiks tema isikuandmeid koguda[284]. Näotuvastuse kasutamisel paljute inimeste peal või rahvahulgas on oht stigmatiseerimisele - süütu inimese andmeid kasutatakse sama moodi nagu kahtlusaluse andmeid[285]. Alaealiste peal näotuvastust kasutada ei tohi[286]. EK kohtupraktika[287] kohaselt peaks riigi pädevad ametiasutused, kellele on

[277] Erilise tuvastusmeetme kohaldamise kord - RT I, 04.06.2014, 11.

[278] EIKo 04.12.2008, ühendatud kohtuasjad 30562/04 ja 30566/04, *S. ja Maprer v the United Kingdom,* p 95; EIKo 02.08.1984, 8691/79, *Malone v the United Kingdom,* para 66-68; EIKo 04.05.2000, 28341/95, *Rotaru v Romania,* para 55; EIKo 16.02.2000, 27798/95, *Amann v Switzerland,* para 56.

[279] EIKo 26.10.2000, 30985/96, *Hasan and Chaush v. Bulgaria,* para 84, p 96.

[280] EIKo 24.01.2019, 43514/15, *Catt v UK*, para 106-107.

[281] EIKo 24.03.1988, 10465/83, *Olsson v Sweden*.

[282] Working Document on the Processing of Personal Data by Means of Video Surveillance. – Article 29 Data Protection Working Party, 25.11.2002, lk 16.

[283] *Ibid*, lk 21.

[284] *Catt v UK*, para 123-124; EIKo 06.06.2006, 62332/00, *Segerstedt-Wiberg and Others v Sweden*, para 79.

[285] *Catt v UK*, para 124.

[286] EIKo 16.12.1999, 24724/94, *T. v the United Kingdom,* para 75, 85.

[287] EKo 21.12.2016, ühendatud kohtuasjad C-203/15 ja C-698/15, *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others.*

antud juurdepääs säilitatavatele andmetele, teavitama sellest asjassepuutuvaid isikuid kohaldatavate riigisiseste menetluste raames alates hetkest, kui see teavitamine ei saa enam kahjustada nende ametiasutuste läbiviidavat menetlust. Selline teavitamine on vajalik selleks, et puudutatud isikud saaks juhul, kui nende õigusi on rikutud, kasutada õiguskaitsevahendeid.[288] Teavitamise kohustus on sideettevõtjalt andmete saamisel sätestatud ka KorS § 35 lg-s 2. Kuigi näotuvastuse puhul ei saa õiguskaitseasutus andmeid sideettevõttelt, vaid kogun isikuandmeid ise, on siiski olemas sarnasus, mis puudutab töötlemisest teavitamise problemaatikat. Võiks argumenteerida, et automatiseeritud näotuvastuse puhul peaks andmesubjektile sellest teada andma, vastasel korral ei saada ta teada, et tema isikut masinnägemisega tuvastati ega saa seetõttu kasutada õiguskaitsevahendeid.

Isikuandmete kaitse reeglite rikkumise kahtluse korral on võimalik pöörduda sõltumatu isikuandmete kaitse asutuse poole, milleks Eestis on AKI (IKS § 28, 51jj). Samuti saab pöörduda hagiavaldusega kohtusse.

3.3.3. Näotuvastustehnoloogial põhineva isikusamasuse tuvastamine UK-s

Masinnägemisel põhineva näotuvastuse reguleerimine on päevakorras UK-s[289], kriitikute sõnul on näotuvastustehnoloogiat testitud "õiguslikus vaakumis" ilma kasutust piiravate regulatsioonideta.[290] Kuigi UK siseministeeriumi väitel rakendatakse testimise reguleerimiseks riigisisest andmekaitseseadust, valvekaamerate head tava ja asjakohaseid inimõigustest tulenevaid printsiipe, ei käsitle neist ükski konkreetselt näotuvastustehnoloogia kasutamist politseitöös. Samuti on UK siseministeerium enda koostatud biomeetria strateegias tunnistanud, et näotuvastustehnoloogia jälgimise regulatsioon ja järelvalve vajavad tugevdamist.[291] Vajalikkuse põhimõtet näotuvastuse konktekstis hinnatuna on leitud, et näotuvastust peaks rakendama valikuliselt, st usutavate, dokumenteeritud ja oluliste ohuallikatele tuvastamise korral[292].

---

[288] *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others*, para 121.

[289] The Work of the Biometrics Commissioner and Regulator Inquiry – Publications. – UK Parliament. Kättesaadav: https://www.parliament.uk/business/committees/committees-a-z/commons-select/science-and-technology-committee/inquiries/parliament-2017/work-of-biometrics-commissioner-and-forensic-science-regulator-17-19-17-19/publications/ (15.04.2019).

[290] Face Off: The Lawless Growth of Facial Recognition in UK Policing. – Big Brother Watch, 10.05.2018, p.3.

[291] J. Purshouse, L. Campbell. Privacy, Crime Control and Police Use of Automated Facial Recognition Technology. – Criminal Law Review 2019/3, lk 15.

[292] *Ibid*, lk 21.

Purhouse'i ja Campelli hinnangul peaks UK seadusandja kehtestama eeskirjad, mis reguleerivad politsei volitusi näotuvastuse järelevalve teostamiseks avalikus ruumis, et tagada selle järjepidevus erinevates üksustes. Kehtiv UK regulatiivne raamistik on nende hinnangul liialt üldsõnaline, võimaldades erinevaid ja kohati murettekitavaid põhjendusi ja tavasid näotuvastuse. Nad leiavad, et näotuvastuse kasutamine võimaldab seni tundmatuid viise inimõiguste riiveks, tuleb politsei volitustele seada konkreetsed piirid ja reeglid, sh minimaalsed õigusi kaitsvad kriteeriumid jälgimisnimekirjade koostamisele, isikliku info kogumisele, töötlemise ja talletamisele ja näotuvastus süsteemide ja kasutatavate piltide kvaliteedile. Reguleeriv raamistik peaks tagama läbipaistvuse ja aruandekohustuse iga näotuvastuse kasutamisjuhtumi korral politseitöös, sh info avalikustamine tehnoloogia tulemuslikkuse (täpsuse) ja valepositiivsete vastete ning nende pinnalt läbiviidud sekkumiste arvu kohta. Samuti on välja pakutud, et oleks vajalik määratleda, millised inimesed jälgimisnimekirjadesse lisatakse, kuna sinna lisatavatel isikutel on suurem tõenäosus saada häbimärgistatud. On pakutud välja, et nimekirjadesse võiksid sisse olla arvatud isikud, kes: (1) on tagaotsitavad seoses kuriteoga või (1) kujutavad usutavasti avalikule turvalisusele olulist ohtu (sh iseendale) ja 1. või 2. punktile lisaks on tõenäoliselt näotuvastuse jälgimisala läheduses.[293] Võrdluseks, et Eesti ABIS andmebaasi oleks koondatud kõik Eesti inimesed.

Näotuvastuse kasutamine võimendab tavaliste videokaameratega jälgimisega võrreldes võimalikku privaatsusõiguse riivet, kuna see võimaldab kogutud ja olemasoleva info baasilt luua isiku kohta uut infot, so kas isik peaks olema kõrgendatud tähelepanu all või mitte. See rikub Purhouse'i ja Campelli arvates sotsiaalset kokkulepet avalikus ruumis viibiva isiku informatsiooni liikumise kohta.[294]

On kritiseeritud, et biomeetrilistel andmetel põhineva näotuvastuse kasutamine riivab isiku privaatsusõigust, kuna isiku näo infoks konverteerimine on dehumaniseeriv ning protsessi käigus isikuandmetena kajastatud kehaosi kasutatakse ja kontrollitakse kellegi teise poolt.[295] Seetõttu võib isik kaotada kontrolli enda näo geomeetriliste tunnuste üle, mis omandavad uusi isiku jaoks teadmatuks jäävaid tähendusi ning mida kasutatakse väljaspool isiku keha.[296]

Kriitikud ütlevad ka, et ainuüksi teadlikkus automatiseeritud näotuvastuse olemasolu kohta on piisav, et jälgitavad subjektid enda käitumist muudaksid. Pidev jälgimine vähendab inimeste

[293] *Ibid*, lk 22.

[294] *Ibid*, lk 10.

[295] P. Brey. Ethical Aspects of Facial Recognition Systems in Public Places. – Journal of Information, Communication and Ethics in Society 2004/2, No 2, lk 97, 107.

[296] J. Purshouse, L. Campbell, lk 10.

võimalikke aktsepteeritud uskumuste ja käitumisotsuste valikut, mis viib inimeste käitumise järkjärgulisele ühtlustumisele. Tulemuseks on ühikonnas väärtustatud mitmekesisuse vähenemine. Privaatsuse vähenemine võib aja jooksul vähendada lisaks väljendatavale individuaalsusele ka inimeste sisemist püüdlust selles suunas.[297]

Kuigi ka praegu võib võõraste tähelepanu alla sattumist ette tulla, on reeglina tegu hetkelise, mitte pikaajalise jälgimisega. Just viimast võimaldab näotuvastuse kasutus, mis eristab tehnoloogiat seni kasutatud tavakaameratest. Inimestel ei ole mõistlikku ootust, et neid avalikus kohas jälgitakse, mistõttu on tehnoloogiat kasutaval õiguskaitseasutusel kohustus põhjendada selle tehnoloogia kasutust EIÕK art 8 lg 2 põhjal[298] ning EL õiguse kohaldamisalas vastavalt hartale ja üldmäärusele või siseriiklikule õigusele, kuhu on üle võetud õiguskaitse asutuste andmekaitsedirektiiv.

UK on näotuvastuse jaoks koostanud seaduseelnõu, mida on aga kritiseeritud, kuna see võimaldab näotuvastusega kogutud andmete edastust nii riigiasutustele kui ka „mitte-riiklike asutustele" ning lisab näotuvastuse andmebaasi kõikide inimeste identiteedidokumendid, nagu näiteks juhiload. Kriitikud leiavad, et näotuvastuse andmebaasis võiks olla ainult raskes süüteos süüdi mõistetud inimesed.[299] UK vastu pöörduti näotuvastuse kasutamise tõttu ka kohtusse. Hagis väidetakse, et lisaks siseriikliku õiguse rikkumistele rikub näotuvastus EIÕK artikleid 8, 10, 11 ja 14[300,301].

Võimalus on näotuvastust reguleerida detailsemalt nt n-ö pehmete meetmetega, näiteks hea tava või juhtnööre pakkuva dokumendiga. UK *Biometrics and Forensics Ethics Group* avalikustas 2019. aasta veebruaris näotuvastuse kasutamise printsiibid seoses avaliku huvi, efektiivsuse, eelarvamuste ja diskrimineerimise vältimise, erapooletuse, vajaduse, proportsionaalsuse, aruandekohustuse ja järelvalve jälgitavate isikute nimekirjade koostamise, avaliku usalduse ja kuluefektiivsusega. Lisaks üheksale printsiibile pakutakse raportis välja üheksa spetsiifilist küsimust samade printsiipide lõikes, mis tulenevad reaalajas näotuvastuse kasutamisest politsei

[297] J. E. Cohen. Examined Lives: Informational Privacy and the Subject as Object. – Stanford Law Review 2000/52, lk 1373, 1425-1426.

[298] J. Purshouse, L. Campbell, lk 11.

[299] C. Petrie. Identity-matching Services Bill 2018 and Australian Passports Amendment (Identity-matching Services) Bill 2018. Eelnõu 110 seisuga 07.02.2018. – Parliament of Australia, 22.05.2018; L. Campbell. Why Regulating Facial Recognition Technology is So Problematic – and Necessary. – The Conversation, 26.11.2018.

[300] M. Goulding. Letter Before Claim. Correspondence to Matt Jukes. Kättesaadav: https://www.libertyhumanrights.org.uk/sites/default/files/180611%20Letter%20before%20action%20to%20SWP.pdf (12.03.2019).

[301] *Ibid*, lk 7jj.

poolt.[302] Näotuvastusele n-ö pehmete meetmetega reguleerimisel ei pea n-ö jalgratast leiutama, vaid tasub lähtuda teiste riikide kogemusest, sh võtta arvesse näiteks neid printsiipe[303].

Kokkuvõtlikult võib teha järelduse, et direktiivi kohaldamisalas on ka riiklik järelevalve, kuid kuna Eesti siseriiklikku õigusesse ülevõtmisel tõlgendati direktiivi kohaldamisala kitsendavalt, kohaldub riiklikule järelevalvele Eestis üldmäärus. Samas ei tohi direktiivi kohaldamisala tõlgendada laiendavalt nagu kohalduks see ka riikliku julgeoleku tagamisele, mis on väljaspool EL õiguse kohaldamisala.

Eelneva analüüsi põhjal tuvastati jälgimisseadmestike kasutamisel Eesti korrakaitses mitmeid andmekaitsega seonduvaid probleeme. Vältida tuleks jälgimisseadmestike osas ühetaolist lähenemist nagu ei sõltuks jälgimisseadmestike eri seadmetest, nende asukohtadest, kasutusviisidest ja tehnoloogiast jälgimisseadmestiku kasutuse õigustatus. Selline seisukoht on ekslik. Osadel juhtudel on kaheldav, kas jälgimisseadmestiku paigaldamine on vajalik ja proportsionaalne meede saavutatava eesmärgi suhtes. Probleeme tuvastati ka läbipaistvuse, andmete säilitamise pikkuse ja konfidentsiaalsusega.

Näotuvastuse puhul töödeldakse biomeetrilisi andmeid, mis on isikuandmete eriliik. Biomeetriliste andmete töötlemine üldmääruse kohaldamisalas on üldiselt keelatud. Direktiiv on selles suhtes paindlikum ning üldist keeldu töötlemisele ei ole. Nii üldmäärus kui ka direktiiv sätestavad sobivad alused näotuvastuse kasutamisele – vastavalt üldmääruse artikkel 9(2)(g) ja direktiivi artikkel 10(a-c). Igal juhul tuleb hinnata nii jälgimisseadmestiku kui ka automatiseeritud biomeetrilise isikusamasuse tuvastamise puhul meetme vajalikkust, sobivust ja proportsionaalsus kitsamas tähenduses ehk kas on vähem riivavaid meetmeid eesmärgi saavutamiseks. Proportsionaalsust mõjutab ka seadme tehniline võimekus, näiteks korrakaitses kasutatavate jälgimisseadmestike puhul on oluline, kas masinnägemist kasutatakse ning millisel määral. Automatiseeritud näotuvastuse kasutamine korrakaitses ja süüteomenetluses andmesubjekti nõusolekuta võib olla õigustatud tungiva vajaduse puhul, näiteks terrorirünnaku või raske kuritöö riski puhul. Alaealiste peal ei ole näotuvastuse kasutamine lubatud. Kuna automatiseeritud näotuvastustehnoloogia kasutamine ilma andmesubjekti nõusolekuta on tugev põhiõiguste riive tuleb hinnata, kas arvestades riive intensiivsust on see seaduses piisava üksikasjalikkusega kirjas, et see oleks inimestele ettenähtav ning inimesed saaksid selle kohaselt oma käitumist reguleerida.

[302] Ethical Issues Arising From The Police Use of Live Facial Recognition Technology. Raport. – Biometrics and Forensics Ethics Group Facial Recognition Working Group, 02.2019.

[303] Vt lisa 2.

KOKKUVÕTE

Magistritöö eesmärk oli välja selgitada, kas masinõppe tehnoloogiate leviku valguses on EL andmekaitse regulatsioonis vajalik gruppide tõhusam kaitse võrreldes praegusega; kas andmekaitse üldmäärus laieneb emotsioonituvastusele, kui isikut ei tuvastata; milliseid andmekaitsenõudeid tuleb järgida masinnägemise võimekusega jälgimisseadmestike kasutamisel ja automatiseeritud isikusamasuse tuvastamisel Eesti korrakaitses ja süüteomenetluses ning tuvastada võimalikud probleemid korrakaitses jälgimisseadmestike kasutusel andmekaitsenõuete täitmisega.

Magistritöös leiti, et masinõppe algoritmid on peamiselt suunatud grupitunnuse põhjal töötlemisele, algoritmilised grupid on muutlikud ning inimesed ei pruugi teada, et nad sinna sattunud on. Seetõttu on keerukas täita n-ö ohvri kriteeriumit ja konkreetse andmesubjektile tehtud kahju kindlaks teha. Gruppide paremaks kaitseks võiks olla siseriiklikult võimalus organisatsioonidel, kellel on põhikirjaga võetud eesmärk tegeleda põhiõiguste kaitsega, minna isikuandmete kaitse õiguse või privaatsusõiguse kaitseks kohtusse ka siis, kui ohvrit või konkreetset kahju pole võimalik tuvastada. Hetkel on selle võimaluse loomine liikmesriigile vabatahtlik. Gruppide privaatsust võib aidata edendada ka uute tehnoloogiliste võimaluste kasutamine, näiteks automaatne kontroll, kas andmekaitsetingimused vastavad EL õigusele. Ex ante järelduste mõistlikkuse põhjendamise kohustuse tunnustamine EK poolt ja selle sisse viimine üldmäärusesse aitaks tagada seda, et andmetöötlusel tehtud otsused on mõistlikud ning usaldusväärsed – see õigus aitaks andmesubjekte ebamõistlike järelduste vaidlustamisel nagu näiteks laenuotsuse puhul, mis tehti vaid isiku Facebooki konto baasil.

Magistritöö esimene hüpotees leidis osaliselt kinnitust. Emotsioonituvastus võib olla nii üldmääruse kohaldamisalas, direktiivi kohaldamisalas, väljaspool kohaldamisala ning nii privaatsusõigust riivav kui ka mitte riivav – see sõltub konkreetsest emotsioonituvastusest. Küsimuses, kas emotsioonituvastuse puhul töödeldakse isikuandmeid ning kas emotsioonituvastusele tuleb kohaldada üldmäärust, on võtmeroll tuvastatavusel ning emotsioonituvastuse eesmärgi hindamisel.

Isikuandmed on sh igasugused andmed, mille puhul inimene on mõistliku tõenäosusega kaudselt tuvastatav võttes seejuures arvesse töötlemise eesmärki, tehnoloogiat, kulukust jne. Kui andmete kombineerimisel muu või muude andmebaasidega on isik tuvastatav (nt

pseudonümiseeritud andmete puhul), on tegu isikuandmetega. Tuvastatavuse kindlakstegemisel tuleb arvesse võtta kõiki vahendeid, mida vastutav töötleja või keegi muu võib füüsilise isiku otseseks või kaudseks tuvastamiseks mõistliku tõenäosusega kasutada, näiteks teiste hulgast esiletoomine. Seejuures tuleb arvesse võtta kõiki objektiivseid tegureid, sh tuvastamise maksumus, tuvastamiseks kuluv aeg, andmesubjekti huvi, tehniliste turvameetmete tase ning millistel eesmärkidel tehnoloogiat kasutatakse.

Otsustamisel, kas tegu on anonüümsete andmetega, mängib rolli töötlemise eesmärk. Kui andmetöötluse eesmärgist tulenevalt või selle täitmise jaoks on vajalik isikute tuvastamine ja nende teatud viisil kohtlemine, võib eeldada, et on täidetud mõistlik tõenäosus isiku tuvastatavuseks, töödeldavad andmed on seotud tuvastatava isikuga ning sellisele andmetöötlusele peab kohaldama andmekaitsereegleid. Kui töötlemise eesmärk ei ole isiku tuvastamine ja nende teatud viisil kohtlemine, võib sõltuda andmete suhtes rakendatud tehnoloogilistest turvameetmetest, kas tegu on isikuandmetega, kuna need turvameetmed on üks kriteerium hindamaks, kas on olemas mõistlik tõenäosus isikute tuvastamiseks. Emotsioonituvastus ei ole üldmääruse ega direktiiviga hõlmatud juhul, kui töödeldakse ainult tõeliselt anonüümseid andmeid, mille põhjal isiku tuvastamine on võimatu või on tuvastamine väga ebatõenäoline arvestades kõiki objektiivseid tegureid. Andmekaitse regulatsiooni kohaldumiseks on piisav, kui tunnuste põhjal kedagi teiste hulgast esile tuuakse ning tuvastatakse selle isiku käitumine või isiksuse omadused, et tema suhtes teatud otsuseid rakendada. Videovalve, millele on lisaks rakendatud emotsioonituvastuse võimalus, on hõlmatud isikuandmete kaitse regulatsiooniga. Kui emotsioonituvastuskaamera on näiteks tänaval eesmärgiga möödamineja emotsiooni tuvastada ning vastavalt sellele tema suhtes reklaami muuta eesmärgiga emotsioonide subjekti mõjutada, tuleks lugeda sellist emotsioonituvastust isikuandmete töötlemiseks, millele rakenduvad isikuandmete kaitse üldmääruse nõuded.

Erandit „ilmselgelt avalikustanud andmed“ tuleb tõlgendada rangelt ning sellele tuginemiseks peab andmesubjekt eesmärgistatult ja tahtlikult tegema oma andmed avalikuks. Avalikku kohta paigutatud kaamerapilti jäämine ei ole selle erandiga kaetud.

Kui konkreetsele emotsioonituvastusele rakendub üldmäärus, tuleb hinnata ka seda, kas emotsioonituvastus omab märkimisväärset mõju. Kui emotsioonituvastusel on märkimisväärne mõju, on selline emotsioonituvasus üldjuhul keelatud, välja arvatud siis, kui täidetud on erand, näiteks selgesõnaline nõusolek. Märkimisväärse mõju olemasolul tuleks emotsioonituvastuse kasutamisel esitada andmesubjektile ka teave kasutatava loogika ja selle kohta, millised on sellise töötlemise tähtsus ja prognoositavad tagajärjed andmesubjekti jaoks.

Grupiprivaatsuse alast kirjandust analüüsidest leiti kohati üldmääruse ja direktiivi materiaalse kohaldumisala kitsendavat tõlgendamist, mida tuleks vältida. Üldmääruse kohaldamiseks ei ole vaja tuvastatavuse kõrget taset. See et isikuandmeid töödeldakse grupitunnuse põhjal, ei pruugi tähendada, et tegevus on väljaspool üldmääruse ja direktiivi kohaldamisala, eriti, kui töötlemine mõjutab konkreetseid isikuid (nt sõnumite saatmine, sotsiaalmeedias postituste sihtimine konkreetsetele inimestele grupitunnuse põhjal). Samuti leiti magistritöös, et isegi kui isikud ei ole tuvastatavad ning seetõttu andmekaitse regulatsioon ei kohaldu, võib tegu olla privaatsusõiguse riivega EIÕK artikkel 8 ja harta artikkel 7 mõttes, kuna mõjutatakse inimese autonoomsust (nt linnas valguse ja lõhnadega mõjutamine). Inimeste liikumise kaardistamise ja selle põhjal neid mõjutavate otsuste tegemise puhul on töötlemine EL andmekaitseregulatsiooni kohaldamisalas. Seetõttu, et emotsioonituvastus on uus tehnoloogia ning seda pole andmekaitse üldmääruses expressis verbis mainitud, ei tohi jätta sellele tehnoloogiale andmekaitsereegleid kohaldamata.

Korrakaitset ja süüteomenetlust puudutavas analüüsis tuvastati, et õiguskaitseasutuste andmekaitsedirektiivi materiaalses kohaldamisalas on nii riiklik järelevalvemenetlus kui ka süüteomenetlus, kuni tegevus on EL õiguse kohaldamisalas, mistõttu teine hüpotees osutus tõeseks. Õiguskaitseasutuste andmekaitsedirektiivi materiaalsele kohaldamisalale lisati 2015. aastal kolmepoolsete läbirääkimiste käigus „sealhulgas avalikku julgeolekut ähvardavate ohtude eest kaitsmiseks ja nende ennetamiseks“. Direktiivi ülevõtmisel tõlgendati direktiivi kohaldamisala aga kitsendavalt võtmata arvesse kolmepoolsetel läbirääkimistel laiendatud direktiivi kohaldamisala ega korrakaitseseadust, mille kohaselt on riikliku järelevalve meetod ka süütegude ennetamine. Direktiivi preambulis kirjeldatakse sunnimeetmete võtmist väljaspool süüteomenetlust, mis on omane korrakaitsele kui ohutõrjele ja sätestatud korrakaitseseaduses. Samuti kirjeldatakse materiaalsesse kohaldamisalasse kuuluvana ohtude teket, mis võivad viia süüteo toimepanemiseni. Selgituses pole piiritletud materiaalset kohaldamisala süüteokahtluse olemasoluga, vaid hõlmatud on ka avaliku korra säilitamine ja ohtude tekke ärahoidmine. Seega on direktiivi materiaalses kohaldamisalas ka ohutõrje iseloomuga olukorrad, kus süüteomenetlus pole alanud ja hoitakse ära ohtude teket avalikule julgeolekule ja ühiskonna põhihuvidele, mitte ainult süüteomenetlus. Direktiivi ülevõtmisel on tõlgendatud direktiivi kohaldamisala kitsendavalt ning ülevõtmisel otsustatud, et direktiiv kohaldub vaid süüteomenetlusele ning korrakaitsele kohaldub üldmäärus. Kuigi direktiivi kohaldamisala on mõistetud kitsendavalt, ei ole korrakaitse allutamine üldmäärusele, kus on rangemad isikuandmete kaitse nõuded ja vähem paindlikkust võrreldes direktiiviga, otseselt vastuolus EL õigusega, kuna lubatud on kehtestada ka direktiivis sätestatust rangemaid

nõudeid. Siiski oleks võinud olla riikliku järelevalve rangematele nõuetele allutamine teadlik otsus, mitte direktiivi kitsendava tõlgendamise tulemus.

Kummutati A. Ivanovi 2018. aastal Tallinna Tehnikaülikoolis kaitstud magistritöö järeldus, et „[j]ulgeoleku tagamine peab toimuma kooskõlas andmesubjektide põhiõiguste ja –vabaduste järgimisega ning tuginema direktiivis 2016/680 sätestatud isikuandmete töötlemise põhimõtetele." Selline järeldus on ekslik, kuna annab direktiivile palju laiema kohaldamisala, hõlmates materiaalsesse kohaldamisalasse ka riikliku julgeoleku tagamise, mis on väljaspool EL õiguse kohaldamisala. Samuti ei ole võimalik direktiivile otse tugineda, välja arvatud siis, kui direktiiv pole võetud üle õigel ajal või on võetud üle valesti, kuna direktiiv pole otsekohalduv erinevalt määrusest.

Riikliku järelevalve allutamine üldmäärusele tähendab, et korrakaitseliste meetmete puhul tuleb lähtuda isikuandmete kaitse üldmääruse nõuetest ning süütegude puhul siseriiklikust õigusest, kuhu on üle võetud direktiivi sätted. Kui tegevus on väljaspool EL õiguse kohaldamisala, näiteks riikliku julgeoleku tagamine, tuleb lähtuda siseriiklikust õigusest, EIÕK-st, muudest ratifitseeritud Euroopa Nõukogu õigusaktidest nagu konventsioon 108, ja EIK praktikast.

Magistritöö kolmas hüpotees leidis kinnitust. Põhiõigusi, sh isikuandmete kaitse õigust tohib EL õiguse kohaldamisalas piirata (1) ainult seadusega, (2) arvestades isikuandmete kaitse õiguse olemust, (3) piirang peab olema proportsionaalne ehk piiranguid tohib seada üksnes juhul, kui need on vajalikud ning vastavad tegelikult EL-i poolt tunnustatud üldist huvi pakkuvatele eesmärkidele või kui on vaja kaitsta teiste isikute õigusi ja vabadusi.

Põhjendatud peaks olema, miks on jälgimisseadmestiku kasutamine konkreetsel juhul vajalik, miks see on sobiv vahend eesmärgi saavutamiseks ja miks on see proportsionaalne saavutatava eesmärgi suhtes, st puudub vähem õigusi riivav alternatiiv. Jälgimisseadmestike kontekstis võiks kaamera paigaldamine olla vajalik näiteks kõrge õnnetuste või õigusrikkumiste arvuga alal. Proportsionaalsuse kaalumisel tuleks leida tasakaal avaliku huvi ja individuaalsete huvide ning hinnata ka kaamera asukohta sobivust ja kaamera tehnilist võimekust. Tuleks põhjendada masinnägemisega nutikamaks tehtud kaamerate vajadust, sobivust ja proportsionaalsust kitsamas tähenduses. Samuti tuleb põhjendada kaamera asukohta – miks on üldiselt turvalise ilma suuremate probleemideta avaliku asukoha ööpäevringne reaalajas jälgimine.

Valvekaamerate kasutamine ei ole õigustatud vähese tähtsusega õigusrikkumiste tuvastamiseks. Ühetaolist ja üldist lähenemist tuleb vältida ning valida ja paigaldada kaamerad vastuseks konkreetsele ja reaalsele turvariskile. Ainult inimese grupilise kuuluvuse põhjal, nt osalemise tõttu kogunemisel või üritusel, ei tohiks tema isikuandmeid koguda.

Kuna kaamerate avalikesse kohtadesse lisamine ja väärteo tunnuste tuvastamine on võimalik masinnägemisel abil muuta efektiivsemaks, on oluline pidada kinni eesmärgi piirangu põhimõttest ning seada masinnägemise eesmärgiks tuvastada vaid sellised objektid, isikud või olukorrad, mis on eesmärgi saavutamiseks vajalikud.

Kuna korrakaitse eesmärgil töötlemine on allutatud isikuandmete kaitse üldmäärusele, tuleb korrakaitses jälgimisseadmestike kasutamise puhul täita üldmääruse nõudeid, sh läbipaistvuse nõuet. Läbipaistvuse nõude kohaselt tuleb inimesele, kui temalt andmeid kogutakse, anda andmetöötleja ja andmetöötluse kohta teavet. Olulisim andmekaitsetingimustest teavitamise puhul on see, et teave oleks kergesti arusaadav ja lihtsasti kättesaadav. Kui inimene ei tea, kelle jälgimisseadmestikuga tegu on, ega pole kirjas ka, kust leida sellekohast infot, ei saa pidada andmekaitsetingimustest teavitamist kergesti arusaadavaks ja lihtsasti kättesaadavaks. Muuhulgas peaks olema avalik informatsioon jälgimisseadmestiku tehnilise funktsionaalsuse kohta, sh kas kasutatakse masinnägemist, kuidas ning millises ulatuses seda tehakse. Seda informatsiooni teadmata on andmesubjektil keeruline hinnata oma õiguste riivet.

Andmete säilitamise aeg peaks olema piiratud rangelt minimaalsega. Eesti õiguse kohaselt peab videosalvestist säilitama vähemalt üks kuu, kuid mitte kauem kui aasta, välja arvatud siis, kui seadusega on sätestatud teisiti. On vaieldav, kas aasta aega video säilitamist on siiski rangelt minimaalne vajalik aeg.

Magistritöös tuvastati jälgimisseadmestike kasutamisel Eesti korrakaitses mitmeid andmekaitsega seonduvaid probleeme. Vältida tuleks jälgimisseadmestike osas ühetaolist lähenemist. Ekslik on seisukoht nagu ei sõltuks jälgimisseadmestike eri seadmetest, nende asukohtadest, kasutusviisidest ja tehnoloogiast jälgimisseadmestiku kasutuse õigustatus. Osadel jälgimisseadmestike paigaldamise juhtudel on kaheldav, kas jälgimisseadmestiku paigaldamine on vajalik ja proportsionaalne meede saavutatava eesmärgi suhtes. Probleeme tuvastati ka läbipaistvuse, andmete säilitamise pikkuse ja konfidentsiaalsusega, kuna isikuandmetele on juurde pääsenud kõrvalised isikud.

Avalike alade ulatusliku süstemaatilise jälgimise puhul tuleb läbi viia ex ante andmekaitsealane mõjuhinnang. Samuti tuleb mõjuhinnang läbi viia, kui hakatakse asukohta jälgima reaalajas. Kui ole kindel, kas innovatiivse tehnilise lahenduse jaoks on vajalik mõjuhinnangu läbiviimine, tuleks seda teha.

Isikusamasuse tuvastamine erilise meetmega kasutades näotuvastust hõlmab biomeetriliste andmete töötlemist. Biomeetriliste andmete töötlemine ei hõlma igasugust fotode või video töötlemist, vaid konkreetse tehnilise vahendiga töötlemist, mis võimaldab isiku kordumatut

tuvastamist või autentimist. Oluline on, milline on tehnoloogia tehniline võimekus ja mida sellega tehakse. Kui kaamera tehniline võimekus on selline, et tuvastatakse biomeetrilisi andmeid, näiteks tuvastatakse videol olev näokujutis, võimaldab kaamera tehniline tase isiku kordumatut tuvastamist ning töödeldakse seega biomeetrilisi andmeid, mis on eriliigilised isikuandmed. Kaamerate tehnilise võimekuse tõstmisel muutub isikuandmete kaitse õiguse riive ulatus, mis mõjutab omakorda töötlemise proportsionaalsust. Seetõttu tuleb kaamera (või muu sensori) tehnilisele tasemele tähelepanu pöörata, kui hinnatakse seda, kas kaamera kasutamine vastab andmekaitsereeglitele.

Korrakaitseliste meetmete puhul, kus töödeldakse biomeetrilisi andmeid, näiteks näotuvastust võimaldavate avalikesse kohtadesse paigutatud kaamerate puhul, peab töötlemine olema vajalik olulise avaliku huviga seotud põhjustel liidu või liikmesriigi õiguse alusel ning olema proportsionaalne saavutatava eesmärgiga, austama isikuandmete kaitse õiguse olemust ja tagatud peavad olema sobivad ja konkreetsed meetmed andmesubjekti põhiõiguste ja huvide kaitseks. Need tingimused peavad olema täidetud kumulatiivselt.

Süüteomenetluses eriliigiliste isikuandmete töötlemise üldist keeldu ei ole. Direktiivi on kohaselt on eriliigilist andmete töötlemine lubatud üksnes siis, kui see on rangelt vajalik, sellele kohaldatakse andmesubjekti õiguste ja vabaduste kaitsmiseks asjakohaseid kaitsemeetmeid ning üksnes järgmistel juhtudel: see on lubatud liidu või liikmesriigi õigusega või et kaitsta andmesubjekti või teise füüsilise isiku elulisi huve või selliselt töödeldakse isikuandmeid, mille andmesubjekt on ilmselgelt avalikustanud. Tegemist on alternatiivsete alustega.

Kuna masinnägemise abil isikusamasuse tuvastamine on isikuandmete kaitse õigust tugevalt riivav, peab selle kasutamine olema õigustatud ning läbi tuleb viia ex ante hinnang, kas selle rakendamise tingimused on täidetud. Proportsionaalsuse hindamisel tuleb arvesse võtta kaamera tehnilist võimekust ja funktsionaalsust, kuna see mõjutab oluliselt isikandmete kaitse riivet.

Mida intensiivsem on isikute põhiõiguste piiramine, seda üksikasjalikumalt peab see olema sätestatud seaduses. Seaduse detailsuse nõutav aste sõltub konkreetsest meetmest, valdkonnast ja adressaatide arvust. Seaduslikkus on seotud laiemalt ka sellega, kas riive on demokraatlikus riigis vajalik, mis tähendab, et sekkuv meede peab vastama “tungivale sotsiaalsele vajadusele” ja olema „proportsionaalne võrreldes taotletava õiguspärase eesmärgiga”. Arvestades masinnägemise abil isikutuvastuse kasutamisel isikuandmete kaitse riive intensiivsust, peaks olema selle tehnoloogia kasutamise tingimused ja tehnilised nõuded täpsemalt sätestatud. Selles

küsimuses tasub vaadata teiste riikide kogemust – näites Ühendkuningriikides on näotuvastuse kasutuse kohta eraldi eelnõu ning koostatud ka eetiliste printsiipide juhend.

PRIVACY AND DATA PROTECTION REGARDING COMPUTER VISION AND MACHINE LEARNING IN EU LAW BASED ON EMOTION TRACKING AND ESTONIAN LAW ENFORCEMENT USE OF MONITORING EQUIPMENT

Abstract

New technologies, particularly artificial intelligence and its' subfields computer vision and machine learning, are transforming the way data is made, collected and used and thus pose challenges for the protection of the right to privacy and the right to data protection enshrined respectively in articles 7 and 8 of the Charter of Fundamental Rights of the European Union (hereinafter: Charter) and in article 8 of the European Convention on Human Rights (hereinafter: ECHR). With the spread of IoT, the world is becoming more connected and machine learning algorithms are becoming increasingly sophisticated at detecting patterns in humans' psychology.

More data is being made during casual use of technology. Data is being acquired increasingly without the deliberate involvement of a person. Decisions regarding privacy are increasingly being made serving the interests of surveillance capitalism. As the goal of surveillance capitalism is to affect the decisions of people with the help of data, surveillance capitalism poses a risk for the autonomy of people. This is not only an issue on the individual level but also on the societal and political level as privacy and autonomy are needed for the functioning of democracy.

In 2016 EU adopted the data protection package with the aim to straighten and renew the data protection regulation for the digital age. The regulation consisting of the GDPR (2016/679) as *lex generalis* and the law enforcement data protection directive (2016/680) as *lex specialis* (hereinafter together referred to as the data protection regulation or regulation) set principles for data protection that are in theory technology neutral and independent of techniques used.

The aims of this thesis were (1) to determine whether it is needed to further strengthen group privacy in the light of the developments and spread of machine learning; (2) to determine whether emotion detection is covered by the GDPR and what are the alternatives for regulating emotion detection and (3) which data protection rules are to be followed in the case of monitoring equipment enhanced with computer vision and machine learning in Estonian law

enforcement and offence procedure and to determine possible infringements of EU-s data protection rules.

The state of art of technology enables to gather information about people themselves, their behaviour and their habits in a way that data is anonymous but says much about groups of people which enables the profiling of people. The impact of new data analytics' techniques has so far been mostly addressed on the individual level although profiling and machine learning are mostly directed at groups. Much of the attention has been on the anonymization of data and the protection of the identity of a person. Groups have only been thought of as a collective.

The data subjects have the right to mandate a not-for-profit body, organisation or association which has been properly constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest, and is active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data to lodge the complaint on his or her behalf. Member States may provide that anybody, organisation or association independently of a data subject's mandate, has the right to lodge, in that Member State, a complaint with the supervisory authority if it considers that the rights of a data subject under GDPR have been infringed as a result of the processing. With new technologies satisfying the victim requirement and determining damages proves to be difficult. Applying this provision in member states could further strengthen the protection of group privacy.

Data protection regulates so-called input data, but not output data. Creating a right to reasonable inferences and a greater focus on what is done with data can be a solution to a number of emotion detection and facial recognition problems, because they are not based on one technology, but address all such data analysis technologies that target the group level.

The EU data protection regulation is based on the protection of identifiable persons and their data. Data which does not enable the direct or indirect identification of a person is outside the scope of the regulation. The regulation does not prohibit the collection of demographic data e.g. age, gender and race if the data gathered about a group and is abstract enough as to not enable identification or singling out of a person. This kind of technology may thus be used without asking the data subjects' consent or following other rules set out in the regulation.

Personal data is all data that may enable the direct or indirect identification of a natural person. To determine this, account should be taken of all the means reasonably likely to be used. The cost, time and the sophistication of technology and security measures and possible likability with other data should be taken into account.

The first hypothesis of the thesis proved to be partly true. Emotion recognition may be subject to the data protetion regulation or not and may infringe the right to privacy depending on circumstances and the technology used. Where identification of persons and their treatment in a particular way is necessary for the purpose of the processing or for its execution, it can be assumed that a reasonable likelihood of identification is fulfilled, the data processed are related to the identifiable person and such data processing is subject to data protection rules. Therefore, in the cases where the purpose of the processing is to identify and treat people in a certain way, data protection rules should apply even if processing is based on a group identifier.

Location data is considered personal data thus the tracking of people's movements and making the decisions that affect them based on that information is within the scope of the EU data protection regulation. The application of data protection regulation does not require a high level of identifiability. In determining whether the data is anonymized, the purpose of the processing should also be taken into account. In advertising for example, if the emotional information is used to target or influence the data subject, then the rules on the protection of personal data should apply to such processing.

The assessment of identifiability depends on the particular situation. For the purposes of identifiability, account must be taken of all means that the controller or anyone else can use with reasonable probability for the direct or indirect identification of a natural person, such as singling out. In order to assess the reasonable likelihood of identifiability, account must be taken of all objective factors, including but not limited to the cost of identification, the time required for identification, the interest of the data subject, the level of technical security measures and the purposes for which the technology is used.

In deciding whether the data is truly anonymous, the purpose of processing should be considered. Where identification of persons and their treatment in a particular way is necessary for the purpose of the processing or for its execution, it can be assumed that a reasonable likelihood of identification is fulfilled and the data processed are related to an identifiable person. Thus such data processing must be subject to data protection rules. If the purpose of the processing is not to identify the person nor to treat them in a certain way, it may depend on the technological security measures applied to the data, whether it is personal data, as the technical measures are one of the criteria for assessing whether there is a reasonable likelihood of identifying individuals.

The processing of emotional data is outside of the scope of the regulation if the data is truly anonymous in the sense that it is impossible or very unlikely to identify a person with all

objective factors considered. The purpose of the processing is an important factor in the assessment of identifiability in cases where it is not clear whether that data is anonymous. For example, if an emotion recognition camera placed on the street for the purpose of detecting emotion and the gathered information is used for personalized advertising with the aim of influencing the subject of emotions, then such processing should be subject to the requirements of the GDPR.

For the applicability of the GDPR it is sufficient if, from a set of characteristics, an individual is singled out and the person's behaviour or personality characteristics are identified in order to apply certain decisions to him.

In case of video surveillance personal data is being processed, even when some people on the video are not practically identifiable. Video surveillance, enhanced with emotion detection, is thus covered by the protection of personal data.

Although it is technically possible to identify and monitor emotions in a way that does not allow the identification of a natural person or confirmation of the identity of a natural person on the basis of the data collected, the technical level does not automatically mean that the data is anonymous, but all other objective factors must also be assessed to find out whether the person might be identifiable.

Emotion detection is a form of automated processing with the goal to evaluate personal aspects of a physical person. Emotions are undoubtedly personal. If the purpose of emotion recognition is not the identification of a person and if the person is not directly or indirectly identifiable, by evaluating all objective factors and a reasonable likelihood of identifiability, the data should be regarded as anonymized data and not covered by the GDPR.

It is not necessary to ask for the consent of the data subject for the processing of personal data when processing personal data which the data subject has manifestly made public – this exception must be interpreted strictly and applied only when the data subject has deliberately made his or her data public. Being recorded by surveillance camera or “sensed” in a public place is not covered by this exception.

When GDPR is applied to a particular emotion recognition, it must also be assessed whether the emotion recognition has legal effects concerning data subjects or similarly significantly affects them. If the emotion recognition falls within the scope of the GDPR but does not have a significant impact, the principles of data processing must be respected and the data subjects must be guaranteed the rights set out in the GDPR. The existence of significant impact must be

assessed based on the specificities of the case, including, the intrusive nature of the profile analysis process, the expectations and wishes of the individuals concerned; the use of advertising or the use of information on vulnerable data subjects. Processing, which has a generally minor impact, can significantly affect vulnerable social groups such as minority groups. Thus, in the case of emotion recognition, a specific situation needs to be looked at to assess whether the emotion recognition has a significant effect. If emotions are used to make price differences for individuals or to affect vulnerable groups, it must be concluded that significant effect exists. If emotion recognition has a significant effect, such emotional recognition is generally prohibited, except when an exception, such as explicit consent, is met. If there is significant impact, the data subject should also be provided with meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

The first hypothesis of the Master's thesis proved to be partly true. Even if a certain emotion recognition is not covered by the EU regulation on the protection of personal data, emotion recognition may still be an infringement of the physical and psychological autonomy of a person within the meaning of Article 8 of the ECHR and Article 7 of the Charter.

There are various alternatives for further regulation of emotion recognition, e.g. the addition of emotional information as a separate data type, or stronger group-based privacy protection. In the current legal framework, it is important to note that the material scope of the GDPR and the directive should not be subject to arbitrary restrictions.

It was found that the understanding of the concept of identifiability is often too restricted. The GDPR and the directive do not require a high probability of identifiability. It is enough if there is a reasonable chance that a data subject might be indirectly identified. Only anonymized data is outside the material scope of the GDPR and the directive. In other cases, like pseudonymized data, it must be concluded that the data processing falls under the scope of the GDPR and the directive.

If the objective of emotion recognition involves identifying and influencing individuals, then such emotional recognition should be covered by the regulation, i.e. the GDPR or the law enforcement directive. Emotion recognition should not be left without scrutiny and outside the regulation only for the reason that it is a new technology and has not been explicitly mentioned in the regulation.

In Estonia, computer vision has so far been met with favourable attitude considering that the state strategy documents envisage the introduction of new technologies in the fields of law

enforcement and public security and introducing new ways for biometric recognition, including facial recognition, and making it possible for third parties to access the state's biometric database for identification purposes. According to a survey, the Estonian people consider cameras most important method in ensuring public security. Police and Border Guard Board uses monitoring equipment, including surveillance cameras and drones, and body cameras to ensure more efficient public order and offence procedure. The state encourages the installation of surveillance cameras and many new cameras are planned to be installed in the near future.

The second hypothesis of the Master's thesis proved to be true. The material scope of the law enforcement data protection directive was expanded in 2015 during trialogues - "or the safeguarding against and the prevention of threats to public security" was added to the material scope of the directive. However, when adopting the directive into Estonian law, the scope of the directive was interpreted restrictively without taking into account the extended scope of the directive in trialogues nor the § 5(7) of the Law Enforcement Act, according to which the prevention of offences a part of law enforcement.

In the preamble of the Directive it is explained that methods of state supervision such as coercive measures taken outside the offense procedure are to be included in the scope of the directive. Likewise, the material scope of the Directive includes the occurrence of threats that may lead to an offense similar to the provisions of § 5(1-2) of the Law Enforcement Act. The explanation does not limit the material scope to the presumption of suspicion, but also covers the maintenance of public order and the prevention of threats. Thus, in the material scope of the Directive, there are situations of a state supervision character, where the offense procedure has not started but the emergence of threats to public security and to the fundamental interests of society have to be avoided. Thus state supervision in the meaning of Estonian Law Enforcement Act is within the scope of the Directive.

However, in transposing the Directive, the scope of the Directive was interpreted restrictively and thus it was decided that the Directive applies only to the offense procedure and the GDPR applies to state supervision, i.e. law enforcement. Although the Directive was narrowly interpreted and thus law enforcement is in Estonia subject to the GDPR that has less flexibility compared to the Directive, the Directive allows adopting stricter requirements than those laid down in the Directive. However, it should have been an informed decision, rather than a restrictive interpretation of the Directive, to subject state supervision to stricter data protection requirements.

The decision to subject state supervision to the GDPR means that law enforcement measures must follow the requirements of the GDPR and, in the case of offense procedure, the national law to which the Directive was transposed to - in particular Chapter 4 of the Personal Data Protection Act. If the activities are outside the scope of EU law, such as activities ensuring state security, then national law, the ECHR, other ratified Council of Europe acts such as Convention 108 and the ECtHR case law must be followed.

The third hypothesis proved to be true. The use of monitoring equipment in Estonian law enforcement must be necessary and proportionate, and the proportionality is affected by the location of the monitoring equipment and the technical capability of the device.

Any limitation on the exercise of the right to data protection within the scope of EU law must follow the criteria set out in Article 52(1) of the Charter: (1) the limitation must be provided for by law, (2) respect the essence of data protection, (3) the limitation must be proportionate, which means that the limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others. The principle of proportionality is also laid down in § 7 of the Law Enforcement Act.

It should be justified why the use of monitoring equipment in a particular case is necessary, why it is a suitable means of achieving the objective and why it is proportionate to the objective to be achieved, i.e. there is no less restrictive alternative. In the context of monitoring equipment, installing a camera could be necessary, for example, in an area with a high number of accidents or offenses. When considering proportionality, a balance should be struck between the public interest and the individual interests. The camera's location and the camera's technical capability should also be assessed.

Since the inclusion of cameras in public places and the identification of misdemeanors can be made more efficient by computer vision, it is important to adhere to the principle of purpose limitation and to keep the purpose of identifying the objects, persons or situations to those which are necessary to achieve the legitimate aim.

If the use of surveillance camera is justified on the grounds of protecting the public against serious crime, then the surveillance cameras should not be used for the detection of minor offenses. A uniform and general approach to monitoring equipment should be avoided and the cameras should be selected and installed in response to a specific and real security risk. Personal data should not be collected only on the basis of a person's group membership, e.g. because of participation in a meeting or event.

As law enforcement processing in Estonia is subject to the GDPR. The requirements of the GDPR, including the transparency requirement, must be met when using monitoring equipment. According to the requirement of transparency, information about the data controller and the data processing must be provided to the individual when the data is collected. The information must be easily understandable and easily accessible. If a person does not know who the controller of the monitoring equipment is, or there is no reference where to find to information about it, then information cannot be easily understood and easily accessed. Among other things, there should be public information on the technical functionality of the monitoring equipment, including if computer vision is used, how and to what extent. Without knowing this information, it is difficult for the data subject to assess the possible infringement of her rights.

The data retention period should be limited to strict minimum. The retention restriction is set out in § 34 (2) of the Law Enforcement Act, which provides that video recordings shall be kept for at least one month, but not longer than one year, unless otherwise provided by law. It is debatable whether a limit of one year is a strictly minimum time considering for example that in Ireland the limit is one month – that is 12 times less.

It was found that the requirement for confidentiality of personal data has been violated in the case of Estonian law enforcement use of monitoring equipment, as unauthorized persons have had access to personal data.

It was found that cameras may have been installed in places where it is not necessary e.g. 7 law enforcement surveillance cameras with real time surveillance 24/7 are installed in Taikse village with 175 habitants where life is “generally calm”.

In the case of extensive systematic monitoring of public areas, an ex ante data protection impact assessment pursuant to Article 35 (3) (c) of the GDPR must be carried out. The impact assessment should also be carried out in the case of real-time monitoring of the location and adoption of new technologies (e.g drones). If it is not clear whether an impact assessment is required for an innovative technical solution, it should be done rather than avoided.

The processing of biometric data does not include all processing of photographs or video, but only processing by specific technical means that allows the individual to be identified or authenticated. The increase in the technical capability of the cameras may alter the scope of the infringement of the right to the protection of personal data, which in turn affects the proportionality of processing. Therefore, attention should be paid to the technical level of the camera (or other sensor) when assessing whether the use of the camera is in accordance with

data protection rules. Identification through a special measure within the meaning of the Law Enforcement Act involves the processing of biometric data.

Processing of biometric data is generally prohibited under GDPR. Article 9 (2) (g) of GDPR provides for an exception and it is the appropriate basis in the context of law enforcement use of facial recognition cameras, which provides for an exemption where processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject. These conditions must be met cumulatively.

There is no general prohibition on processing different types of personal data in an offense procedure. Processing of biometric data in offense procedures is allowed only where strictly necessary, subject to appropriate safeguards for the rights and freedoms of the data subject, and only where authorized by Union or Member State law or to protect the vital interests of the data subject or of another natural person.

Since identification by computer vision without the data subject's consent is a serious infringement of the right to the protection of personal data, its use must be justified and an ex ante evaluation must be carried out to determine whether the conditions for its implementation are met. When assessing proportionality, the technical capability and functionality of the camera must be taken into account, as that significantly affects the protection of personal data.

The more severe the limitation of the fundamental rights of individuals, the more detailed it must be provided for by law. The degree of detail required depends on the specific measure, area and number of people affected. Lawfulness of the limitation is related to whether a violation is necessary in a democratic society, which means that an intervening measure must meet a pressing social need and be proportionate to the legitimate aim pursued. Given the intensity of the limitation of the right to data protection in using facial recognition cameras, the conditions and technical requirements for the use of this technology should be specified. In this regard, it is worth looking at the experience of other countries - for example in the United Kingdom there is a draft law on the use of facial recognition and a guideline to ethical principles of facial recognition technology used in law enforcement.

KASUTATUD ALLIKATE LOETELU

Teaduskirjandus

1. **Akinnuwesi, B., Agagu, T. T**. Automated Students' Attendance Taking in Tertiary Institution Using Facial Recognition Algorithm. – Journal of Computer Science and Its Application 2012/19, No 2.
2. **Bakir, V**. Veillant Panoptic Assemblage: Mutual Watching and Resistance to Mass Surveillance after Snowden. – Media and Communication 2015/3, No 3.
3. **Barocas, S., Nissenbaum, H**. Big Data's End Run around Anonymity and Consent. Cambridge: Cambridge University Press, 2014.
4. **Binns, R**. Data Protection Impact Assessments: a Meta-Regulatory Approach. – International Data Privacy Law 2017/7, No 1.
5. **Brayne, S**. Big Data Surveillance: The Case of Policing. – American Sociological Review, 2017/82, No 5.
6. **Brey, P**. Ethical Aspects of Facial Recognition Systems in Public Places. – Journal of Information, Communication and Ethics in Society 2004/2, No 2.
7. **Chandra, B, Sharma, R. K**. Fast learning in Deep Neural Networks. – Neurocomputing, 2016/171.
8. **Cohen, J. E**. Examined Lives: Informational Privacy and the Subject as Object. – Stanford Law Review 2000/52.
9. **Coseraru, R**. Facial Recognition Systems and their Data Protection Risks Under the GDPR. Magistritöö. Tilburg: Tilburg University, 2017.
10. **Custers, B.** jt. EU Personal Data Protection in Policy and Practice. – Information Technology and Law Series, 2019/29.
11. **Docksey, C**. Four Fundamental Rights: Finding the Balance. – International Data Privacy Law, 2016/6, No 3.
12. **Edwards, L., Veale, M**. Enslaving the Algorithm: From a 'Right to an Explanation' to a 'Right to Better Decisions'? – IEEE Security & Privacy, 2018/16, No 3.
13. **Eljas, C.** jt. Järelevalve- ja süüteomenetluse piiritlemine. Sisekaitseakadeemia, 2018.
14. **Ezeoke, S. E**. Näo emotsiooni ja soo tuvastus kasutades konvulutsioonilisi närvivõrke. Magistritöö. Tallinn: TTÜ, 2018.
15. **Gellman, R**. Privacy and Biometric ID Systems: An Approach Using Fair Information Practices for Developing Countries. Washington DC: Center for Global Development, 2013/28.
16. **Greenleaf, G**. 'Modernised' Data Protection Convention 108 and the GDPR. Sidney: UNSW Law, 2018.
17. **Greenwood, D.** jt. The New Deal on Data: A Framework for Institutional Controls. – Cambridge: Cambridge University Press, 2014.

18. **Grout, V**. No More Privacy Any More? – Information, 2019/10, No 1.

19. **Guaragnella, C., D'Orazio, T**. A Survey of Automatic Event Detection in Multi-Camera Third Generation Surveillance Systems. – International Journal of Pattern Recofnition and Artificial Intelligence, 2014/29, No 1.

20. **Güven, K.** Facial Recognition Technology: Lawfulness of Processing under the GDPR in Employment, Digital Signage and Retail Context. Magistritöö. Tilburg: Tilburg University 2019.

21. **Hildebrandt, M., Koops, B.J**. The Challenges of Ambient Law and Legal Protection in the Profiling Era. – The Modern Law Review, 2010/73, No 3.

22. **Idrees, H.** jt. Enhancing Camera Surveillance Using Computer Vision: a Research Note. – Policing: An International Journal of Police Strategies & Management 2018/41, No 2.

23. **Ivanov, A**. Füüsilise isiku kui andmesubjekti osaluse suurendamine isikuandmete kogumise ja töötlemise protsessis. Magistritöö. Tallinn: TTÜ, 2018.

24. **Jasserand, C**. Subsequent Use of GDPR Data for a Law Enforcement Purpose: The Forgotten Principle of Purpose Limitation? – University of Groningen Faculty of Law Research Paper Series, 2018/26.

25. **Kaltheuner, F., Bietti, E**. Data is Power: Towards Additional Guidance on Profiling and Automated Decision-Making in the GDPR. – Journal of Information Rights, Policy and Practice, 2018/2, No 2.

26. **Kammourieh, L.** jt. Group Privacy in the Age of Big Data. – Philosophical Studies Series, 2017/126.

27. **Kramer, A. D. I.** jt. Experimental Evidence of Massive-Scale Emotional Contagion through Social Networks. – Proceedings of the National Academy of Sciences 2014/111, No. 24.

28. **Kumaran, S. K.** jt. Anomaly Detection in Road Traffic Using Visual Surveillance: A Survey. Odisha: Indian Institute of Technology Bhubaneswar, 2019.

29. **Kärner, M.**. Mõned korrakaitseseadusega kaasnenud muudatused kriminaalmenetluses: järelevalve- ja süüteomenetluse piiritlemisprobleem. – Juridica 2014/6.

30. **Laaring, M**. Eesti korrakaitseõigus ohuennetusõigusena. Doktoritöö. Tartu: TÜ, 2015.

31. **Lewinski, P.** jt. Face and Emotion Recognition on Commercial Property under EU Data Protection. – Psychology & Marketing, Wiley Periodicals, 2016/33, No 9.

32. **Lewinski, P**. jt. Face and Emotion Recognition on Commercial Property under EU Data Protection. – Psychology & Marketing, Wiley Periodicals 2016/33, No 9.

33. **Li, S. Z.** (toim). Encyclopedia of Biometrics. – Springer, 2009.

34. **Lundevall-Unger, P., Tranvik, T**. IP Addresses – Just a Number? – International Journal of Law and Information Technology, 2010/19, No 1.

35. **Lõhmus, U**. Põhiõiguste kaitse kolmnurgas riik - Euroopa Nõukogu - Euroopa Liit. – Juridica 2010/5.

36. **Lynskey, O**. Deconstruction Data Protection: The „Added Value" of a Right to Data Protection in the EU Legal Order. – International & Comparative Law Quarterly 2014/63, No 3.

37. **Mai, J-E**. Big Data Privacy: the Datafication of Personal Information. – The Information Society, 2016/32, No 3.

38. **Marran, S-T**. Sentimentaalne analüüs eestikeelse peavoolumeedia veebiartiklite kommentaaride baasil. Bakalaureusetöö. Tartu Ülikool: Tartu 2012.

39. **Mayer-Schönberger, V., Cukier, K**. Big Data. – Boston, NY: Mariner Books, 2014.

40. **McDermott, Y**. Conceptualising the Right to Data Protection in an Era of Big Data. – Big Data & Society, 2017.

41. **McStay, A**. The Right to Privacy in the Age of Emotional AI. Bangor: Bangor University 2018.

42. **Mokrosinska, D**. Privacy and Autonomy: on Some Misconceptions Concerning the Political Dimensions of Privacy. – Law and Philosophy 2018/37.

43. **Montjoye, Y-A.** jt. Unique in the Shopping Mall: On the Reidentifiability of Credit Card Metadata. – Science, 2015/347, No 6221.

44. **Neff, G.** Why Big Data Won't Cure Us. – Big Data, 2013/1, No 3.

45. **Pajunoja, L. J**. The Data Protection Directive on Police Matters 2016/680 Protects Privacy - The Evolution of EU´s Data Protection Law and its Compatibility with the Right to Privacy. Magistritöö. Helsingi: Helsingi Ülikool, 2017.

46. **Purshouse, J., Campbell, L**. Privacy, Crime Control and Police Use of Automated Facial Recognition Technology. – Criminal Law Review 2019/3.

47. **Pärnamägi, I**. Põhiõigustesse sekkumise materiaalõiguslikud tingimused ning nende piiritlemine ohutõrjes ja süüteomenetluses. Tallinn: TTÜ, 2018.

48. **Renaud, K, Zimmermann, V**. Guidelines For Ethical Nudging in Password Authentication. – SAIEE African Research Journal 2018/109, No 2.

49. **Ridgeway, G**. Policing in the Era of Big Data. – Annual Review of Criminology, 2018/1.

50. **Rouvroy, A., Poullet, Y**. The Right to Informational Self-Determination and the Value of Self-development: Reassessing the Importance of Privacy for Democracy. Dordrecht: Springer, 2009.

51. **Sajfert, J., Quintel, T**. Data Protection Directive (EU) 2016/680 for Police and Criminal Justice Authorities. –Cole/Boehm GDPR Commentary, Edward Elgar Publishing 2019. (Käsikiri avaldamisel.)

52. **Sajjad, M.** jt. Raspberry Pi Assisted Facial Expression Recognition Framework for Smart Security in Law-Enforcement Services. – Information Sciences, 2019/479.

53. **Salignat, C.** The Impact of the Emergence of the European Union as a Human Rights Actor on the Council of Europe. – Baltic Yearbook of International Law 2014/4.

54. **Sedenberg, E., Chuang, J**. Smile for the Camera: Privacy and Policy Implications of Emotion AI Elaine Sedenberg. Berkeley: University of California, Berkeley.

55. **Sehver, K**.. Privaatsusõiguse riive proportsionaalsuse hindamise kriteeriumid Euroopa Liidu õiguses elektroonilise side andmete kaitse valdkonna näitel. Magistritöö. Tallinn: TÜ 2017.

56. **Sharma, K.** jt. A Dataset of Continuous Affect Annotations and Physiological Signals for Emotion Analysis. Tööversioon. – Arxiv 2018.

57. **Shi, J.** jt. How Effective Are Landmarks and their Geometry for Face Recognition? – Computer Vision and Image Understanding, 2006/102, No 2.
58. **Somers, M**. Emotion AI, explained. Cambridge: MIT Sloan School of Management, 2019.
59. **Soni, N**. Piiriturvalisuse tagamine elektriaia ja näotuvastuse alusel. Magistritöö. Tallinn: TTÜ, 2017.
60. **Sonka, M**. jt. Image Processing, Analysis, and Machine Vision. Boston: Springer 2008.
61. **Zuboff, S**. Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. New York: Public Affairs, 2019.
62. **Taylor, L.** jt. Conclusion: What Do We Know About Group Privacy? – Philosophical Studies Series 2017/126.
63. **Taylor, L.** jt. Group Privacy: New Challenges of Data Technologies. – Philosophical Studies Series, 2017/126.
64. **Tikk, E., Nõmper, A**. Informatsioon ja õigus. Tallinn: Juura 2007.
65. **Trzaskowski, J.** jt. Introduction to EU Internet Law. Copenhagen: Ex Tuto Publishing, 2015.
66. **Tupay, P. K**. Õigusest eraelule kuni andmekaitse üldmääruseni ehk tundmatu õigus isikuandmete kaitsele. - Juridica 2016/IV.
67. **Tänav, P**. Reaalaja sardsüsteemil põhinev objekti detekteerimis- ja jälgimissüsteem. Magistritöö. Tallinn: TTÜ, 2018.
68. **Wachter, S**. Data Protection in the Age of Big Data. – Nature Electronics, 2019/2.
69. **Wachter, S., Mittelstadt, B**. A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI. – Columbia Business Law Review, 2019. (Käsikiri avaldamisel.)
70. **Van der Sloot, B**. Editorial European Data Protection Law Review 2016_1. – European Data Protection Law Review 2016/1.
71. **Van der Sloot, B**. Legal Fundamentalism: Is Data Protection Really a Fundamental Right? – Law, Governance and Technology Series, 2017/36.
72. **Wetzling, T., Vieth, K**. Upping the Ante on Bulk Surveillance An International Compendium of Good Legal Safeguards and Oversight Innovations. – Heinrich Böll Stiftung Democracy, 2018/50.
73. **Whittaker, M.** jt. AI Now Report 2018. New York: AI Now Institute at New York University 2018.
74. **Õim, K.** Learning and Recognition of Facial Expression with Decision Trees. Magistritöö. Tallinn: TTÜ 2018.

Eesti õigusaktid

75. Eesti Vabariigi Põhiseadus - RT I, 15.05.2015, 2.
76. Erilise tuvastusmeetme kohaldamise kord - RT I, 04.06.2014, 11.
77. Isikuandmete kaitse seadus - RT I, 04.01.2019, 11.
78. Julgeolekuasutuste seadus - RT I, 13.03.2019, 67.

79. Jälgimisseadmestiku kasutamisest avalikkuse teavitamise kord. – RT I, 26.06.2014, 2.
80. Karistusseadustik - RT I, 13.03.2019, 77.
81. Korrakaitseseadus - RT I, 13.03.2019, 95.
82. Väärteomenetluse seadustik - RT I, 13.03.2019, 200.

Euroopa Liidu õigusaktid

83. Euroopa Liidu põhiõiguste harta. – ELT C 326, 26.10.2012.
84. Euroopa Parlamendi ja nõukogu direktiiv (EL) 2016/680, 27. aprill 2016. Õiguskaitseasutuste direktiivis sätestatud õigusnormid käsitlevad füüsiliste isikute kaitset isikuandmete töötlemisel pädevate asutuste poolt süütegude tõkestamiseks, uurimiseks, avastamiseks, nende eest vastutusele võtmiseks või kriminaalkaristuste täitmisele pööramiseks, sealhulgas avalikku julgeolekut ähvardavate ohtude eest kaitsmiseks ja nende ennetamiseks. – Euroopa Liidu Teataja, 27.04.2016, L 119/89.
85. Euroopa Parlamendi ja nõukogu määrus (EL) 2016/679, 27. aprill 2016, füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus). – Euroopa Liidu Teataja, 4.05.2016, L 119.

Rahvusvahelised õigusaktid

86. Inimõiguste ja põhivabaduste kaitse konventsioon. - RT II 2000, 11, 57.
87. Kodaniku- ja poliitiliste õiguste rahvusvaheline pakt - RT II 1994, 10, 11.
88. Konventsioon 108.
89. Konventsioon 108+.

Kohtupraktika

Euroopa Kohtu lahendid

90. EKo 16.11.2018, C-207/16, M*inisterio Fiscal*.
91. EKo 20.12.2017, C-434/16, *Peter Nowak v Data Protection Commissioner.*
92. EKo 21.12.2016, ühendatud kohtuasjad C-203/15 ja C-698/15, *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others.*
93. EKo 17.07.2014, ühendatud kohtuasjad C-141/12 ja C-372/12, *YS v Minister voor Immigratie, Integratie en Asiel and Minister voor Immigratie, Integratie en Asiel v M and S.*
94. EKo 6.03.2014, C-206/13, *Cruciano Siragusa v Regione Sicilia.*
95. EKo 6.03.2014, C-206/13, *Siragusa.*
96. EKo 7.05.2013, C-617/10, *Åkerberg Fransson.*
97. EKo 29.01.2013, C-396/11, *Ciprian Vasile Radu.*
98. EKo 24.04.2012, C-571/10, *Servet Kamberaj v Istituto per l'Edilizia sociale della Provincia autonoma di Bolzano (IPES) et al.*
99. EKo 15.11.2011, C-256/11, *Murat Dereci and Others v Bundesministerium für Inneres.*

100. EKo 05.10.2010, C-400/10, J. McB. v L. E.
101. EKo 29.06.2010, C-28/08 P, Commission v Bavarian Lager.
102. EKo 18.06.2008, C-1/06, Bonn Fleisch Ex- ja Import GmbH vs. Hauptzollamt *Hamburg-Jonas*.
103. EKo 07.09.2006, C-53/04, *Marrosu v Sardino.*
104. EKo 05.10.2004, C-3717/01, *Pfeiffer jt*.
105. EKo 22.10.1998, ühendatud kohtuasjad C-10/97 kuni C-22/97, *Ministero delle Finanze vs. IN.CO.GE.'90*.
106. EKo 14.12.1995, ühendatud kohtuasjad C-430/93 ja C-431/93, *Van Schijndel v Stichting Pensioenfonds voor Fysiotherapeuten.*

Euroopa Inimõiguste Kohtu lahendid

107. EIKo 24.01.2019, 43514/15, *Catt v. United Kingdom.*
108. EIKo 12.01.2016, 37138/14, *Szabó and Vissy v. Hungary.*
109. EIKo 04.12.2015, 47143/06, *Roman Zakharov v. Russia.*
110. EIKo 10.02.2009, 25198/02, *Lordachi and others v. Moldavia.*
111. EIKo 04.12.2008, ühendatud kohtuasjad 30562/04 ja 30566/04, *S. ja Maprer v the United Kingdom.*
112. EIKo 01.07.2008, 58243/00, *Liberty v. Great Britain.*
113. EIKo 06.06.2006, 62332/00, *Segerstedt-Wiberg and Others v Sweden.*
114. EIKo 19.10.2005, 32555/96, *Roche v. the United Kingdom.*
115. EIKo 30.07.2005, 45036/98, *Bosphorus vs. Iirimaa*.
116. EIKo 04.01.2005, 14462/03, *Pentiacova and Others v. Moldova.*
117. EIKo 09.03.2004, 61827/00, *Glass v. the United Kingdom.*
118. EIKo 08.07.2003, 27677/02, *Sentges v. the Netherlands.*
119. EIKo 13.02.2003, *Odièvre v. France.*
120. EIKo 28.01.2003, 44647/98, *Peck v. United Kingdom*.
121. EIKo 21.03.2002, 65653/01, *Nitecki v. Poland.*
122. EIKo 25.09.2001, 44787/98, *P.G. and J.H. v. the United Kingdom.*
123. EIKo 06.02.2001, 44599/98, *Bensaid v. the United Kingdom.*
124. EIKo 26.10.2000, 30985/96, *Hasan and Chaush v. Bulgaria*.
125. EIKo 04.05.2000, 28341/95, *Rotaru v Romania*.
126. EIKo 16.02.2000, 27798/95, *Amann v Switzerland.*
127. EIKo 16.12.1999, 24724/94, *T. v the United Kingdom.*
128. EIKo 09.06.1998, 21825/93 ja 23414/94, *McGinley and Egan v. the United Kingdom.*
129. EIKo 24.03.1988, 10465/83, *Olsson v Sweden*.
130. EIKo 02.08.1984, 8691/79, *Malone v the United Kingdom*.
131. EIKo 09.10.1979, 6289/73, *Airey v. Ireland*.
132. EIKo 06.11.1978, 5029/71, *Klass and others v. Germany.*
133. Euroopa Inimõiguste Komisjon 19.05.1976, 6959/75, *Brüggemann and Scheuten v. Germany*.

Riigikohtu lahendid

134. RKo 3-3-1-79-08.
135. RKÜKo 3-3-1-75-11.

136. RKHKo 3-3-1-41-00.
137. RKÜKo 3-3-1-41-06.
138. RKÜKo 3-4-1-10-00.
139. RKPJKa 3-4-1-3-06.
140. RKÜKo 3-4-1-19-07.

Muud allikad

141. Artificial Intelligence Deployments Have Expanded to Include 258 Unique Use Cases Across Enterprise, Consumer, and Government Markets. – Tractica, 19.12.2018.
142. Biin, S. Ringkiri jälgimisseadmestiku kasutamisest kohalikes omavalitsustes. – Andmekaitse Inspektsioon, 24.03.2016. Kättesaadav: https://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/Ringkiri_jalgimisseadmestiku_kasutamisest.pdf (10.03.2019).
143. Bowcott, O. Police Face Legal Action Over Use of Facial Recognition Cameras. – The Guardian, 14.06.2018;
144. Buckley, R. L&RS Note: Data Privacy and Community CCTV Schemes. – Oirechtas Library & Research Service, 08.01.2019.
145. Burt, C. Moscow to Expand Facial Biometrics to More of Massive Surveillance Camera Network in 2019. - Biometric Update, 19.01.2019.
146. Campbell, L. Why Regulating Facial Recognition Technology is So Problematic – and Necessary. – The Conversation, 26.11.2018.
147. Cardiff Resident Launches First UK Legal Challenge to Police Use of Facial Recognition Technology in Public Spaces. – Liberty, 13.06.2018.
148. Chinese Man Caught By Facial Recognition at Pop Concert - BBC News, 13.04.2018.
149. Code of Practice for Community Based CCTV Systems. – Department of Justice and Equality. Kättesaadav: http://www.justice.ie/en/JELR/PD_001_Code_of_Practice.pdf/Files/PD_001_Code_of_Practice.pdf (10.04.2019).
150. Convention for the Protection of Individuals with Regard to the Processing of Personal Data (CETS 108). Tabel. – Euroopa Nõukogu, 2018. Kättesaadav: https://rm.coe.int/cahdata-convention-108-table-e-april2018/16808ac958 (16.02.2019).
151. Doffman, Z. Facial Recognition Is Coming To Police Body-Worn Cameras In 2019. – Forbes, 10.01.2019.
152. Donovan, K. P., Nyst, C. Privacy for the Other 5 Billion. – Slate, 17.05.2013.
153. Draft Ethics Guidelines for Trustworthy AI. Working Document for stakeholders' consultation. Brüssel: The European Commission's AI HLEG, 2018. Kättesaadav: https://www.euractiv.com/wp-content/uploads/sites/2/2018/12/AIHLEGDraftAIEthicsGuidelinespdf.pdf (10.03.2019).
154. EK 17.07.2014, ühendatud kohtuasjad C-141/12 ja C-372/12, *YS v Minister voor Immigratie, Integratie en Asiel and Minister voor Immigratie, Integratie en Asiel v M and S*. Kohtujurist Sharpston arvamus.
155. EK 20.12.2017, C-434/16, *Peter Nowak v Data Protection Commissioner*. Kohtujurist Kokott arvamus.

156. EK 18.12.2014, C-2/13, arvamus.
157. Ethical Issues Arising From The Police Use of Live Facial Recognition Technology. Raport. – Biometrics and Forensics Ethics Group Facial Recognition Working Group, 02.2019.
158. EU Charter of Fundamental Rights: When Does It Apply and Where to Go in Case of Violation? Skeem. – Euroopa Komisjon, *sine loco*, *sine anno*. Kättesaadav: https://ec.europa.eu/info/sites/info/files/charter-application_en.pdf (04.03.2019).
159. Euroopa Liidu põhiõiguste harta kohaldamisala. Temaatiline ülevaade. – EK, 12.2017. Kättesaadav: https://curia.europa.eu/jcms/upload/docs/application/pdf/2018-05/fiche_thematique_-_charte_-_et.pdf (27.03.2019).
160. Face Off: The Lawless Growth of Facial Recognition in UK Policing. – Big Brother Watch, 10.05.2018.
161. Garcia-Garcia, J. M. jt. Emotion Detection: a Technology Review. Conference Paper. NY: ACM, 2017.
162. Global Video Surveillance Market: Focus on Ecosystem (Camera, Monitor, Storage, Software, Services), Applications, and Emerging Trends - Analysis and Forecast: 2018-2023. BIS Research 2018. Kättesaadav: https://bisresearch.com/industry-report/video-surveillance-market.html (11.03.2019).
163. Goasduff, L. Emotion AI Will Personalize Interactions. – Gartner, 22.01.2018.
164. Goel, V. 'Big Brother' in India Requires Fingerprint Scans for Food, Phones and Finances. - The New York Times, 07.04.2018.
165. Goulding, M. Letter Before Claim. Correspondence to Matt Jukes. Kättesaadav: https://www.libertyhumanrights.org.uk/sites/default/files/180611%20Letter%20before%20action%20to%20SWP.pdf (12.03.2019).
166. Grother, J. jt. Ongoing Face Recognition Vendor Test (FRVT) Part 2: Identification. National Institute of Standards and Technology Interagency/Internal Report 8238, 2018.
167. Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing is "Likely to Result in a High Risk" for the Purposes of Regulation 2016/679. – Article 29 Data Protection Working Party, 04.04.2017.
168. Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework. – United Nations Human Rights, Office of the High Commissioner. New York, Geneva: United Nations, 2011.
169. Handbook on European Data Protection Law. Käsiraamat. – FRA. Luxemburg: Euroopa Liidu Väljaannete Talitus, 04.2018.
170. Hao, K. A Little-known AI Method Can Train on Your Health Data without Threatening Your Privacy. – MIT Technology Review, 11.03.2019.
171. Herm, T. Teralised abilised mundris ja mundrita inimestele. – Virumaa Teataja, 06.04.2019.
172. Hiina „suur vend" näeb arvatust halvemini – Digi, 01.08.2018.
173. Hughes, M. Three Arrested Using Facial Recognition Technology during Wales' Six Nations Opener. – WalesOnline, 06.02.2018.
174. Inimkeskne ja nutikas kriminaaljustiitssüsteem ja kuriteoennetus: Kriminaalpoliitika põhialused aastani 2030. Eelnõu seisuga 29.11 2018. – Justiitsministeerium.
175. Introduction of Facial Recognition into South Wales Police. – South Wales Police, 2018.
176. Isikuandmete töötleja üldjuhend. – Andmekaitse Inspektsioon, 31.05.2018. Kättesaadav:

https://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/Juhised/2019%20juhised/Isikuandmete%20tootleja%20uldjuhend.pdf (10.03.2019).
177. Jacob, M. Facial Recognition Gains Grounds in Europe, Among Big-Brother Fears. – EURACTIV, 20.10.2017.
178. Koovisk, K. Mida on tehtud, et Kuressaare kesklinnas turvalisem oleks? – Saaremaa Teataja, 07.02.2019.
179. Korrakaitseseaduse eelnõu - SEN Seletuskiri RT I, 22.03.2011, 4, jõust 01.07.2014.
180. Kullamäe, H. Politsei ja Piirivalveameti vastus 2.1-3/23169-3 K. Käsperi (Eesti Inimõiguste Keskus) poolt esitatud arupärimisele droonide kasutamise kohta, 10.09.2018.
181. Kutsumata külalised purustasid külapoe akna ja varastasid sigarette. – Tartu Postimees, 20.03.2019.
182. Kuul, M. Valdav osa Eesti elanikke peab Eestit turvaliseks riigiks – ERR uudisteportaal, 24.09.2018.
183. Kütt, K. Turvalise identiteedi tulevik. – Director, 01.04.2019.
184. Laaring, M. jt. Korrakaitseseadus: kommenteeritud väljaanne. Komm vlj. Tallinn: Siseakadeemia 2017.
185. Lauri, U. Politsei soovib Läänemaa valve alla panna. – Lääne Teataja, 07.03.2019.
186. Lauristin, M. Protecting Personal Data Processed for the Purposes of Police and Judicial Cooperation in Criminal Matters. – Legistlative Train Schedule, 20.03.2019.
187. Lohr, S. Facial Recognition Is Accurate, If You're a White Guy. - The New York Times, 02.09.2018.
188. Lueth, K. L. State of the IoT 2018: Number of IoT devices now at 7B - Market accelerating – IOT Analytics, 08.08.2019.
189. Lõugas, H. Päris inimeste küsimused: mis asi see Elisa näotuvastus on ja kas ma peaks seda kartma? – Digigeenius, 10.09.2018.
190. Maanteeamet alustab Tallinnas keelava fooritule eiramise automaatkontrolli testperioodiga. – Maanteeamet, 18.02.2019.
191. Maigre, M., Kaska, K. Küberkaitsest terviklikult. – Diplomaatia, 14.09.2018.
192. Manko, R. EU Accession to the European Convention on Human Rights (ECHR). Briifing. – European Parliamentary Research Service (EPRS), 07.2017.
193. Mann, S. Surveillance (Oversight), Sousveillance (Undersight), and Metaveillance (Seeing Sight Itself). Workshop paper. The IEEE Conference on Computer Vision and Pattern Recognition (CVPR) Workshops, 2016.
194. Miidla, M. jt. Euroopa Liidu ja rahvusvaheliste õigusaktide analüüs identiteedihalduse valdkonnas. – Sorainen, 03.12.2018.
195. Montjoye, Y-A. jt. On the Trusted Use of Large-Scale Personal Data. – IEEE Data Engineering Bulletin, 2012/35.
196. Mozur, P. Inside China's Dystopian Dreams: A.I., Shame and Lots of Cameras. - The New York Times, 08.07.2018.
197. Naranjo, D. Data Protection Directive on Law Enforecement: The Loopholes. – EDRi, 18.11.2015.
198. NeoFace Watch: High Performance Face Recognition. Brožüür. – NEC Corporation, 2016. Kättesaadav: https://www.nec.com/en/global/solutions/safety/face_recognition/PDF/Face_Recognition_NeoFace_Watch_Brochure.pdf (10.02.2019).
199. Nilsson, P. How UK Police Are Using Facial Recognition Software. – Financial Times, 12.10.2018.

200. Nutt, M. ÜRO inimõiguste ülddeklaratsioon 70. – Diplomaatia, 2018/184.
201. Oh Behave! How Behavioral Analytics Fuels More Personalized Marketing. White Paper. IBM Corporation, 2013.
202. Opinion 2/2012 on Facial Recognition in Online and Mobile Devices. – Article 29 Data Protection Working Party, 22.03.2012.
203. Opinion 4/2007 on the Concept of Personal Data. - Article 29 Data Protection Working Party, 20.06.2007. Kättesaadav: https://www.clinicalstudydatarequest.com/Documents/Privacy-European-guidance.pdf (22.03.2019).
204. Opinion 5/2014 on Anonymization Technique. – Article 29 Data Protection Working Party, 10.04.2014.
205. Pau, A. Revolutsioon isikutuvastuses: Eesti asub looma sõrmejälgede hiigelandmebaasi – Postimees, 7.08.2018.
206. Petrie, C. Identity-matching Services Bill 2018 and Australian Passports Amendment (Identity-matching Services) Bill 2018. Eelnõu 110 seisuga 07.02.2018. – Parliament of Australia, 22.05.2018.
207. Pettey, C. Treating Information as an Asset. – Gartner, 17.02.2016.
208. Piovesan, C. How Privacy Laws Are Changing To Protect Personal Information – Forbes, 05.04.2019.
209. Police Defend Facial Recognition Technology that Wrongly Identified 2,000 People as Potential Criminals. – The Telegraph, 5.05.2018.
210. Politseinike arv on aastatega kahanenud ligi tuhande võrra – Lõuna-Eesti Postimees, 21.08.2018.
211. Privacy and Freedom of Expression in the Age of Artificial Intelligence. – Article 19, 04.2018. Kättesaadav: https://privacyinternational.org/report/1752/privacy-and-freedom-expression-age-artificial-intelligence (4.03.2019).
212. Proposal for a Directive of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data by Competent Authorities. Ülemkogu ettepanek. – Euroopa Ülemkogu, 02.10.2015. Kättesaadav: http://data.consilium.europa.eu/doc/document/ST-12555-2015-INIT/en/pdf (05.04.2019).
213. Raigla, M-L.. Läänemaal on kuritegevus Eesti keskmine. – Lääne Elu, 01.04.2019; M-L. Raigla. Sel aastal tulevad Haapsalu sissesõitudele kaamerad. – Lääne Elu, 01.04.2019.
214. Ratt, S. Taikse küla sai endale turvakaamerad. – Järva Teataja, 04.04.2019.
215. Report on Best Practices and Lessons Learned on How Protecting and Promoting Human Rights Contribute to Preventing and Countering Violent Extremism. ÜRO dokument A/HRC/33/29. – UN High Commissioner for Human Rights, 21.07.2016.
216. Reservations and Declarations for Treaty No.005 - Convention for the Protection of Human Rights and Fundamental Freedoms – Euroopa Nõukogu. Kättesaadav: https://www.coe.int/en/web/conventions/search-on-treaties/-/conventions/treaty/005/declarations (02.03.2019).
217. Rise of Surveillance Camera Installed Base Slows. – SDM, 5.05.2016.
218. Rouse, M. The Essential Guide to Managing HR Technology Trends: AI (Artificial Intelligence). – SearchEnterpriseAI. Kättesaadav: https://searchenterpriseai.techtarget.com/definition/AI-Artificial-Intelligence; (21.03.2019).

219. Schwartz, O. Don't Look Now: Why You Should Be Worried About Machines Reading Your Emotions. – The Guardian, 6.03.2019.
220. Seletuskiri isikuandmete kaitse seaduse eelnõu juurde. – RT I, 04.01.2019, 11 – jõust. 15.01.2019.
221. Singh, A. jt. Disguised Face Identification (DFI) with Facial KeyPoints using Spatial Fusion Convolutional Network. Veneetsia: IEEE International Conference on Computer Vision Workshops 2017.
222. Siseministri käskkirja "Siseturvalisuse arengukava 2015-2020" 2018-2021 programmide kinnitamine. Lisa 1 – Turvalisemad kogukonnad.
223. Solsman, J. E. Cities Worldwide Spend Over $3 Billion Last Year to Peep on You. – CNET, 28.03.2018.
224. Szalai, J. O.K., Google: How Much Money Have I Made for You Today. – The New York Times, 16.01.2019.
225. Surveillance Capitalism and the Challenge of Collective Action. – New Labor Forum, 01.2019. Kättesaadav: https://newlaborforum.cuny.edu/2019/01/22/surveillance-capitalism/ (27.02.2019).
226. Suunised automatiseeritud töötlusel põhinevate üksikotsuste tegemise ja profiilianalüüsi kohta määruse 2016/679 kohaldamisel. – Artikli 29 alusel asutatud andmetekaitse töörühm, 06.02.2018.
227. Suunised, mis käsitlevad andmekaitsealast mõjuhinnangut ja selle kindlaksmääramist, kas isikuandmete töötlemise tulemusena „tekib tõenäoliselt suur oht" vastavalt määrusele (EL) 2016/679. – Artikli 29 alusel asutatud andmekaitse töörühm, 04.04.2017.
228. The Work of the Biometrics Commissioner and Regulator Inquiry – Publications. – UK Parliament. Kättesaadav: https://www.parliament.uk/business/committees/committees-a-z/commons-select/science-and-technology-committee/inquiries/parliament-2017/work-of-biometrics-commissioner-and-forensic-science-regulator-17-19-17-19/publications/ (15.04.2019).
229. Thomas, D. The Cameras That Know if You're Happy – or a Threat. – BBC News, 17.07.2018.
230. Usaldusväärne ja turvaline identiteedihaldus aastateks 2019-2022. Siseministri käskkirja „„Siseturvalisuse arengukava 2015–2020" 2018–2021 programmide kinnitamine" lisa 7.
231. Valge Raamat: Identiteedihaldus ja isikut tõendavad dokumendid 1.0. – Riigi Infosüsteemi Amet 2018.
232. Veski, V. Poolik lahendus tõi Karmani parklasse pooliku öörahu. – Raplamaa Sõnumid, 27.03.2019.
233. Virk, K. PPA hankis piiriturvalisuse tagamiseks militaardroonid. – Politsei- ja Piirivalveamet, 12.01.2018.
234. Working Document on the Processing of Personal Data by Means of Video Surveillance. – Article 29 Data Protection Working Party, 25.11.2002.
235. ÜRO inimõiguste ülddeklaratsioon. Kättesaadav: https://vm.ee/et/uro-inimoiguste-ulddeklaratsioon (01.04.2019)

LISA 1 – EMOTSIOONITUVASTUSE KASUTUSVALDKONNAD

Järgnev on mitteametlik tõlge A. McStay koostatud ülevaatest emotsioonituvastuse kasutamisvaldkondade kohta[304].

Sektor/grupp	**Jälgimisviis**	**Huvi emotsioonide tuvastamiseks**
Reklaamijad ja turundajad	Meelestatuse analüüs, hääl, näo kodeerimine, biomeetria	Eelistuste, käitumise ja reaktsioonide parem mõistmine, reklaamide loomingulise osa optimeerimine
Tehisintellekt / kognitiivsed teenused	Meelestatuse analüüs, hääle analüüs, näo kodeerimine, biomeetria	Inimese ja masinate/teenuste/sisu vahelise suhtluse parandamine
Artistid	Meelestatuse analüüs, näo kodeerimine, biomeetria	Kunsti/meelelahutuse loomine ja publiku kaasatuse mõõtmine
Linnaplaneerimine	Meelestatuse analüüs, näo kodeerimine, biomeetria	Elanike seisukohtade tundma õppimine erinevate algatuste kohta
Informatsiooni maakler/kaupmees	Meelestatuse analüüs, näo kodeerimine, biomeetria	Müüdava informatsiooni rahalise väärtuse suurendamine
Haridus	Näo kodeerimine, biomeetria	Õpilaste käitumise, õppimise ja kaasatuse analüüsimine
Finantssektor	Meelestatuse analüüs (social media)	Turul valitsevate emotsioonide hindamine
Mängutööstus	Näo kodeerimine, biomeetria	Sisendseadmed parandavad mänguelamust

[304] A. McStay. The Right to Privacy in the Age of Emotional AI. Bangor: Bangor University 2018.

Tervishoid	Meelestatuse analüüs, hääle analüüs, näo kodeerimine, biomeetria	Inimeste mentaalse ja füüsilise seisundi jälgimine
Kodu, asjade internet (IoT)	Meelestatuse analüüs, hääle analüüs, näo kodeerimine, biomeetria	Teenuste ja reklaamide personaliseerimine
Kindlustus	Meelestatuse analüüs, näo kodeerimine, biomeetria	Klientide emotsionaalse ja mentaalse seisundi mõistmine (nt autos käitumise hindamine)
Politsei/turvateenistus	Meelestatuse analüüs, biomeetria	Kodanike tunnete/häirituse mõõtmine, teenistujate kutsumine
Poliitilised erakonnad	Meelestatuse analüüs	Üldsuse reaktsiooni mõõtmine eri poliitikatele ning eelnõudele
Robootika	Näo kodeerimine, hääle analüüs	Robotite ja inimeste vahelise suhtluse parandamine
Seksitehnoloogia	Biomeetria	Sekselu parandamine, seadmete tundlikkuse suurendamine
Sotsiaalmeedia	Meelestatuse analüüs, näo kodeerimine	Ligipääs meelestatusele, emotikonide kasutusele, grupi käitumisele, individuaalsele profileerimisele, muudatuste ja postituste käitumismustritele
Televisioon/filmindus	Meelestatuse analüüs, näo kodeerimine, biomeetria	Vaatajate reaktsiooni testimine
Kaubandus	Meelestatuse analüüs, hääle analüüs, näo kodeerimine, biomeetria	Mõõta kaupluse-sisest käitumist (võimalik selle alusel klientide segmenteerimine)

Toodete testimine	Meelestatuse analüüs, näo kodeerimine, biomeetria	Toodete kasutamise reaktsioonide mõõtmine
Riide- ja moetööstus	Biomeetria	Inimeste reaktsioonide, emotsioonide ja tujude jälgimine
Tööandjad, organisatsioonid	Meelestatuse analüüs, biomeetria	Emotsioonide ja tujude jälgimine organisatsioonis

LISA 2 – UK BIOMETRICS AND FORENSICS ETHICS GROUP ETTEPANEKUD NÄOTUVUVASTUSTEHNOLOOGIA KASUTAMISE PRINTSIIPIDEKS

Järgnev on mitteametlik tõlge UK *Biometrics and Forensics Ethics Group* koostatud printsiipidest[305] näotuvastuse kasutamiseks.

1. Avalik huvi. Selliste tehnoloogiate kasutamine on lubatud ainult juhul, kui tehnoloogia kasutus teenib avalikku huvi. Mõned sellised olukorrad võivad olla selgesti tuvastatavad, näiteks on avalikkuse huvides tuvastada kriminaalses tegevusest osa võtnud isikuid. Teistes olukordades võib piir olla hägusem ning tõlgendamisruumi enam.

2. Efektiivsus. Selliste tehnoloogiate kasutamine saab olla õigustatud ainult juhul, kui see on efektiivne viis inimeste tuvastamiseks ehk ebatäpset tehnoloogiat ei tohiks kasutada.

3. Eelarvamuste ja ebaõiglaste algoritmide vältimine. Tehnoloogia ei tohi sisaldada ega kajastada põhjendamatuid eelarvamusi. Põhjendamatud eelarvamused võivad suurendada ebaõiglust kahel viisil. Esiteks, mõned eelarvamused on olemuslikult alandavad ja solvavad. Teiseks, selliseid eelarvamusi sisaldav tehnoloogia võib põhjustada ebavõrdset ja diskrimineerivat kohtlemist (näiteks võib see kaasa tuua osade rühmade esindajate tõenäolisema kinnipidamise või vajaduse tuvastamiseks). Avalikes kohtades kasutatavad biomeetrilistel andmetel põhinevad tuvastussüsteemid (sh infokogumise viisid süsteemide õppeprotsessis) peaksid olema peaks olema avatud kontrollile ja tõhusale järelevalvele.

4. Erapooletus kasutuselevõtul. Kui tehnoloogiat kasutatakse politseitööks, tuleb seda kasutada ühtlaselt. Näiteks ei tohiks seda ilma mõjuva põhjuseta kasutada sellistel viisidel, mis oleksid ebaproportsionaalselt suunatud teatud sündmustele, kuid mitte teistele.

5. Vajadus. Üksikisikutel on õigus elada ilma, et neid jälgitaks ja kontrollitaks. Arvestades, et tuvastustehnoloogiate kasutamine riivab neid õigusi, võib tehnoloogiat kasutada ainult siis, kui muud, vähem õigusi riivavad meetodid, ei ole kättesaadavad. Tehnoloogiat tuleks kasutada viisil, mis minimeerib seadusekuulekate inimeste kaasatust.

6. Proportsionaalsus. Lisaks „vajalikkuse" nõudele peab tehnoloogia kasutamine vastama ka „proportsionaalsuse" nõudele. See tähendab, et tehnoloogia kasutamine saab olla lubatud ainult juhul, kui saadav hüve on proportsionaalne vabaduse ja eraelu puutumatuse riivega. Saadavad hüved peavad olema piisavalt suured, et õigustada teiste õiguste riivamist.

[305] Ethical Issues Arising From The Police Use of Live Facial Recognition Technology. Raport. – Biometrics and Forensics Ethics Group Facial Recognition Working Group, 02.2019.

7. Erapooletus, aruandekohustus ja järelvalve jälgitavate isikute nimekirjade koostamisel. Kui jälgitavate isikute nimekirjade koostamisest võtavad osa inimesed (või algoritmid), on oluline, et nad oleksid erapooletud ja eelarvamustevabad. Nimekirjade koostamist peab kontrollima sõltumatu organ.

8. Avalikkuse usaldus. Kui tehnoloogiat kasutatakse politseitöös, on oluline, et seda kasutavad isikud (nii testimis- kui kasutusfaasis) osaleksid sellekohases avalikus diskussioonis ja selgitaksid tehnoloogia kasutamise põhjuseid.

9. Kuluefektiivsus. Enne tehnoloogia kasutusele võtmist tuleb hinnata, kas olemasolevaid ressursse saaks mujal paremini rakendada.

Toetavad küsimused eetiliste printsiipide rakendamisel õiguskaitseasutustele reaalajas näotuvastustehnoloogia kasutamisel. Järgnevaid küsimusi ei tohiks käsitleda ammendavana ega kontrollnimekirjana:

1. Avalik huvi

- Miks konkreetses situatsioonis reaalajas näotuvastustehnoloogiat kasutatakse (kuritöö takistamine, informatsiooni kogumine jne)?

2. Efektiivsus

- Milline on tehnoloogia täpsus? Kuidas arvutatakse vale-positiivsete ja vale-negatiivsete vastuste määra?
- Kas näotuvastustehnoloogia on valideeritud kasutades tegelikke empiirilisi andmemassiive?
- Kuidas hinnatakse kasutamise edukust? Tõesed vasted/väärate vastete puudumine, sagenenud arreteerimised, vähenenud kriminaalne aktiivsus/vähenenud arreteerimised?
- Milline on kasutatavate piltide kvaliteet?
- Milline on süsteemi seadistus? Kaamera positsiooni või andmete edastamiseks kasutatav võrguühenduse olulisus.
- Kui palju väheneb täpsus kiiruse parenemisel ja vastupidi (süsteemi tunnused)?
- Kui kiiresti on võimalik kohapealsetel politseinikel infole (huvipakkuv tuvastatud isik) reageerida (süsteemi asukoht)?
- Milline info süsteemi vaste kohta jõuab kohapealsete politseinikuteni? Kas informatsioon on piisavalt detailne, et isik täpselt tuvastada ja olukorda sekkuda?

- Milline on süsteemi inimoperaatorite väljaõpe?
- Kas inimoperaatorite nõustumist ja mittenõustumist algoritmi tulemustega jälgitakse ja hinnatakse?
- Kuidas inimoperaatorist tulenevaid eksimusi mõõdetakse?

3. Eelarvamuste ja ebaõiglaste algoritmide vältimine
    - Kas on algoritmilist kallutatust arvesse võetud?
    - Kuidas algoritmi kallutatust mõõdetakse?
    - Millist infot kasutatakse alogritmide õpetamiseks?
4. Erapooletus ja kasutuselevõtt
    - Mille alusel otsustakse asukohad, kus LFR tehnoloogiat rakendatakse?
    - Kes otsustab, kus LFR tehnoloogiat rakendatakse?
    - Kas on läbi viidud mõjuhinnang kogukonnale?
5. Vajadus
    - Millisel õiguslikul alusel, kui üldse, tehnoloogia kasutamine baseerub?
    - Kas jälgitavate isikute nimekiri sisaldab pilte lastest?
6. Proportsionaalsus
    - Mis eesmärgil näotuvastustehnoloogiat kasutatakse?
    - Kas näotuvastustehnoloogia kasutamine on proportsionaalne?
    - Millised on süsteemi kasutamise negatiivsed mõjud (isikuvabadustele) ja tulud (avalikule turvalisusele)?
    - Kas salvestatud piltide või andmete säilitamine on proportsionaalne?
7. Erapooletus, aruandekohustus ja järelvalve jälgitavate isikute nimekirjade koostamisel
    - Kes teostab tehnoloogia kasutuselevõtu üle järelvalvet?
    - Kuidas näotuvastustehnoloogiate kasutamist hinnatakse?
    - Kes koostas jälgitavate isikute nimekirja?
    - Kui mahukas see nimekiri on?
    - Miks just selline nimekiri?

- Kust pärinevad nimekirjas kasutatavad pildid?
- Kui täpsed on nimekirjas kasutatavad pildid?
- Milliseid juhiseid järgides on nimekiri kokku pandud?
- Kes teostab nimekirja kokkupaneku üle järelvalvet?
- Kas ja mil määral pildid või informatsioon salvestatakse?
- Kui pika perioodi vältel kasutatud pilte või informatsiooni säilitatakse?
- Kus kasutatud pilte või informatsiooni talletatakse?
- Kellel on ligipääs salvestatud piltidele või informatsioonile?
- Kui pilte ja infot jagatakse teiste asutustega, siis kellega ja miks?

8. Avalik usaldus

- Kas automatiseeritud näotuvastustehnoloogia on test- või operatiivkasutuses?
- Kui laialdaselt näotuvastustehnoloogia kasutuselevõttu kogukonnas reklaamitakse?
- Kui teadlik on üldsus tehnoloogia kasutuselevõtust?
- Kas kasutuselevõtt on piisavalt läbipaistev?
- Kas kogukonna liikmetel on võimalik lihtsa vaevaga tehnoloogia kasutuselevõtu kohta informatsiooni saada?
- Kui süsteemi üle teostatakse kollegiaalset järelvalvet, siis kas sellesse kuulub ka kogukonna esindaja?

9. Kuluefektiivsus

- Kas näotuvastustehnoloogia kasutamine on kuluefektiivne?

LIHTLITSENTS LÕPUTÖÖ REPRODUTSEERIMISEKS JA LÕPUTÖÖ ÜLDSUSELE KÄTTESAADAVAKS TEGEMISEKS

1. Mina, Kea Kruuse, annan Tartu Ülikoolile tasuta loa (lihtlitsentsi) enda loodud teose magistritöö pealkirjaga „Privaatsuse ja isikuandmete kaitse masinnägemise ja masinõppe kasutusel Euroopa Liidu õiguses emotsioonituvastuse ja Eesti korrakaitse jälgimisseadmestike näitel“, mille juhendaja on *PhD* Carri Ginter,
   1.1. reprodutseerimiseks säilitamise ja üldsusele kättesaadavaks tegemise eesmärgil, sealhulgas digitaalarhiivi DSpace-is lisamise eesmärgil kuni autoriõiguse kehtivuse tähtaja lõppemiseni;
   1.2. üldsusele kättesaadavaks tegemiseks Tartu Ülikooli veebikeskkonna kaudu, sealhulgas digitaalarhiivi DSpace´i kaudu kuni autoriõiguse kehtivuse tähtaja lõppemiseni.

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

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

Tallinnas, **30.04.2019**