

Peatükk 25

Tehnoloogia ja inimõigused

Anna-Maria Osula, Maarja Pild, Karmen Turk

Sissejuhatus

Juba praegu on maailmas internetiga ühenduses olevaid seadmeid¹ rohkem kui planeedil elanikke ning aastaks 2025 ennustatakse nutistusse kuuluvate seadmete arvuks 25 miljardit.² Sarnaselt nutistu haardega on hüppeliselt kasvanud ka salvestatud ning töödeldavate andmete maht. Prognoositakse, et aastaks 2025 on kogu maailma andmete maht 175 zettabaiti.³

Kahtlemata on tehnoloogia sellisel plahvatuslikul arengul suur mõju meie ühiskonnale, igapäevaelule ning ka inimõiguste kaitsele.⁴ Digiajastu teeb võimalikuks inimõigusi teostada viisil, mis oli varem kujutlematu. Interneti vahendusel saab igaüks vaid mõne sekundiga levitada oma ideid ja arvamusi miljonite inimesteni ning leida soovitud informatsiooni. Veebis saame esitada maksudeklaratsioone, suhelda riigiasutuste ja poliitikutega, taotleda isikut tõendavaid või muid dokumente ning seda kõike tehes hoida kokku hulga aega, mis muidu kuluks ametiasutustes järjekorras seismisele.

Aina põletavamaks muutuvad aga ka inimõiguste kaitsega seotud probleemid, mida tehnoloogia kiire areng, laialdane levik ning meie enda käitumine kaasa toovad. Mitmed mured seonduvad andmete jagamise, kogumise ja töötlemisega. Interneti tavakasutajale jääb tihti hoomamatuks, kui palju ta oma oma igapäevategevusega andmeid loob ja jagab. Samuti jäetakse – kas teadlikult või teadmatusel – enda tegevusest kübermaailmas maha ohtralt nn digitaalset jalajälgi ega omata ülevaadet, kes ja mis tingimustel meie isikuandmetele ligi pääseb või neid kolmandatele isikutele edasi saadab. Siin ei ole aga oluline üksnes elektrooniliste sidevahendite abil saadatud sõnumite või avalike postituste sisu, vaid tihti märkamata jäävate andmete kogumine ja analüüs. Näiteks teenusepakkujad koguvad oma kasutajate kohta suurel hulgal andmeid (sh metaandmed⁵), mida võidakse mitmesugustel tingimustel jagada nii riikide valitsuste kui ka eraettevõtetele. Mitmed tehnoloogilised

¹ Nn asjade internet ehk nutistu on Rahvusvahelise Telekommunikatsiooni Liidu definitsiooni kohaselt infoühiskonna globaalne taristu, mis võimaldab täiustatud teenuseid koostalitlusvõimeliste asjade ühendamise kaudu. Nutistusse kuuluvad asjad võivad olla sidevõrkudega ühendatud nutitelefonid, külmkapid, sõidukid, aktiivsusmonitorid jms seadmed, mis saavad edastada teavitusi oma olekust ja ümbruskonna seisundist. Overview of the Internet of things. International Telecommunication Union. Recommendation. 06.2012. – ITU-T Y.2060.

² Joint communication to the European Parliament and Council. The EU's Cybersecurity Strategy for the Digital Decade – JOIN (2020) 18 final, lk 1.

³ Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A European Strategy for Data. European Commission. 19.02.2020 – COM(2020) 66.

⁴ ÜRO inimõiguste ülemvolinik Michelle Bachelet on tehnoloogia arengu mõju inimõigustele iseloomustanud järgmiselt: „Parimal juhul annab digitaalrevolutsioon juurde võimalusi, ühendab, informeerib ja päästab elusid. Halvemal juhul muudab see jõuetuks, lahutab, annab valeinformatsiooni ja maksab elusid.“

⁵ Ka Euroopa Inimõiguste Kohus näib olevat seisukohal, et metaandmete kaitse võib kuuluda nii kommunikatsioonisaladuse kui ka eraelu puutumatuse kaitsealasse: EIK, 62617/00, Copland vs. Ühendkuningriik; vt ka Laos, S., Sepp, H. Paragrahv 43. – Madise, Ü. et al. (toim). Eesti Vabariigi põhiseadus. Kommenteeritud väljaanne. Tartu: Sihtasutus Iuridicum 2020, p 10. – <https://pohiseadus.ee/sisu/3514>.

lahendused⁶ võimaldavad samas näiteks informatsiooni krüpteerimise ja anonüümimise abil inimõiguste paremat kaitset.⁷

Aina rohkem õiguslikke küsimusi tekitavad ka riikide ning ettevõtete kogutavad biomeetrilised andmed, nagu DNA, näo geomeetria, hääl, silmaiirise mustrid ja sõrmejäljed, mille väärkasutus võib rikkuda inimeste õigusi.⁸ Lisaks andmete mahu suurenemisele on hüppeliselt kasvanud tehnoloogiline võimekus neid andmeid töödelda ning suurtest andmemahtudest (nn suurandmed) eesmärgipärast teavet tuletada.⁹ Näiteks Londonis võib kaameratega jälgida sisuliselt tervet linna ning tulemuslikumaks infokogumiseks katsetatakse näotuvastust.¹⁰ Hiinas on näotuvastamist võimaldava tehnoloogia kasutamine suurlinnades juba laialt levinud ning väidetavalt on võimalik seda kasutada ka etniliste vähemuste tuvastamiseks.¹¹ Samuti saab inimese käitumist veebisaitidel ning sotsiaalmeediaplatvormidel analüüsida viisil, mis loob isikust kirjelduse, mille abil on võimalik meie ekraanile suunata kindlaid reklaame või muud meediasisu ning ennustada meie käitumist. Selliseid meetodeid kasutades võib mõjutada kindla inimgrupi käitumist, mis võib päädida riiklikult oluliste otsustega.¹²

Kriitilise tähtsusega on ka andmeturve, millega kaitstakse andmete konfidentsiaalsust, terviklikkust ning käideldavust. Eespool kirjeldatud kasvav sõltuvus info- ja kommunikatsioonitehnoloogiast ning andmete suurenev maht toob aga paratamatult kaasa riskid ja võimaliku haavatavuse. Seda omakorda kasutavad õigusvastases tegevuses ära kurjategijad, terroristlikud rühmitused, aga ka riikide valitsused. Nii on aina enam sazenenud arvutikuritegevus ja küberoperatsioonid, mis võivad kaasa tuua inimõiguste rikkumisi. Näiteks rahalise kasu eesmärgil rünnatakse üksikisikute ja asutuste seadmeid ning andmeid. Poliitilistel ja sotsiaalsetel põhjustel mõjutatakse ühiskondlikke protsesse või tungitakse

⁶ Näiteks võimaldab Tor võrk kasutada interneti nii, et see peidab kasutaja tegeliku IP-aadressi. Loe: Minárik, T., Osula, A.-M. Tor does not stink: Use and abuse of the Tor anonymity network from the perspective of law. – Computer Law and Security Review 2016/32 (1), lk 111–127.

⁷ Nastic, M. The impact of the informational and communication technology on the realization and protection of human rights – Balcan Social Science Review 2021/17, lk 81–83. Siinkohal tuleb tähelepanu pöörata, et mitmed anonüümimist lubavad tehnoloogiad on kahetiselt kasutatavad. Ühelt poolt aitavad need kaitsta privaatsust ja sõnavabadust tsenseerimist rakendavates ühiskondades, teisalt aga võivad samad tehnoloogiad abistada kurjategijaid nende ebaseaduslikus tegevuses. Nii tekitab suuri vaidlusi näiteks krüpteerimist võimaldavate tehnoloogiate reguleerimine, riigiasutuste ligipääs krüptograafilistele protokollidele ning toodetele nn tagaukse lisamine. Samuti mõjutavad internetifiltrid ja side jälgimine inimõiguste kaitsjate poolt salajase teabe edastamist.

⁸ Hiinas on kasutusel palju tehnoloogilisi vahendeid ühiskonna jälgimiseks. Loe: Harwell, D. *et al.* Huawei Tested AI Software That Could Recognize Uighur Minorities and Alert Police, Report Says. – Washington Post 12.03.2021.

⁹ Niisamuti kasvab digimaailma mõju keskkonnale. Näiteks on alles viimastel aastatel hakatud laialdasemalt uurima, millised on ühe selvefoto (selfi) või ka laiema sotsiaalmeedia ja internetiga kasutamisega keskkonnale tekkivad tagajärjed. Kui ühe foto näiteks Instagrami laadimine ei oma erilist mõju, siis selge on, et miljonite kasutajate poolt ka üksnes sotsiaalmeedia kasutamine jätab keskkonnale oma jälje. Vt Priest, C., Schien, D., Blevis, E. Understanding and Mitigating the Effects of Device and Cloud Service Design Decisions on the Environmental Footprint of Digital Infrastructure. Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems.

¹⁰ Väidetavalt on London maailmas esirinnas turvakaamerate arvu poolest elanike arvu kohta. Nüüd arutletakse selle üle, kas lisada kaameratesse näotuvastuse võimekus. Loe: Satariano, A. London Police Are Taking Surveillance to a Whole New Level. – The New York Times 24.01.2020.

¹¹ Doffman, Z. China Is Using Facial Recognition To Track Ethnic Minorities, Even In Beijing. – Forbes 03.05.2019.

¹² Näiteks võib tuua 2018. aastal lahvatanud skandaali Cambridge Analytica ja Facebooki ümber, kui selgus, et Cambridge Analytica kogus ja analüüsis miljonite Facebooki kasutajate andmeid, selleks et mõjutada nende valikut USA 2017. aasta presidendivalimistel. Vt Confessore, N. Cambridge Analytica and Facebook: The Scandal and the Fallout So Far. – The New York Times 04.04.2018.

riiklikesse süsteemidesse ja taristuid haldavatesse võrkudesse, et häirida nende toimimist ja tekitada kahju või lekitada andmeid. Raskematel juhtudel võivad ohus olla inimeste tervis ning elu. Samuti arendavad mitmed riigid autonoomseid relvasüsteeme, mis suudavad sihtmärke valida ning rünnata ilma inimese igakülgse kontrollita. See tõstatab põletavaid probleeme seoses sõjaõiguse põhimõtete järgimisega.¹³

Tehnoloogia on loonud väljendusvabaduse kasutamiseks uued võimalused, aga ka proovikivid. Euroopa Inimõiguste Kohus on selgitanud, et väljendusvabaduse mõju on tehnoloogia tõttu võimendatud, arvestades seda, kui kergesti, ulatuslikult ja kiiresti teave internetis levib ja kui visalt jääb püsima kord juba avaldatud teave.¹⁴ Arvestada tuleb ka asjaolu, millises ulatuses kontrollivad tehnoloogilisi võimalusi eraõiguslikud isikud. Seetõttu on tehnoloogiat arendavatel ja kasutavatel ettevõtetel nagu riikidelgi kohustus ja vastutus austada, kaitsta, järgida ja teostada inimõigusi. Muu hulgas kerkivad esile küsimused infole ligipääsu ning info jagamise kohta võrgus, kus eraõiguslikud isikud on otsustaja rollis, samuti selle kohta, kes vastutab internetis avaldatu sisu eest.

Väljendusvabaduse põhiõiguse teostamine on järjest enam surve all seoses selliste uute tehnoloogiate nagu tehisintellekti ja algoritmiliste süsteemide kasutuselevõtmisega. Tehisintellekti puhul on enim kõlapinda tekitanud otsimootorite, algoritmilise ennustamise ja isikupärastamise (profileerimine), algoritmilise modereerimise ja algoritmide poolt sisu loomisega seonduvad tehnoloogiad ja nende kasutamine. Arusaadavalt on ülemaailmsel digitaalsetel platvormidel ning uutel tehnoloogiatel suur mõju nii üksikisikute kui ka ühiskondade teabekeskkondadele, kus automatiseeritud algoritmid otsustavad, kuidas käsitleda, prioriseerida, levitada ja kustutada või eemaldada kolmanda osapoole sisu veebis.

Ka kogunemis- ja ühinemisvabadus ei ole tehnoloogia arengust – nii positiivselt kui ka negatiivselt – mõjutamata. Tehnoloogia loob enneolematud võimalused ühistegevuseks. Samaaegselt võimaldab seesama tehnoloogia lihtsalt tuvastada üritusel osalevaid isikuid ja selle organiseerijaid, samuti on lihtne jälgida ühinemise või meeleavalduse kulgemist. Just massjälgitamine ja inimeste eraellu sekkumised, mida tehakse seoses õiguskaitse ja riikliku julgeoleku nimel ning teenuse osutaja poolt, on saamas proovikiviks.

Mastaapsemaks muutuvad küsimused digitaalsest enesemääramisõigusest olukorras, kus automaatselt kohandatakse inimeste informatsioonilisi valikuid ja keskkonda, et ennustada üksikisikute käitumist, huve, eelistusi ja haavatavust.

Selles peatüks analüüsimegi, kuidas inimõiguste standardeid austades eespool nimetatud väljakutsetega rinda pista.

1. Riigi kohustused põhiõiguste tagajana tehnoloogia tähtsuse suurenemisel

Riigil tuleb kaitsta isikut nii riigivõimu kui ka kurjategijate ja kolmandate riikide tegevuse eest. Euroopa Inimõiguste Kohus on rõhutanud, et riigil ei lasu mitte ainult kohustust hoiduda sekkumast isikute õigustesse, vaid tal on ka positiivne kohustus võtta meetmeid isikuõiguste kaitseks.¹⁵

¹³ Loe küberoperatsioonide ning inimõiguste kohta lähemalt: Schmitt, M. N. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. – Cambridge: Cambridge University Press 2017.

¹⁴ EIK, 64659/09, Delfi AS vs. Eesti, 16.06.2015.

¹⁵ EIK, 28955/06, 28957/06, 28959/06 ja 28964/06, Palomo Sánchez ja Others vs. Spain, 12.09.2011, p 59.

Selline positiivne kohustus on ajas muutuv. Euroopa Inimõiguste Kohus arutas juhtumit (kohtuasi *Pravoye Delo vs. Ukraina*), kus ajakirjandusväljaanne avaldas internetiavarustest leitud anonüümse kirja, mille väidetavalt oli kirjutatud Ukraina julgeolekuteenistuse töötaja. Kirjas väideti, et julgeolekuteenistuse Odessa piirkondliku osakonna kõrgemate ametnike tegevus on olnud ebaseaduslik ja korruptiivne ning eelkõige seda, et neil on sidemeid organiseeritud kuritegelike rühmituste liikmetega. Ukraina kohus tuvastas *Pravoye Delo* tegevuses rikkumise ning kohustas väljaannet vabandama.¹⁶ Euroopa Inimõiguste Kohus aga sedastas, et Ukraina riik on jätnud täitmata oma positiivse kohustuse, kuivõrd riigisisene õigus sisuliselt ei võimalda anonüümse materjali avaldamist ega anna piisavat selget käitumisjuhist. Kohus märkis: „Piisava õigusliku raamistiku puudumine riigisisel tasandil, mis võimaldab ajakirjanikel kasutada internetist saadud teavet, kartmata sanktsioonide kehtestamist, takistab tõsiselt ajakirjanduse elutähtsa funktsiooni täitmist „avaliku vahikoerana“.“¹⁷

Suurenev digitaliseeritus tähendab ka seda, et küberohtudega võitlemiseks peab üha enam arvestama nii interneti, sellega seotud tehnoloogiate kui ka digitaalselt salvestatud või elektrooniliselt edastatud andmete omapäraga. Viimane viitab muu hulgas sellele, et riigiasutustel peavad olema õigused, oskused ja vahendid vajalike tõendite ja andmete kogumiseks ning analüüsimiseks. Samal ajal ei tohi riigi tegevus kuritegevuse ning terrorismiga võitlemisel muutuda ettekäändeks, millele toetudes viia läbi näiteks massilist jälgimist ning seeläbi ülemäära riivata üksikisiku inimõigusi. Seda põhimõtet on selgitanud ka Euroopa Kohus.¹⁸

Kui positiivse kohustuse põhimõte tähendab traditsiooniliselt riigi kohustust kaitsta isikut riigivõimu eest, siis praeguseks on see laienenud ka juhtumitele, kus võimalik oht inimõigustele ei tulene mitte avalikult võimult, vaid eraallikaist (nn horisontaalne mõju). Horisontaalse mõju õigusliku aluse on Euroopa Inimõiguste Kohus sõnastanud põhimõttes, et riigil on kohustus kaitsta konventsioonis sätestatud õigusi ja vabadusi, aga ka kohustus tagada nende õiguste teostamise võimalus, ning selle tõttu peab riik nõudma igahelilt enda jurisdiktsioonis konventsiooni austamist.¹⁹ Riigil on kohustus kaitsta isikuid inimõiguste rikkumise eest kolmandate isikute, sealhulgas äriettevõtete poolt, ning riik peab võtma ka meetmed ning looma sobiva õigusraamistiku, et rakendada ÜRO ettevõtete ja inimõiguste juhtpõhimõtteid.²⁰

Euroopa Nõukogu on eespool öeldule viidanud kui kohustusele rakendada ÜRO ettevõtluse ja inimõiguste juhtpõhimõtteid, mis tuginevad kolmele sambale: 1) riikide kohustus austada, kaitsta ja järgida inimõigusi ja põhivabadusi (riigi kohustus kaitsta inimõigusi); 2) ettevõtete kui ühiskonna eriorganite roll, kes täidavad eriülesandeid ja on kohustatud järgima kõiki kohaldatavaid seadusi ja austama inimõigusi (ettevõtete kohustus austada inimõigusi); 3) vajadus, et õiguste ja kohustuste rikkumise korral oleks võimalik kasutada asjakohaseid ja tõhusaid õiguskaitsevahendeid (õiguskaitse kättesaadavus).²¹ Tehnoloogiaga seoses on paratamatu, et tehnoloogiaettevõtted on peamine lüli, mille kaudu saavad isikud teostada enda

¹⁶ EIK, 33014/05, Editorial board of *Pravoye Delo* ja *Shtekel vs. Ukraine*, 05.08.2011.

¹⁷ *Ibid.*

¹⁸ EK, C-203/15, *Tele2 Sverige AB vs. Post- och telestyrelsen ja Secretary of State for the Home Department (C-698/15) vs. Tom Watson, Peter Brice, Geoffrey Lewis*, ECLI:EU:C:2016:970; EK liidetud kohtuasjad C-293/12 ja C-594/12, *Digital Rights Ireland Ltd jt vs. Minister for Communications jt*, ECLI:EU:C:2018:788.

¹⁹ EIK, 71503/01, *Assanidze vs. Gruusia*, 08.04.2004.

²⁰ ÜRO Inimõiguste Nõukogu resolutsioon inimõigustest, transnatsionaalsetest korporatsioonidest ning muudest äriettevõtetest; rakendamiskohustus tuleneb ka Euroopa Nõukogu Ministrite Komitee soovitusel CM/Rec(2016)3 inimõigustest ja ettevõtlusest. ÜRO, A/HRC/17/31.

õigusi ja vabadusi (nt interneti- või nutistu teenuseid kasutades). Seetõttu laieneb muu hulgas ka tehnoloogiaettevõtetele kohustus ning vastutus austada, kaitsta, järgida ja viia ellu inimõigusi.

2. Tehnoloogiaajastu tuumikpõhimõtted

2.1. Pärismaailm *versus* virtuaalmaailm ehk samade reeglite järgimine mõlemas keskkonnas

Virtuaalmaailmas ning pärismaailmas peaksid kehtima ühesugused reeglid. See tähendab, et virtuaalmaailma ei tohiks kohelda teisiti, kui koheldakse pärismaailma. Esmakordselt tehti sellekohane avalik poliitiline avaldus Bonni ministrite konverentsi²² deklaratsioonis 1997. aastal.²³ Deklaratsiooni artiklis 22 sätestatud printsiip kõlab: „Ministrid rõhutavad, et üldist õigusraamistikku tuleks kohaldada võrgus (*online*) nii nagu võrguühendusesta (*offline*). Pidades silmas uute tehnoloogiate arengukiirust, tuleks püüda luua õigusraamistikku, mis on tehnoloogianeutraalne, arvestades samas vajadust vältida tarbetut reguleerimist.“²⁴

Ühinenud Rahvaste Organisatsiooni (ÜRO) Inimõiguste Nõukogu võttis esmakordselt aastal 2012 ühehäälselt vastu resolutsiooni isikute sõnavabaduse kaitsmiseks internetis. See oli esimene selleteemaline resolutsioon. Kõrgetasemeline resolutsioon sätestab ka virtuaal- ja pärismaailma võrdsena kohtlemise põhimõtte: „[...] samu õigusi, mis inimestel on võrguühendusesta, tuleb kaitsta ka võrgus, eriti sõnavabadust, mida kohaldatakse piiridest sõltumata ja mis tahes valitud meedia kaudu vastavalt inimõiguste ülddeklaratsiooni artiklile 19 ja kodaniku- ja poliitiliste õiguste rahvusvahelisele paktile.“²⁵

Ka Euroopa Inimõiguste Kohus on näiteks kohtuasjas Węgrzynowski ja Smolczewski *vs.* Poola väljendusvabaduse põhimõtet rakendades rõhutanud, et nii nagu kaitseme Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artiklile 10²⁶ toetudes ajakirjandusväljaande paberarhiive, on kaitse all ka väljaande digitaalsed arhiivid internetis. Kohus rõhutas, et internetiarhiivid on oluline haridus- ja ajaloouringute allikas, eriti seetõttu, et need on üldsusele hõlpsasti kättesaadavad ja üldiselt tasuta.²⁷ Seega ei ole vaidlust selle üle, et ka internetis ajalooliselt avaldatu on kaitse all. Niisiis ei piisa informatsiooni eemaldamiseks argumendist, et veebis midagi teostada on lihtne ja odav. Veebiarhiivides avaldatu väärrib sama palju kaitset nagu paberarhiivides avaldatu. Kui me ei kiirusta väljaannet kohustama eemaldama sisu paberväljaandest, siis ei tohiks seda nõuda ka veebiväljaandelt lihtsalt sel põhjendusel, et seda on lihtne ja odav teostada.

²¹ Recommendation to Member States on Human Rights and Business. Committee of Ministers 02.03.2016. – CM/Rec(2016)3.

²² Bonnis toimunud kohtumisel osalesid Euroopa Liidu liikmesriigid, Euroopa Vabakaubanduse Assotsiatsiooni liikmed ja Küpros, kuid lisaks Euroopa riikidele said konverentsil kaasa rääkida Kanada, Jaapan, Venemaa ja Ameerika Ühendriigid.

²³ Reed, C. Online and Offline Equivalence: Aspiration and Achievement. – International Journal of Law and Information Technology. 2010/3, lk 248.

²⁴ Global Information Networks: Releasing the Potential. European Ministerial Conference. Luxembourg: Office for Official Publications of the European Communities 1998, lk 1.

²⁵ The promotion, protection and enjoyment of human rights on the Internet. United Nations Human Rights Council. 16.07.2012. – A/HRC/RES/20/8. Praeguseks on resolutsiooni juba korduvalt uuendatud ja täiendatud. Viimati tehti seda aastal 2018: The promotion, protection and enjoyment of human rights on the Internet. United Nations Human Rights Council. 04.07.2018. A/HRC/38/L.10/Rev.1.

²⁶ Euroopa inimõiguste ja põhivabaduste kaitse konventsioon. – RT II 2010, 14, 54.

²⁷ EIK, 33846/07, Węgrzynowski and Smolczewski *vs.* Poland, 16.10.2013.

2.2. Tehnoloogia- ja võrguneutraalsus

Tehnoloogia arenguga kaasneb ka aina uute õigusnormide vastuvõtmise vajalikkuse küsimus. Õigusnormide eesmärgipärane tõlgendamine võimaldab rakendada ka aastakümneid tagasi vastu võetud norme tänapäevast tehnoloogiat ja uusi vajadusi arvestades.²⁸ Nii välditakse uute tehnoloogispetsiifiliste õigusnormide vastuvõtmist. Seda õigusloome aluspõhimõtet teenib osaliselt ka tehnoloogianeutraalsuse põhimõte.

Tehnoloogianeutraalsus tähendab laiemas mõttes, et õiguslik regulatsioon ei tohiks konkreetset tehnoloogiat soosida ega diskrimineerida.²⁹ Tehnologianeutraalsuse põhimõttele tugineva seadusloome eesmärk on, et norme saaks tõhusalt kasutada ka uute tehnoloogiate leiutamise ja arendamise korral.³⁰ Vältida tuleks normistikku, mis uue tehnoloogia väljaarendamisel muutub kasutuks. Näiteks liiklusseaduse § 2 punkti 68¹ järgi on robotliikur ratastel või muul veermikul maapinnaga kontaktis liikuv osaliselt või täielikult automaatne või kaugjuhitav sõiduk, mis kasutab ümbritseva keskkonna kohta teabe saamiseks andureid, kaameraid või muid seadmeid ja mis on saadud teavet kasutades suuteline liikuma osaliselt või täielikult juhi kontrollita.³¹ Märgitud liiklusseaduse normi kohta võib küsida, et kas seadusandja ei ole läinud reguleerimisega liiale, defineerides robotliikuri „maapinnaga kontaktis“ olevaks sõidukiks. Tehnologianeutraalsuse põhimõtte kohaselt tuleks seadusandjal sedavõrd detailset ja konkreetset tehnoloogial põhinevat regulatsiooni vältida.

Võrguneutraalsuse (*net neutrality*) rakendamise eesmärk on kaitsta eelkõige väljendusvabadust ning seega vältida kahjulikke mõjusid isikute õigusele pääseda juurde internetis nende valitud sisule, rakendustele ja teenustele ning neid levitada, olenemata sellest, kas seda pakutakse tasuta või mitte, kasutades enda valitud sobivaid seadmeid.³² Võrguneutraalsust on juba aastal 2003 defineeritud kui põhimõtet, mille kohaselt peavad internetiühenduse pakkujad kohtlema võrdselt kõiki veebiteenuseid ja kogu edastatavat infot, ilma diskrimineerimise, piirangute ja sekkumiseta, olenemata info saatjast, vastuvõtjast, tüübist või sisust. Eesmärk on mitte piirata internetikasutajate valikuvabadust, et ei eelistataks konkreetse sisu või konkreetsete teenuste, rakenduste või seadmetega seotud internetiliiklust.³³ Euroopa Nõukogu on oma soovitusel CM/Rec(2016)1 võrguneutraalsuse põhimõtet põhjalikult selgitanud, nimetades võrguneutraalsuse osana internetiliikluse võrdset kohtlemist; pluralismi ja informatsiooni mitmekesisust; privaatsust; läbipaistvust ja

²⁸ EIK on rõhutanud, et tõlgendamise tulemus peab olema „praktiline ja efektiivne“. Vt täpsemalt: EIK, 5856/72, *Tyrer vs. Ühendkuningriik*, 25.04.1978, p 31; EIK, 6833/74, *Marckx vs. Belgium*, 13.06.1979, p 41. EIK, 7525/76, *Dudgeon vs. Ühendkuningriik*, 22.10.1981, p 23. EIK, 1474/62; 1677/62; 1691/62; 1769/63; 1994/63; 2126/64, *Case Relating to Certain Aspects of the Laws on the Use of Languages in Education in Belgium vs. Belgium*, 23.06.1978, p 5.

²⁹ Commission of the European Communities. *Towards a new framework for Electronic Communications infrastructure and associated services*. – The 1999 Communications Review. 1999/539, lk vi.

³⁰ Reed, lk 249.

³¹ Liiklusseadus. – RT I, 10.12.2020, 15.

³² Recommendation of the Committee of Ministers to member States on protecting and promoting the right to freedom of expression and the right to private life with regard to network neutrality. Committee of Ministers. 13.01.2016. CM/Rec (2016)1.

³³ Wu, T. *Network Neutrality, Broadband Discrimination*. – Journal of Telecommunications and High Technology Law 2003/2, lk 141.

vastutust.³⁴ 2015. aastal kehtestati samalaadsed eeskirjad andmeliikluse võrdseks ja mittediskrimineerivaks käsitlemiseks ka Euroopa Liidu tasandil määruses 2015/2120.³⁵

Võrguneutraalsuse reeglite rikkumise küsimus on üles kerkinud seoses Facebooki rakendusega Free Basics. Facebook pakub selle rakenduse vahendusel mõnes Aasia, Aafrika ja Lääne-Ameerika riigis eelkõige tasuta ligipääsu väikesele osale internetist. Rakendus lubab kasutada vaid Bingi otsingumootorit, kindlaid sponsoreeritud rakendusi, nagu näiteks ettevõtte Johnson & Johnson rahastatud rakendust, mis annab nõu beebiteemalistes küsimustes, ja populaarsetest sotsiaalmeediarakendustest vaid Facebooki.³⁶ Rakendus keelati ära Indias võrguneutraalsuse reeglite rikkumise tõttu 2016. aastal.³⁷ See ei tähenda, et keeldu oleks rakendatud kõigis riikides, kus Free Basics on jõudnud kanda kinnitada. Seda, kas rakendus vastab võrguneutraalsuse reeglitele, hakkavad riigid alles otsustama.

2.3. Sidusrühmi hõlmav otsustamine

Interneti puudutavat õigusnormistikku hakati rahvusvahelisel tasemel välja töötama alles 2003. aastal. Rahvusvaheline Telekommunikatsiooni Liit kutsus Šveitsis kokku infoühiskonna tippkohtumise³⁸, kus esmakordselt arutati interneti kiire kasvuga kaasnevaid probleeme ning moodustati töörühm, kelle ülesanne oli koostada raport, mis koondab soovitusi järgnevate sammude kohta.³⁹ Raport valmis aastal 2005 ning koos Tuneesia tegevuskavaga⁴⁰ sätestab see interneti haldamise alused. Just Tuneesia tegevuskava sätestab ka sidusrühmi hõlmava otsustamise põhimõtte, mis käib käsikäes interneti haldamisega.⁴¹ Sidusrühmi hõlmav otsustamine kui termin tähendab internetiressursside ühist haldamist asjakohaste rühmade poolt, kelleks on riikide valitsused, ettevõtted ning kodanikuühiskond, kellel kõigil on oma roll.⁴² Ka Euroopa Komisjon on kinnitanud, et „interneti-infrastruktuuri terviklikkuse ja pideva toimimise ning kasutajate usalduse ja interneti usaldatavuse säilitamiseks on vaja edendada riiklikku ja rahvusvahelist mitme sidusrühmaga koostööd“.⁴³

³⁴ Recommendation to member States on protecting and promoting the right to freedom of expression and the right to private life with regard to network neutrality. Committee of Ministers. 13.01.2016. CM/Rec(2016)1. Vt võrguneutraalsuse põhimõtte kohta ka Euroopa Parlamendi määruse (EÜ) nr 2015/2120 artiklit 3, millega nähakse ette avatud internetiühendust käsitlevad meetmed ning millega muudetakse direktiivi 2002/22/EÜ universaalteenuse ning kasutajate õiguste kohta elektrooniliste sidevõrkude ja -teenuste puhul ning määrust (EL) nr 531/2012, mis käsitleb rändlust üldkasutatavates mobiilsidevõrkudes liidu piires.

³⁵ Euroopa Parlamendi ja nõukogu määrus (EL) 2015/2120, 25. november 2015, millega nähakse ette avatud internetiühendust käsitlevad meetmed ning millega muudetakse direktiivi 2002/22/EÜ universaalteenuse ning kasutajate õiguste kohta elektrooniliste sidevõrkude ja -teenuste puhul ning määrust (EL) nr 531/2012, mis käsitleb rändlust üldkasutatavates mobiilsidevõrkudes liidu piires (EMP-s kohaldatav tekst), OJ L 310, 26.11.2015, p-d 1–18.

³⁶ Can Facebook Connect the Next Billion? – Advox 27.06.2017. –

<https://advox.globalvoices.org/2017/07/27/can-facebook-connect-the-next-billion/> (28.03.2021).

³⁷ Brandom, R. Mark Zuckerberg says Free Basics shutdown won't keep Internet.org out of India. – The Verge 08.02.2016. – <https://www.theverge.com/2016/2/8/10939594/mark-zuckerberg-internet-org-india-court-defeat-zero-rating> (28.03.2021).

³⁸ World Summit on the Information Society. Genf 2003. – <https://www.itu.int/net/ws/is/> (28.03.2021).

³⁹ Working Group on Internet Governance. Report of the Working Group on Internet Governance. Château de Bossey 2005. – <https://www.wgig.org/docs/WGIGREPORT.pdf> (28.03.2021).

⁴⁰ The Tunis Agenda for the Information Society 2005. Tunis: WSIS-05/TUNIS/DOC/6(Rev. 1)-E. – <http://www.itu.int/net/ws/is/docs2/tunis/off/6rev1.html> (28.03.2021).

⁴¹ Kulesza, J. International Internet Law (1. vlj). – New York: Routledge 2012, lk 138–139.

⁴² The Tunis Agenda for the Information Society 2005.

⁴³ Euroopa Nõukogu Ministrite Komitee. Ministrite Komitee soovitus liikmesriikidele Interneti universaalsuse, terviklikkuse ja avatuse kaitse ja edendamise kohta. 21.09.2011. CM/Rec(2011)8.

Aastatel 2013–2015 uuendas Majandusliku Koostöö ja Arengu Organisatsioon (OECD) oma julgeolekusuuniseid. Selleks kaasas OECD ettevõtete, kodanikuühiskonna, ametühingute ning interneti tehnilise kogukonna esindajad. 2015. aastal valmis OECD suunis „Digitaalse turvalisuse riskijuhtimine majandusliku ja sotsiaalse heaolu tagamiseks”⁴⁴, mida peetakse sidusrühmi hõlmava otsustamise tulemusel sündinud regulatsiooni heaks näiteks.

Üks sidusrühmade osapool on ka digitaalsetele õigustele pühendunud vabaühendused, nagu Article-19, Digital Rights Foundation, Privacy International, European Digital Rights, Electronic Frontiers Foundation ja Digital Freedom Fund. Just vabaühendused ning ajakirjandus täidavad internetiga seotud inimõiguste kaitstes tihti ühiskonna valvekoera rolli: nad juhivad tähelepanu riikide halvale praktikale, inimõigusi ohustavatele tehnoloogia kasutusviisidele ning arutelu all olevate seaduste murekohtadele.

3. Privaatsus, isikuandmete kaitse ja tehnoloogia

Mitmes meie kultuuriruumi inimõigusi käsitlevas põhidokumendis, nagu Euroopa inimõiguste ja põhivabaduste konventsioon⁴⁵, Euroopa Liidu põhiõiguste harta⁴⁶ ning Eesti Vabariigi põhiseadus⁴⁷, pole terminit *privaatsus* otsesõnu kasutatud. Selle asemel sätestavad Euroopa inimõiguste konventsioon (art 8), Euroopa Liidu põhiõiguste harta (art 7) ja Eesti põhiseadus (§-d 26, 33, 43) perekonna- ja eraelu ning kodu puutumatuse ja sõnumisaladuse kaitse.

Privaatsust mainitakse siiski eraldi mitmes teises inimõiguste kaitset käsitlevas olulises rahvusvahelises dokumendis, näiteks ÜRO inimõiguste ülddeklaratsioonis (artikkel 12). Selget privaatsuse definitsiooni otsides jääme aga hätta, sest privaatsuse mõiste ei ole üheselt defineeritud ning võib hõlmata mitmeid sotsiaalseid ning kultuurilisi mõõtmegi, samuti mõjutab õiguse piire näiteks tehnoloogia areng.⁴⁸ Selle peatüki autorid pooldavad laiahaardelist lähenemist, mille järgi kuuluvad privaatsusõiguse alla perekonna-, eraelu ning kodu puutumatus ja sõnumisaladuse kaitse.

Tuleb nentida, et tehnoloogia tormiline areng on kaasa toonud olukordi, kus nii Euroopa kui ka kodumaistel kohtutel on keeruline selgelt piiritleda sõnumisaladuse, perekonna- ja eraelu ning kodu puutumatuse kaitsealasid. Selge piiritlemise asemel liigub rahvusvaheline kohtupraktika paindlikuma lähenemise suunas, kus teatud inimõiguste vahel on nii tihe seos, et näiteks Euroopa Inimõiguste Kohus ei püüagi alati kaitsealasid eristada ning võib tunnistada mõlema õiguse üheaegset riivet.⁴⁹ Nimetatud õiguste kaitsealade ning tõlgendamise kohta on ohtralt kohtupraktikat.⁵⁰

⁴⁴ OECD. Digital Security Risk Management for Economic and Social Prosperity. Paris, 2005. – <https://www.oecd.org/publications/digital-security-risk-management-for-economic-and-social-prosperity-9789264245471-en.htm> (30.09.2021).

⁴⁵ Inimõiguste ja põhivabaduste kaitse konventsioon. – RT II 2010, 14, 54. Konventsioonile kirjutati alla 4. novembril 1950, see jõustus 3. septembril 1953. Konventsiooni on ratifitseerinud kõik 47 Euroopa Nõukogu liikmesriiki.

⁴⁶ Euroopa Liidu põhiõiguste harta 30.03.2010. – ELT C 83/02.

⁴⁷ Eesti Vabariigi põhiseadus. – RT I, 15.05.2015, 2.

⁴⁸ Privaatsusõiguse ulatust annab olemuslikult hästi edasi 1890. aastal avaldatud kuulus fraas, mille kohaselt tähendab see mõiste eelkõige „õigust olla jäetud üksi“. Warren, S. D., Brandeis, L. D. Right to privacy. – Harvard Law Review 1890–1891/4 (5), lk 193. Privaatsusõiguse kujunemise kohta vt Lõhmus, U. Põhiõigused kriminaalmenetluses. Tallinn: Juura 2014, lk 301–312.

⁴⁹ Lõhmus, lk 307.

⁵⁰ Euroopa Inimõiguste Kohtu kontekstis privaatsusõiguse ning digitaalse ajastu puutepunkte uuriv ülevaateartikkel: Çınar, Ö. H. The current case law of the European Court of Human Rights on privacy: challenges in the digital age. – The International Journal of Human Rights 2021/25 (1), lk 26–51.

Lisaks eespool nimetatud neljale inimõigusele – perekonna-, eraelu ning kodu puutumatus ja sõnumisaladuse kaitse – tuleb eraldi tähelepanu pöörata isikuandmete kaitse õiguslikule regulatsioonile. Esimene rahvusvaheline andmekaitsele keskendunud riikidevaheline leping oli isikuandmete automatiseeritud töötlemisel isiku kaitse konventsioon, mis võeti vastu 1981. aastal.⁵¹ Isikuandmete kaitset on mainitud ka Euroopa Liidu põhiõiguste harta artiklis 8. Samas tuleb märkida, et inimõigusena ei mainita isikuandmete kaitset ei Euroopa inimõiguste konventsioonis ega ka Eesti põhiseaduses. See aga ei tähenda, et isikuandmete kaitse oleks jäetud tähelepanuta ning isikud kaitseta. Näiteks Euroopa Inimõiguste Kohus on arvukates lahendites märkinud, et kuigi inimõiguste konventsiooni artikli 8 lõike 1 sõnastusest *expressis verbis* isikuandmete kaitset kui eraldiseisvat õigust ei leia, on ka isikuandmete kaitse küsimused artikli 8 kaitsealas.⁵²

Näiteks kohtuasjas *S. ja Marper vs. UK* leidis Euroopa Inimõiguste Kohus, et isikuandmete (antud juhul sõrmejälgede ning DNA näidiste) kogumist ning säilitamist olukorras, kus neid enam uurimiseks ei kasutatud, võib pidada artiklis 8 sätestatu rikkumiseks.⁵³ Euroopa Inimõiguste Kohus tuvastas artiklis 8 sätestatud nõude ebaproportsionaalse rikkumise ka kohtuasjas *Peck vs. Ühendkuningriik*. See puudutas juhtumit, kus meedias avaldati hagejast turvakaamerate poolt avalikus ruumis salvestatud video ilma tema nõusolekuta ja tema identiteeti varjamata.⁵⁴

Euroopa Liidu kõige olulisem isikuandmete kaitset reguleeriv dokument on Euroopa Parlamendi ja nõukogu isikuandmete kaitse üldmäärus, mis hakkas Euroopa Liidu liikmesriikides kehtima 2018. aastal.⁵⁵ Üldmäärus sisaldab mitu kesket põhimõtet, nagu näiteks õigus olla unustatud ja võimalikult väheste andmete kogumise põhimõte. Uudsenä on üldmääruses välja toodud õigus andmete ülekandmisele, profileerimisega seotud õigused ning ka lõimitud ning vaikimisi andmekaitse põhimõte, mida varasemast Euroopa Liidu õigusest sellisel kujul ei leia.

Nende põhimõtete sisustamine uute tehnoloogiate valguses on tõstatanud mitmeid õiguslikke küsimusi ka juba enne üldmääruse vastuvõtmist. Näiteks õigus olla unustatud tõusis terava tähelepanu alla 2014. aastal kohtuasjas *Google vs. AEPD ja Mario Gonzàles*. Euroopa Kohus leidis siis, et otsingumootorite haldajaid tuleb käsitada isikuandmete vastutavate töötajatena ning et kui isikuandmed on nende töötlemise kunagisi eesmärgi ning möödunud aega arvestades ülemäärased ning pole parajasti asjakohased, peab otsingumootori haldaja need isikuandmed otsingutulemuste seast kõrvaldama.⁵⁶

⁵¹ Isikuandmete automatiseeritud töötlemisel isiku kaitse konventsioon. – RT II 2001, 1, 3.

⁵² EIK, 44787/98, *P. G. ja J. H. vs. Ühendkuningriik*, 25.09.2001; EIK, 59842/00, *Vetter vs. Prantsusmaa*, 31.05.2005; EIK, 71611/01 *Wisse vs. Prantsusmaa*, 20.12.2005; EIK, 52019/07, *L. H. vs. Läti*, 29.04.2014.

⁵³ EIK, 30562/04, 30566/04, *S. ja Marper vs. Ühendkuningriik*, 04.12.2008.

⁵⁴ EIK, 44647/98, *Peck vs. Ühendkuningriik*, 28.01.2003.

⁵⁵ Euroopa Parlamendi ja nõukogu määrus (EL) 2016/679, füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus). Koos üldmäärusega võttis EL vastu ka direktiivi riigiasutustes isikuandmete õiguskaitse eesmärgil töötlemise kohta, millega kehtestatakse andmekaitse eeskirjad ja põhimõtted, mis reguleerivad isikuandmete töötlemist süütegude tõkestamise, uurimise, avastamise ja nende eest vastutusele võtmise või kriminaalkaristuste täitmisele pööramise eesmärgil. Euroopa Parlamendi ja nõukogu direktiiv (EL) 2016/680, mis käsitleb füüsiliste isikute kaitset seoses pädevates asutustes isikuandmete töötlemisega süütegude tõkestamise, uurimise, avastamise ja nende eest vastutusele võtmise või kriminaalkaristuste täitmisele pööramise eesmärgil ning selliste andmete vaba liikumist ning millega tunnistatakse kehtetuks nõukogu raamotsus 2008/977/JSK.

Inimõiguste omavahelised piirid on hõlgunud, aga riigid on arendanud digitaalse ühiskonna uute õiguspõhimõtete tõlgendusi. Näiteks arendas Saksa Liidukonstitutsioonikohus 1983. aastal uue põhiõigusena õiguse informatsioonilisele enesemääramisele. Selle kohaselt on isikul õigus teada tema kohta käivate andmete kogumisest ja otsustada oma andmete üle. Saksa Liidukonstitutsioonikohus sõnastas 2008. aastal veel ühe tehnoloogia arenguga tugevalt seotud põhiõiguse: õiguse infotehnoloogiasüsteemide konfidentsiaalsusele ja terviklikkusele.⁵⁷ Selle kohaselt võivad julgeolekuasutused varjatult jälgida IT-süsteemide kasutamist ning pääseda ligi salvestatud andmetele ainult siis, kui tegu on ohuga põhilistele õigushuvidele ning kohtu loal.

Pidades silmas uusi tehnoloogiaid, rõhutavad privaatsusõiguse kaitse tähtsust ka mitmed teised rahvusvahelised organisatsioonid. Näiteks on ÜRO inimõiguste ülemvoliniku büroo võtnud tähelepanu alla privaatsuse kaitse, pöörates eraldi tähelepanu tehnoloogia ja privaatsusega seotud teemadele, nagu massjälgimine, isikuandmete kaitse, DNA andmekogud, avaandmed ning suurandmed.⁵⁸ Alates 2013. aastast on ÜRO vastu võtnud mitu resolutsiooni pealkirjaga „Õigus eraelu puutumatusele digitaalajastul“⁵⁹, mis on tõmmanud rahvusvahelist tähelepanu tehnoloogia rollile inimõiguste kaitsmisel ning rikkumisel ning on märkimisväärne just oma globaalse haarde poolest. Teema olulisuse tõttu alustas ÜRO-s tegevust ka eraelu puutumatuse õiguse eriraportöör, kelle üks tööülesanne on koguda infot eraelu puutumatuse ja uute tehnoloogiatega seotud tavade ja kogemuste kohta, jagada ja edendada riikide parimaid tavasid ning tuvastada võimalikke murekohti. Valdkonna konkreetsem käsitlemine ÜRO tasandil on märk sellest, et teadlikkus inimõiguste ning tehnoloogia valupunktidest on riikides suurenenud, kuid samas jätkuvad mitmetes riikides just tehnoloogia toel selged inimõiguste rikkumised.

3.1. Isikuandmete kaitse

Isikuandmete kaitse on tehnoloogia arenguga muutunud üha olulisemaks. Aastatega on Euroopa Liidu regulatsioon arenenud aina nüansirikkamaks ning samas mõjutanud ka teiste regioonide ning riikide andmekaitseõiguse arengut (nn Brüsseli efekt).⁶⁰

Eelmises alapeatükis mainisime, et Euroopa Liidu keskne isikuandmete kaitsele pühendatud instrument on Euroopa Liidu isikuandmete kaitse üldmäärus. Üldmääruse kohaselt vastutab isikuandmete „vastutav töötleja“ selle eest, et isikuandmete töötlemisel jälgitaks üldmääruses sätestatud põhimõtteid⁶¹, olenemata sellest, milliseid tehnoloogiaid on isikuandmete töötlemisel kasutatud. Kuivõrd isikuandmete kaitsega seotud õiguslikke küsimusi on rohkem, kui siin peatükis jõuame katta, toome järgnevalt kolm näidet üldmääruse rakendamisel tekkinud küsimuste kohta.

⁵⁶ EK, C-131/12, Google Spain SL ja Google Inc. vs. Agencia Española de Protección de Datos (AEPD) ja Mario Costeja González, ECLI:EU:C:2014:317.

⁵⁷ BVerfG, 1 BvR 370/07 ja 1 BvR 595/07. 27.02.2008. –

https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2008/02/rs20080227_1bvr037007.html (19.12.2021). Nimetatud õigus on eesti keelde tõlgitud ka kui „õigus infotehnoloogiasüsteemide konfidentsiaalsusele ja puutumatusele“; vt ka Lõhmus, lk 305.

⁵⁸ ÜRO inimõiguste ülemvoliniku büroo. Privaatsuse eriraportöör. –

<https://www.ohchr.org/EN/Issues/Privacy/SR/Pages/SRPrivacyIndex.aspx>, (28.03.2021).

⁵⁹ Viimati: ÜRO Peaassamblee. Resolution on the right to privacy in the digital age. A/HRC/RES/42/1. 26.09.2019.

⁶⁰ Bradford, A. The Brussels Effect: How the European Union Rules the World. – New York: Oxford University Press 2020.

Isikuandmete kaitse üldmäärus, artikkel 5, p 2.

⁶¹ Isikuandmete kaitse üldmäärus, artikkel 5, p 2.

Esiteks on uute tehnoloogiate puhul keeruline määratleda, kas kogutavad ja töödeldavad andmed kuuluvad isikuandmete kaitse üldmääruse mõistes isikuandmete alla või millal on need n-ö piisavalt anonüümseks muudetud ning seeläbi üldmäärus neile ei kohaldu. Näiteks IP-aadresside puhul leidis Euroopa Kohus, et nii staatilised kui ka dünaamilised IP-aadressid võivad olla üldmääruse mõistes isikuandmed, sest need võivad viia füüsilise isiku tuvastamiseni, kes nimetatud IP-aadressi kasutab.⁶² Samas on endiselt ebaselge, kas näiteks plokiahela tehnoloogias kasutatavad räsid vastavad samuti üldmääruse isikuandmete definitsioonile või tuleks neid käsitada anonüümitud teabena.⁶³ See omakorda mõjutab otseselt tehnoloogia- ja teenusepakkujate õigusi ja kohustusi ning samal ajal ka tehnoloogiate kasutajate kaitset.

Teise näitena saab tuua suurandmed ning tehisintellekti kasutamisega seotud küsimused. Siin on peamised õiguslikud probleemid seotud töödeldavate isikuandmete mahu ja mitmekesisuse ning töötlemise tingimuste ja tulemustega. Näiteks võib olla keeruline kindlaks määrata andmete omanikku, kui kogutakse ja töödeldakse suuri andmekogusid, mis koosnevad mitmestest allikatest ning on salvestatud erineval kujul ning mille töötlemine ei pruugi alati toimuda algselt määratud eesmärkidel. Samuti võib probleeme tekitada vastutava ja volitatud töötleja kindlaksmääramine ning täpsete volituste ning kohustuste defineerimine, kui andmeid töötlevad nutikad masinad ja tarkvara. Oluline on ka otsustada, millistel eesmärkidel võidakse tulemusi kasutada ning kuidas õiguslikult käsitleda tehisintellekti tehtud otsuseid, mis põhinevad tehisintellekti enda välja töötatud andmetöötlusel.⁶⁴

Kolmandaks, uute tehnoloogiate igapäevane kasutuselevõtt tekitab erinevaid arusaamu isikuandmete töötlemise lubatavuse kohta. Isikuandmete kaitse üldmäärus nimetab ühe töötlemise alusena andmesubjekti nõusolekut. Üldmääruse kohaselt peab nõusolek olema antud viisil, millega andmesubjekt kinnitab „vabatahtlikult, konkreetselt, teadlikult ja ühemõtteliselt nõusoleku teda puudutavate isikuandmete töötlemiseks“.⁶⁵ Sotsiaalmeedia, mitmesuguste elektrooniliste teenuste ning tehnoloogiate kontekstis saab aga küsida, kas nõusolek andmete töötlemiseks vastab alati üldmääruses nimetatud tingimustele. Kas andmesubjekti nõusolek on vabatahtlik ehk kas andmesubjekt on saanud valida (nt kas ta soovib personaliseeritud reklaame)? Kas nõusolek on konkreetne ja teadlik ehk kas andmesubjekt kui teenuse kasutaja mõistab täiel määral, kuidas kasutatakse tema andmeid või kellele neid edastatakse (nt mis tingimustel saavad andmetele ligipääsu kolmandad isikud või riigid)? Andmesubjekti teadlikkus on seotud ka läbipaistvuse nõudega, mille kohaselt peab vastutav töötleja teavitama andmesubjekti tema isikuandmete töötlemise viisidest ning eesmärkidest „kokkuvõtlikult, selgelt, arusaadavalt ning lihtsasti kättesaadavas vormis, kasutades selget ja lihtsat keelt“⁶⁶, mille rakendamine keeruliste tehnoloogiliste lahenduste puhul võib osutuda väljakutseks.

3.2. Sideandmete säilitamine

Inimõiguste kaitse ja turvalisuse tagamise vahel tasakaalu leidmine on alati olnud keeruline ülesanne ning tehnoloogia kiire areng võib kaalukaasi veelgi enam uppi lüüa.

⁶² EK, C-582/14, Patrick Breyer vs. Saksamaa, ECLI:EU:C:2016:779.

⁶³ Finck, M., Pallas, F. They who must not be identified – distinguishing personal from non-personal data under the GDPR. – International Data Privacy Law 2020/10 (1).

⁶⁴ Loe lähemalt: Euroopa Liidu Põhiõiguste Amet ja Euroopa Nõukogu. Euroopa andmekaitseõiguse käsiraamat. – Luxembourg: Euroopa Liidu Väljaannete Talitus 2020, pkt 10.

⁶⁵ Isikuandmete kaitse üldmäärus, preambuli p 32.

⁶⁶ Isikuandmete kaitse üldmäärus, artikkel 12 lg 1.

Ilmekas näide selle kohta on pikalt kestnud debatt sideandmete säilitamise tingimuste üle. Nimelt kuulutas Euroopa Kohus 2014. aastal Euroopa Liidu sideandmete säilitamise direktiivi 2006/24 kehtetuks.⁶⁷ Euroopa Kohus küll nentis, et sideandmete säilitamine on eesmärgipärane kuritegevuse ja kuritegude, eriti organiseeritud kuritegevuse ennetamisel, uurimisel, avastamisel ja kohtus menetlemisel, kuid leidis, et direktiiv hõlmas üldistatult kõiki isikuid ning kõiki elektroonilise side vahendeid ja liiklusandmeid, ilma et raskete kuritegude vastu võitlemise eesmärki arvestades oleks ette nähtud mingit eristamist, piirangut või erandit.⁶⁸ Seega puudusid direktiivis reeglid, mis reguleeriksid Euroopa Liidu põhiõiguste harta artiklites 7 ja 8 ette nähtud inimõiguste riive ulatust, ning kohus tõdes, et direktiiv tõi kaasa Euroopa Liidu õiguskorras nende inimõiguste ulatusliku ja väga raske riive, ilma et see riive oleks täpselt piiritletud sätetega, mis lubaksid tagada, et riive piirdub vaid vältimatult vajalikuga.⁶⁹ Samuti ei näinud direktiiv muu hulgas ette piisavalt garantiisid, mis võimaldaksid tagada säilitatavate andmete tõhusa kaitsmise juhuks, kui keegi soovib salvestatud andmeid kuritarvitada.⁷⁰ Kohtule ei olnud meelepärane veel see, et direktiiv ei nõudnud andmete säilitamist EL-i territooriumil ning seetõttu ei saanud pidada täiel määral tagatuks, et vajalikke andmekaitse ja andmeturbega seotud nõuete täitmist saab kontrollida sõltumatu asutus.⁷¹

Euroopa Kohus on neid küsimusi arutanud ka hiljem ning kinnitas ka 2016. aastal, et liikmesriigid võivad kehtestada õigusnormistiku, mis võimaldab raske kuritegevuse vastu võitlemise eesmärgil ennetavalt säilitada liiklus- ja asukohaandmeid, kui säilitatavate andmete liigid, asjasse puutuvad sidevahendid ja isikud ning säilitamise kestus on piiratud rangelt vajalikuga ning kui on tagatud, et riigi pädevatele ametiasutustele antakse juurdepääs säilitatavatele andmetele ainult rangelt vajalikus ulatuses.⁷² Ka rõhutas kohus andmetele juurdepääsu saamise eeltingimusena kohtu või sõltumatu haldusasutuse eelneva kontrolli vajalikkust, mis tehakse juurdepääsu taotleva asutuse põhjendatud taotluse alusel, mis omakorda on ennekoike esitatud kuriteo ennetamise, avastamise või menetlemise raames.⁷³ Samasuguse tulemuseni jõudis kohus ka 2020. aastal käsitletud asjades, kui leidis, et üldine sideandmete säilitamine ei ole EL-i õigusega kooskõlas, kuigi on võimalikud erandid: sideandmeid võib säilitada näiteks riigi julgeoleku kaalutlustel ja kindla aja jooksul, kui säilitamine on valikuline ja piiratud, või kui andmed puudutavad konkreetset rasket kuritegu või terrorirünnakut.⁷⁴

Vaatamata eespool nimetatud Euroopa Kohtu otsustele kehtis Eestis endiselt õigusnormistik, mis kohustas teenuseosutajaid säilitama aasta aega kõigi kasutajate sideandmed (näiteks sideseansi algus ja lõpp, kasutatud teenus, kellega ühendust peeti jne) ning need seaduses sätestatud tingimustel edastama riigi uurimis-, jälitus- või julgeolekuasutustele, prokuratuurile, kohtule või teistele seaduses määratud asutustele.⁷⁵ Olukord muutus alles pärast Euroopa Kohtu 2021. aastal tehtud otsust. Selles otsuses täpsustati, et üldine sideandmete säilitamine on EL-i õigusega vastuolus, kui sideandmetele juurdepääs ei piirdu

⁶⁷ EK, C-293/12, Digital Rights Ireland and Seitlinger and Others, ECLI:EU:C:2014:238.

⁶⁸ *Ibid.*, p-d 43 ja 57.

⁶⁹ *Ibid.*, p 65.

⁷⁰ *Ibid.*, p 66.

⁷¹ *Ibid.*, p 68.

⁷² EK, C-203/15, Tele2 Sverige, ECLI:EU:C:2016:970, p-d 110, 115, 116, 118, 119.

⁷³ *Ibid.*, p 120.

⁷⁴ EK, C-623/17, Privacy International vs. Secretary of State for Foreign ja Commonwealth Affairs jt, ECLI:EU:C:2020:790.; EK, C-511/18, La Quadrature du Net jt vs. Premier minister jt, ECLI:EU:C:2020:791.

⁷⁵ Elektroonilise side seadus. – RT I, 22.10.2021, 15, § 111¹.

menetlustega, mille eesmärk on võitlus raske kuritegevuse vastu või avalikku julgeolekut ähvardava suure ohu ärahoidmine, ning olenemata sellest, millise ajavahemiku andmetele on juurdepääsu taotletud ning olenemata selle ajavahemiku kohta kättesaadavate andmete hulgast ja liigist ning samuti siis, kui puudub kohtu või sõltumatu haldusasutuse eelnev kontroll.⁷⁶ Seejärel otsustas Riigikohus, et Eestis kehtiv andmete laussäilitamine ning nende andmete kasutamist reguleeriv kord on vastuolus EL-i õigusega ning seetõttu on välistatud kriminaalmenetluse eesmärkidel sideandmete säilitamine ja kasutamine nii kaua, kuni Eesti pole viinud oma sellekohast õigusnormistikku vastavusse EL-i õigusega.⁷⁷

3.3. Jälitustoimingud

Ulatuslikud inimõiguste, sealhulgas sõnumisaladuse kaitse riived võivad kaasneda ka jälitustoimingutega⁷⁸, mille läbiviimise vahendid ja võimekus kasvavad tehnoloogia arenguga samas rütmis. Eraldi tuleb käsitleda piiratud isikustatud jälgimist ning tehnoloogia arenguga võimalikuks saanud elektroonilist lausjälgimist.

Euroopa Inimõiguste Kohus on kohtuasjas *Klass jt vs. Saksamaa* rõhutanud, et salajane jälgimine, sealhulgas kommunikatsiooni jälgimine, tuleb tasakaalustada tõhusate ja piisavate tagatistega võimalike kuritarvituste vastu ning et üksikisikute lausjälgimist ei saa õigustada luure- ning terrorismivastase võitlusega.⁷⁹ Sarnase seisukoha on Euroopa Inimõiguste Kohus võtnud kohtuasjas *Szabó ja Vissy vs. Ungari*. Kohus on öelnud, et ka terrorismikuritegude ärahoidmisel ja avastamisel peab kommunikatsiooniandmete töötlemine olema vältimatult vajalik selle eesmärgi saavutamiseks ja seaduses tuleb sätestada tingimused, mis õigustavad konkreetse ohu tõrjumiseks konkreetsete isikute sõnumite saladuse riivet, mitte aga lubama sekkumist määratlemata hulga inimeste kommunikatsiooniandmetesse.⁸⁰

Euroopa Inimõiguste Kohus kinnitas kohtuasjas *Kopp vs. Šveits*, et sõnumisaladuse piiramise juhud ja kord peavad olema täpselt ja arusaadavalt sätestatud seaduses.⁸¹ Kohtuasjas *Weber ja Saravia vs. Saksamaa* analüüsis kohus Saksamaal kehtinud telekommunikatsiooni pealtkuulamise korda ning lisas täpsustusena kuus kaitsemeedet isikustatud jälgimise kohta kriminaalmenetluses. Kohtu hinnangul tuleb õigusnorme sätestades arvestada, 1) milliste süütegude puhul võib jälitustegevust kasutada; 2) milliste isikute suhtes võib jälitustegevust teostada; 3) millised on piirangud jälitustegevuse kestusele; 4) milline on saadud andmete uurimise, kasutamise ja säilitamise kord; 5) millised on ettevaatusabinõud andmete teistele isikutele edastamise korral; 6) milline on jälitustegevusega saadud andmete kustutamise ja hävitamise kord. Pärast põhjalikku analüüsi leidis kohus, et hagejate vaidlustatud pealtkuulamine oli riigi määratud eesmärgi arvestades demokraatlikus ühiskonnas vajalik.⁸²

Kohtuasjas *Roman Zakharov vs. Venemaa* rõhutas Euroopa Inimõiguste Kohus, et mobiiltelefonikõnede salajast pealtkuulamist reguleerivad normid peavad andma üksikisikule

⁷⁶ EK, C-746/18, Prokuratuur (Conditions d'accès aux données relatives aux communications électroniques), ECLI:EU:C:2021:152.

⁷⁷ RKKK, 1-16-6179, 18.06.2021, p 105.

⁷⁸ Jälitustoiminguid võidakse Eestis teha kriminaalmenetluse seadustiku, julgeolekuasutuste seaduse või Kaitseväe korralduse seaduse alusel. Loe täpsemalt: Jaanimägi, K., Oja, L. Paragrahv 26. – Madise, Ü. *et al.* (toim). Eesti Vabariigi põhiseadus. Kommenteeritud väljaanne, p 23.

⁷⁹ EIK, 5029/71, *Klass jt vs. Saksamaa*, 06.09.1978.

⁸⁰ EIK, 37138/14, *Szabó ja Vissy vs. Ungari*, 12.01.2016; loe täpsemalt: Laos, Sepp, p 25.

⁸¹ EIK, 13/1997/797/1000, *Kopp vs. Šveits*, 25.03.1998.

⁸² EIK, 54934/00, *Weber ja Saravia vs. Saksamaa*, 29.06.2006.

võimaluse kindlaks teha, kas tema kõnesid on pealt kuulatud, ning üksikisikul peab olema juurdepääs õiguskaitsevahenditele.⁸³

Jälitustoimingute puhul võib ristuda eraelu puutumatuse kaitsealaga ka sõnumisaladuse kaitseala. Kuivõrd Eesti põhiseaduse järgi on sõnumisaladusse sekkumine rohkem piiratud kui perekonna- ja eraelu sekkumine, on Riigikohus korduvalt käsitlenud kahe kaitseala piiritlemise küsimust. Riigikohus on leidnud, et sõnumisaladuse kaitsealas on vaid need sõnumid, mis on parajasti kommunikatsiooniprotsessis, ning isiku valduses olev ülejäänud informatsioon, nagu e-kiri või selle mustand, on kaitstud põhiseaduse §-ga 26.

Eraelu kaitsealasse kuuluvad ka sõnumi metaandmed, millest ei selgu sõnumi sisu.⁸⁴ Kohus põhjendas seda sellega, et sõnumi teeloleku ajal, kui sõnum on väljunud saatja valdusest ning pole veel adressaadini jõudnud, on sõnum isiku mõjusfäärist väljas ning ta ei saa seda kolmandate isikute eest kaitsta.⁸⁵ Interneti vahendusel edastatud sõnumid on teel vaid väga lühikest aega ning seetõttu leiavad sõnumisaladuse mõiste laiema tõlgenduse pooldajad, et saatmisele kuuluvad ja kohale jõudnud sõnumid väärivad samaväärset kaitset nagu kommunikatsiooniprotsessis olevad sõnumid. Kuidas näiteks oleks muidu kaitstud e-kiri, mille saatja on välja saatnud ning ootab lugemist, olles salvestatud teenusepakkuja serverisse? Või kuidas on kaitstud e-kiri, mida meelega pole välja saadetud, vaid mis ootab lugemist e-kirja kontol, millele võib ligi pääseda igaüks, kes teab õiget kasutajanime ja parooli? Seega ei tohiks sõnumi kaitse sõltuda sellest, kas sõnum on tehtud saajale kättesaadavaks, vaid sellest, kas isik soovib sõnumi sisu jätta avalikustamata. Sõnumisaladuse kaitseala laiemat tõlgendust toetavad ka Euroopa inimõiguste konventsiooni ja harta sõnastus ja rakenduspraktika.⁸⁶

Jälitustoiminguid võivad elektroonilisi vahendeid kasutades teha ka luure- või julgeolekuasutused ning mitmetest lahvatanud skandaalidest teame, et mitte ainult riigisiselt.⁸⁷ Rahvusvaheline õigus riikidevahelist luuretegevust otseselt ei keela, küll aga võib rahvusvahelist õigust rikkuda viis, kuidas luuretegevust läbi viiakse. Seejuures pole oluline, kas tegu on n-ö traditsiooniliste vahendite abil tehtud või küberluurega (*cyber espionage*).

Küberluures kasutatakse mitmesuguseid viise, kuidas andmeid koguda ka teise riigi territooriumil viibimata. Näiteks võib mõne toote tootmisel riistvarasse sisestada koodi, mis muudab võimalikuks riistvara kaugjälgimise. Samuti võib konkreetsete isikute seadmete operatsioonisüsteemid nakatada pahavaraga, mille abil saab ligi seadmetesse salvestatud andmetele või pealt kuulata seadmete kaudu toimuvat suhtlust. Lisaks võib kasutada andmepüüki ehk kalastamisrünnet, et kätte saada salasõnad, mille abil süsteemidesse sisenedes varjatult vajalikku infot koguda. Oluline on, et teatud elemendid, nagu näiteks tekitatud füüsiline kahju või operatsioonisüsteemide toimimise halvamine, võivad kätkeda rahvusvahelise õiguse reeglite (näiteks suveräänsuse või mittesekkumise printsiibi) rikkumist.⁸⁸

⁸³ EIK, 47143/06, Roman Zakharov vs. Venemaa, 04.12.2015.

⁸⁴ RKKK, 3-1-1-51-14, 23.02.2015, p 21.

⁸⁵ RKKK, 3-1-1-14-14, 30.06.2014, p-d 816 ja 817; loe täpsemalt: Laos, Sepp, p 5.

⁸⁶ Laos, Sepp, p 6.

⁸⁷ Näitena võib tuua vihjeandja Edward Snowdeni 2013. aastal avaldatud materjalid, mille kohaselt oli USA riiklikul julgeolekuametil väidetavalt lausjälgimise jaoks ligipääs suurte IT-firmade serveritele ning võimekus valguskaabli kaudu inimesi pealt kuulata ja krüptograafilisi võtmeid murda. Loe täpsemalt: MacAskill, E. *et al.* NSA Files Decoded: Edward Snowden's Surveillance Revelations Explained. – The Guardian 01.11.2013.

⁸⁸ Schmitt, M. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. – Cambridge: Cambridge University Press 2017, lk 168–174.

Huvipakkuvad on hiljutised Euroopa Inimõiguste Kohtu otsused, mis puudutavad riikide massilise signaaliluure⁸⁹ regulatsiooni ning elektroonilist lausjälgimist. Näiteks hindas Euroopa Inimõiguste Kohtu suurkoda kohtuasja *Centrum för Rättvisa vs. Rootsi* otsuses, et arvestades ohte, millega riigid peavad silmitsi seisma, ning seda, et nende tegude toimepanijad ning osalised kasutavad suhtluseks internetti ning samas püüavad oma internetisuhtluse jälgimist takistada kõrgetasemelise tehnoloogiaga, on riikidel kaalutlusõigus otsustada, millist süsteemi vajab riik julgeolekuohtude väljaselgitamiseks ning turvalisuse tagamiseks. Kohus analüüsis mitme kriteeriumi alusel, kas õigusaktides, millele toetudes signaaliluure teel jälgitakse sidekanalite kaudu edastatavat kommunikatsiooni ja metaandmeid, on ette nähtud piisavalt kaitsemeetmeid, et kaitsta elanikke võimalike riigipoolsete kuritarvituste eest.

Olulise arenguna möönis Euroopa Inimõiguste Kohus, et pidades silmas tehnoloogia arengut, tuleb sideandmete massjälgimise hindamisel arvestada tavalisele isikustatud jälgimisele kohaldatavaid põhimõtteid, mida kohus oli sätestanud eespool mainitud *Weber ja Saravia vs. Saksamaa* kohtuasjas. Lisaks täpsustas kohus elemente, mida riigisisene õigusnormistik peab nii sideandmete kui ka sideandmetega seotud andmete massjälgimisel kajastama. Kuigi kohus kiitis üldiselt heaks Rootsi lausjälgimist reguleeriva õigusnormistiku, tuvastati ka kolm puudujääki: 1) puudusid selged reeglid selle kohta, kuidas hävitada andmeid, mis ei sisalda isikuandmeid; 2) õigusnormistik, mis puudutas kogutud andmete jagamist kolmandate riikidega, puudus viide üksikisiku privaatsuse olulisusele; 3) puudus toimiv *ex post facto* kontroll. Sellest lähtuvalt otsustas kohus, et Rootsi õigusnormistik rikub Euroopa inimõiguste konventsiooni artiklis 8 sisalduvat privaatsusõigust.⁹⁰

Sarnaseid küsimusi käsitleti ning samasugust lähenemist kohaldati Euroopa Inimõiguste Kohtu asjas *Big Brother Watch jt vs. Ühendkuningriik*, milles suurkoda otsustas, et Suurbritannia on üksikisikute lausjälgimisega rikkunud konventsiooni artikleid 8 ja 10. Kohus viitas artikli 8 rikkumist tuvastades kolmele puudujäägile: massjälgimise loa andja ei olnud täitevvõimust sõltumatu; sideandmete massjälgimise luba ei sisaldanud piisavaid otsingukriteeriume; konkreetse isikuga seotud otsingukriteeriumidele ei pidanud eelnevalt taotlema luba.⁹¹

Kuigi seda Euroopa Inimõiguste Kohtu otsust saab pidada inimõiguste kaitsele pühendunud organisatsioonide suureks võiduks, sest mõlema otsuse kohaselt tuvastas kohus artikli 8 rikkumise, kardavad kriitikud, et seesuguste otsustega normaliseeritakse lausjälgimine, sest lausjälgimist ennast ei peetud ebaproportsionaalseks.⁹² Seoses piiriüleste jälitustoimingute lubatavusega tuleb eraldi ära märkida murranguline Saksa Liidukonstitutsioonikohtu otsus,

⁸⁹ Üldtermin, mille alla käib elektrooniline ja sideluure. Enim kasutatavad elektroonilise side võrgud on andmeside-, mobiiltelefoni-, kaabelvõrk ja elektrikaablisüsteem. Signaaliluure erineb tavapärasest varjatud jälgimisest selle poolest, et on ennetava iseloomuga ning tihti vähem piiritletud, samuti ei pruugi see olla suunatud ainult sisejulgeolekule. Suurel hulgal sõnumite sisu puudutavaid andmeid ning metaandmeid kogutakse eri viisil ning analüüsitakse arvutite abil valitud kriteeriumide järgi. Filtreerimise aluseks võivad olla inimeste nimed, keeled, võtmesõnad, kommunikatsiooni teekonnad ja teised tehnilised andmed. Loe täpsemalt: Euroopa Nõukogu, Venice Commission Report on the Democratic Oversight of Signals Intelligence Agencies, 2015. – [https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD\(2015\)011-e](https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2015)011-e) (24.10.2021).

⁹⁰ EIK, 35252/08, *Centrum för Rättvisa vs. Sweden*, 25.05.2021.

⁹¹ EIK, 58170/13, 62322/14 ja 24960/15, *Big Brother Watch jt vs. Ühendkuningriik*, 25.05.2021.

⁹² Milanovic, M. The Grand Normalization of Mass Surveillance: ECtHR Grand Chamber Judgments in *Big Brother Watch* and *Centrum för rättvisa*. – EJIL:Talk! 26.05.2021. – <https://www.ejiltalk.org/the-grand-normalization-of-mass-surveillance-ecthr-grand-chamber-judgments-in-big-brother-watch-and-centrum-for-rattvisa/> (13.09.2021).

mille kohaselt peab ka piiriüleste jälitustoimingute tegemine olema kooskõlas Saksamaa põhiseadusega. Liidukonstitutsioonikohtu otsusega tunnistati seega 2020. aastal kehtinud vastav regulatsioon õigusvastaseks.⁹³

3.4. Läbiotsimine

Tehnoloogia levik ja areng on muutnud ka teiste kriminaalmenetluses tõendite kogumiseks kasutatavate toimingute tegemist. Näiteks ei sisalda Eesti õigus elektrooniliste teabekandjate läbiotsimise käigus äravõtmise ja läbivaatuse kohta eriregulatsiooni.⁹⁴ Teabekandja äravõtmine eraldivõetuna ei riiva sõnumisaladust, kuid üldjuhul on toimingu eesmärk saada teada edastatud sõnumite sisu, mistõttu on teabekandja äravõtmine vähemalt puutumuses sõnumisaladusega. Samuti võib teabekandja uurimine tekitada mitmeid küsimusi, nagu läbiotsitavate andmete mahu piiritlemine ning läbiotsimisest teavitamine.⁹⁵ Seetõttu ei ole kehtivate õigusnormide tõlgendamine üheselt arusaadav. See toob kaasa õigusliku ebaselguse, avara tõlgendamise- ning tegutsemisruumi, sealhulgas ka inimõiguste kaitse suhtes. Kuna tänapäeval vahetatakse sõnumeid valdavalt elektrooniliste sidevahendite kaudu ning palju andmeid salvestatakse elektroonilistele andmekandjatele, tekib õigustatud ootus, et tehnoloogia arengut arvestades tuleks ajakohastada ka kriminaalmenetluse vastava sisuga õigusnormistik.⁹⁶

Olulise aspektina tuleb vaadelda ka andmete asukoha problemaatikat, sest aina rohkem tekib olukordi, kus kohtueelses menetluses kogutavad tõendid ei asu asja menetleva riigi territooriumil või polegi nende füüsilist asukohta võimalik tuvastada. Näitena võib tuua pilvetehnoloogiad, kus andmete salvestamine ainult kasutaja koduriigi territooriumil on pigem erand kui reegel ning kus peegeldatud andmebaaside, eri serverite ning rakenduste tõttu ei suuda tihti peale isegi teenuse osutajat täielikult identifitseerida andmete tegelikku asukohta.

Elektrooniliste tõendite kogumisel võidakse kriminaalmenetluses kasutada nn kaugläbiotsimist, mida tehakse (arvuti)süsteemis ning mida laiendatakse selle (arvuti)süsteemi kaudu teistesse, mujal asuvatesse (arvuti)süsteemidesse või mida tehakse kriminaalmenetlust teostava uurimisasutuse (arvuti)süsteemi kaudu. Selline otsene ligipääs andmetele on märksa kiirem kui traditsiooniline rahvusvaheline kriminaalkoostöö, kuid võib lisaks teise riigi suveräänsuse rikkumisele tekitada küsimusi ka üksikisiku inimõiguste kaitse kohta.

4. Väljendusvabadus tehnoloogiaajastul: kaitseala ja kontekst

Väljendusvabaduse legaalseadus on sätestatud Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artiklis 10. Euroopa Inimõiguste Kohus on kirjeldanud sõnavabadust kui „ühiskonna põhialust ja üht põhilist tingimust demokraatliku ühiskonna edendamiseks ja iga inimese arenguks”.⁹⁷ Eesti Vabariigi põhiseaduses on sätestatud sõnavabadus §-s 45 igaühe õiguse ja vabadusena levitada ideid, arvamusi, veendumusi ja muud informatsiooni sõnas, trükis, pildis või muul viisil. Euroopa inimõiguste konventsiooni artikli 10 kohaselt käteb see

⁹³ BVerfG, 1 BvR, 2835/17, 19.05.2020.

⁹⁴ Kuigi KrMS § 91 ei nimeta otsesõnu teabekandjat kui läbiotsimise objekti, võidakse läbiotsimise käigus teabekandjad (nt arvuti kõvaketas, e-kirja väljatrükk, mobiiltelefon) ära võtta ning rakendada vaatlust. Kriminaalmenetluse seadustik. – RT I, 08.07.2021, 9.

⁹⁵ Lõhmus, lk 312–313.

⁹⁶ Laos, Sepp, p 15; Lõhmus, lk 312–313.

⁹⁷ EIK, 5493/72 Handyside vs. Suurbritannia, 07.12.1976, p 49.

õigus vabadust oma arvamusele ja vabadust nii levitada kui ka saada teavet ja ideid ilma võimude sekkumiseta ja sõltumata riigipiiridest.

Väljendusvabaduse kui inimõiguse esemeline kaitseala hõlmab nii teavet, arvamusi kui ka mõtteid ja kohaldub mitte ainult ideedele ja informatsioonile⁹⁸, mida võetakse vastu meelsasti või mida peetakse mitteründavaks või mis jätab ükskõikseks, vaid ka neile ideedele, mis solvavad, šokeerivad ja häirivad riiki või ükskõik millist osa rahvastikust.⁹⁹ Sellised on pluralismi, tolerantsuse ja avatud mõtlemise nõuded, ilma milleta ei oleks demokraatlikku ühiskonda.¹⁰⁰

Isikulise kaitseala moodustab nii üksiksiku õigus ja vabadus kui ka juriidilise isiku, sealhulgas meediaorganisatsiooni õigus ja vabadus (nn pressivabadus). Väljendusvabaduse inimõigust iseloomustab tõik, et Euroopa inimõiguste konventsioon ning Euroopa Liidu põhiõiguste harta seavad lisakriteeriumi „sõltumata riigipiiridest“. Arusaadavalt on see kriteerium õiguslikult keeruline, kuna kehtib riikide suveräänsuse põhimõte ja arusaam, et riigi õiguskorral ei ole mõju väljaspool selle territooriumi. Näiteks Prantsusmaal kehtinud seadus, mis andis Prantsusmaa siseministrile õiguse rakendada üldist ja absoluutset levitamise ja müügikeeldu iga välismaist päritolu dokumendi kohta, oli Euroopa Inimõiguste Kohtu hinnangul otseses vastuolus konventsiooni artikliga 10, mis tunnustab artiklis sätestatud õigusi olenemata riigipiiridest.¹⁰¹

Tehnoloogia on loonud väljendusvabaduse kasutamisele uued võimalused, aga ka proovikivid. Euroopa Inimõiguste Kohus on selgitanud, et väljendusvabaduse mõju on tehnoloogia tõttu võimendatud, arvestades seda, kui kergesti, ulatuslikult ja kiiresti teave internetis levib ning kui visalt jääb püsima kord juba avaldatud teave¹⁰² ning millises ulatuses kontrollivad tehnoloogilisi võimalusi eraõiguslikud isikud. Seetõttu on tehnoloogiat arendavatel ja kasutatavatel ettevõtetel nagu riikidelgi kohustus ja vastutus austada, kaitsta, järgida ja teostada inimõigusi.

4.1. Väljendusvabadus, internet ja internetiteenuse osutajad

Internet on oluline vahend inimeste igapäevategevuses (kommunikatsioon, teave, teadmised, äritehingud) ning sellest lähtuvalt tekib õiguspärane ootus, et internetiteenused on kättesaadavad ja taskukohased, turvalised, usaldusväärsed ja püsivad. Internetikasutajal peaks olema internetiühendus, mis on taskukohane ja mittediskrimineeriv.¹⁰³ Arvestades interneti

⁹⁸ Esemeline kaitseala hõlmab ka „muud informatsiooni“, mis viitab sellele, et väljendus peab sisaldama informatsiooni ehk teisisõnu, kui ideedes, arvamustes, veendumustes informatsiooni ei ole, siis see väljendusvabaduse kaitse alla justkui ei kuuluks. Selline tõlgendus oleks ilmselt liialt kitsendav, sest jätaks välja mitmed väljendusvormid, muljed ja hinnangud, mille informatiivsus on ebaselge, või ideed ja arvamused, mille informatiivsus võib ilmnedas alles tulevikus, ning jätab ka selgusetuks, kes ja kuidas informatiivsust hindab. Põhiõiguste esemelise kaitseala määratlemisel tuleb lähtuda laiendava tõlgendamise põhimõttest. Asjakohane on märkida, et EIÕK ja ELPH viitavad „teabele“, mitte informatsioonile. Vt ka Maruste, R., Turk, K. Paragrahv 45. – Madise, Ü. et al. (toim). Eesti Vabariigi põhiseadus. Kommenteeritud väljaanne, p 11

⁹⁹ Euroopa Inimõiguste Kohus on teabe kohta täpsustanud, et selle all tuleb mõista avalikkusele põhjendatult huvi pakkuvat informatsiooni (EIK, 37374/05, Társaság a Szabadságjogokért vs. Ungari, 14.04.2009, p 26), kultuurilist, kunstilist ja meelelahutuslikku teavet (EIK, 23883/06, Khurshid Mustafa ja Tarzibachi vs. Rootsi, 16.03.2009), ärilist ja kaubanduslikku teavet (EIK, 10572/83, Markt intern Verlag GmbH vs. Saksamaa, 20.11.1989, p 26) ning igasuguseid andmeid.

¹⁰⁰ EIK, 5493/72, Handyside vs. Suurbritannia, 07.12.1976, p 49.

¹⁰¹ EIK, 39288/98, Association Ekin vs. Prantsusmaa, 17.07.2001.

¹⁰² EIK, 64659/09, Delfi AS vs. Eesti, 16.06.2015.

¹⁰³ Recommendation to human rights for Internet users. Committee of Ministers. 16.04.2014. CM/Rec(2014)6.

juurdepääsetavust ning võimet talletada ja edastada tohutut hulka teavet, parandab see oluliselt avalikkuse juurdepääsu uudistele, meelelahutusele, kultuurile, teadusele ja aitab üldisemalt kaasa teabe levitamisele.¹⁰⁴

Inimõigustega seotud küsimused kerkivad üles eelkõige selle tõttu, et potentsiaalne kahju, mida interneti sisu ja selle kaudu toimuv suhtlus võib tekitada inimõiguste ja põhivabaduste teostamisele, eriti õigusele eraelu puutumatusel, on kindlasti suurem kui trükiajakirjandusest või ka audivisuaalsest meediast tulenev oht.¹⁰⁵ Tehnoloogia on andnud võimaluse õigusvastase sisu enneolematuks ja globaalseks levikuks ning toonud kaasa tõdemuse, et demokraatlikes ühiskondades on vähe tõhusaid lahendusi selle piiramiseks.

Internet toimib üldjuhul eraõiguslike isikute pakutavate teenuste kaudu ja abil. Sellised teenused võivad olla ka sisuteenused (nt ettevõtte veebileht) või vahendusteenused. Vahendajad täidavad interneti ökosüsteemis olulist rolli, olles informatsiooni vārav ja inimõiguste võimaldaja. Vahendamine on sellise isiku roll, kes võimaldab kasutajale ühenduse internetiga; sisu talletamise ja indekseerimise; kauplemise, sealhulgas makseteenused; otsiteenused; kaupade turustamise paiga jms. Selliste vahendusteenuste puhul tuleb leida tasakaal vahendajate ja kolmandate isikute huvide ja õiguste vahel.¹⁰⁶ Infoühiskonnas on üles kerkinud kaks küsimust: õigus end väljendada, pääseda teabele ligi ja seda levitada ning küsimus vastutusest.

Vahendaja on üldjuhul eraõiguslik isik. Kui riigi kohta sätestab põhiseadus (§ 45), et tsensuuri ei ole, siis eraõiguslike isikute kohta selline norm puudub. Seega on aastaid arutatud, kas, millal ja mis tingimustel võib eraõiguslik isik sekkuda väljendusvabadusse ja piirata seda, mida levitatakse, arvestades et teise isiku teenus on vajalik väljendusvabaduse teostamiseks. Õigusvastase sisu levik alates vaenu õhutamisest (eesti keeles tihti nimetatud ka *vihakõneks*), üleskutsetest vägivallale ja väärinfost ning lõpetades kaubanduslike petuskeemide ja intellektuaalomandiõiguste rikkumistega on muutunud globaalseks probleemiks, millega võitlemiseks püüavad leida lahendusi seadusandjad üle maailma.¹⁰⁷

Teine küsimusteriing puudutab vastutust kasutaja loodud materjali eest. Juba 1831. aastal vastu võetud Belgia konstitutsioon kajastab euroopalikku vārtust, et „kui autor on teada ja elab Belgias, ei saa kirjastajat, trükikoda ega levitajat vastutusele võtta“¹⁰⁸. Sellest põhimõttest tuleneb ka digiruumis kehtiv üldreegel: internetiteenuse vahendaja ei vastuta kasutajate loodud või üleslaaditud sisu eest. Esmakordselt sätestati see põhimõte internetiteenuse vahendajate kohta 28. mail 2003 Euroopa Nõukogu Ministrite Komitee 840. ministrite asetäitjate kohtumisel vastu võetud deklaratsioonis kommunikatsioonivabaduse kohta internetis:

¹⁰⁴ EIK, 3111/10, Ahmet Yıldırım vs. Türki, 18.12.2012, p 48; EIK, 3002/03, Times Newspapers Ltd (nr 1 ja 2) vs. Ühendkuningriik, 10.03.2009, p 27.

¹⁰⁵ EIK, 33014/05, Editorial Board of Pravoye Delo ja Shtetel vs. Ukraina, 07.02.2018, p-d 63–64.

¹⁰⁶ Maruste, Turk, p 11.

¹⁰⁷ Näiteks Euroopa Komisjon andis 2017. aasta septembri teatises võitluse kohta ebaseadusliku veebisisuga lubaduse jälgida ebaseadusliku veebisisuga võitlemisel tehtavaid edusamme ning hinnata, kas ebaseadusliku veebisisu kiireks ja ennetavaks tuvastamiseks ja kõrvaldamiseks on vaja võtta lisameetmeid, mis võivad hõlmata muu hulgas kehtivat õigusraamistikku täiendavaid seadusandlikke meetmeid. Sellest ajast alates on Euroopa Liidu seadusloome võitluses õigusvastase internetisisuga olnud aktiivne.

¹⁰⁸ Belgia Esindajatekoda. Belgia põhiseadus. Jaanuar 2009. Artikkel 25. –

http://www.dekamer.be/kvvcr/pdf_sections/publications/constitution/GrondwetUK.pdf (13.09.2021).

„Liikmesriigid peavad tagama, et teenuseosutajaid ei peeta vastutavaks internetis leiduva teabe eest, kui nende tegevus piirneb riigisisese õigusega määratletu kohaselt teabeedastusega või internetile juurdepääsu pakkumisega.

Kui teenuseosutajate tegevusala on laiem ja nad talletavad teistelt isikutelt pärit teavet, võivad liikmesriigid pidada neid kaasvastutajateks, kui nad viivitamata ei kõrvalda teavet või teenuseid või ei tühista juurdepääsu teabele või teenustele kohe, kui nad riigisisese õigusega määratletu kohaselt saavad teada teabe või teenuste ebaseaduslikkusest või kahju hüvitamise nõude korral tegevuse või teabe ebaseaduslikkusele viitavatest faktidest või asjaoludest.“¹⁰⁹

Deklaratsioonist on see leidnud tee e-kaubanduse direktiivi artiklitesse 12–14 ¹¹⁰ ning infoühiskonna teenuse seaduse paragrahvidesse 8–10.¹¹¹

Endiselt on küsimus selles, et olulisi avalikke hüvesid evivate teenuste pakkujate seas on palju eraõiguslikke isikuid. Internetiteenuse vahendajate rolli ja vastutust käsitlevaid õigusakte ajakohastas Euroopa Nõukogu Ministrite Komitee aastal 2018, mil võeti vastu soovitus liikmesriikidele internetiteenuse vahendajate rolli ja kohustuste kohta.¹¹²

Eeltooduga seondub põhimõte, et riigid ei tohi kehtestada teenuseosutajatele üldist kohustust jälgida internetis leiduvat teavet, millele nad võimaldavad juurdepääsu või mida nad edastavad või talletavad, ega kohustust otsida ebaseaduslikku tegevust näitavaid fakte ja asjaolusid.¹¹³

Euroopa Liidu Kohus on leidnud, et internetiteenuse pakkuja kohta ei tohi teha ettekirjutust, mis kohustaks teenuseosutajat rakendama filtreerimissüsteemi, mis filtreerib kogu tema teenuse raames toimuva elektroonilise side; mida kohaldatakse vahet tegemata kõigile tema klientidele; mis on ennetav; mida rakendatakse ainult tema kulul ja mis ei ole ajaliselt piiratud. Sellise filtreerimissüsteemi eesmärk on blokeerida autoriõigust rikkuvate failide edastamine. Süsteem on võimeline tuvastama teenusepakkuja võrgus selliste failide vahetuse, mis sisaldavad muusika-, kinematograafilisi või audiovisuaalteoseid, mille intellektuaalomandi õigusi ettekirjutuse nõude esitaja väidab omavat.¹¹⁴

¹⁰⁹ Euroopa Nõukogu Ministrite Komitee 840. ministrite asetäitjate kohtumisel vastu võetud deklaratsiooni suhtlemisvabaduse kohta internetis, vastu võetud 28. mail 2003;

¹¹⁰ Euroopa Parlamendi ja nõukogu 08.06.2000 direktiiv nr 2000/31/EÜ infoühiskonna teenuste teatavate õiguslike aspektide, eriti elektroonilise kaubanduse kohta siseturul (e-kaubanduse direktiiv).

¹¹¹ Infoühiskonna teenuse seadus. – RT I, 22.06.2021, 14; Vabariigi Valitsuse seaduse ja teiste seaduste muutmise seadus. – RT I, 12.12.2018, 3.

¹¹² Ministrite Komitee soovitus liikmesriikidele seoses interneti teenuse vahendajate rollide ja vastutusega. 07.03.2018. CM/Rec(2018)2.

¹¹³ Vt 28. mail 2003 Euroopa Nõukogu Ministrite Komitee 840. ministrite asetäitjate kohtumisel vastu võetud deklaratsiooni suhtlemisvabaduse kohta internetis; samuti Euroopa Parlamendi ja EL Nõukogu 8. juuni 2000 direktiivi nr 2000/31/EÜ infoühiskonna teenuste teatavate õiguslike aspektide, eriti elektroonilise kaubanduse kohta siseturul (e-kaubanduse direktiiv), artikkel 15 (üldise jälgimiskohustuse puudumine).

¹¹⁴ EK, C-70/10, Scarlet Extended SA vs. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM), ECLI:EU:C:2011:771; EK, C-360/10, Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) vs. Netlog NV, ECLI:EU:C:2012:85.

4.2. Väljendusvabadus ja platvormid

Väljendusvabaduse seisukohalt on oluline roll internetiplatvormi teenuse pakkujatest internetiteenuse vahendajatel. Just platvormidele langeb suur roll internetisisu üle otsustamisel, eelkõige „selgelt ebaseadusliku“ sisu üle otsustamisel.

Euroopa Inimõiguste Kohus on välja töötanud põhimõtted selliste vahendajate tarbeks, kelle ülesanne on kolmandate isikute loodud sisu talletamine ja avalikustamine. Internetiteenuse vahendajate puhul on kõikide asjaosaliste õiguste ja huvide tasakaalustamiseks sobiv vahend teatamise ja kõrvaldamise süsteem, millega kaasnevad kiiret reageerimist võimaldavad tõhusad protseduurid.¹¹⁵ Euroopa Inimõiguste Kohtu praktika kohaselt on erandiks eelkõige juhud, kui kolmandate isikute loodud sisu on vaenu õhutatav ja vahetult isikute füüsilise puutumatuse vastu suunatud ähvarduste vormis. Sellistel juhtudel võivad teiste isikute ja ühiskonna kui terviku huvid anda riikidele õiguse võtta internetiteenuse vahendajad vastutusele, ilma et tekiks vastuolu konventsiooni artikliga 10. Uudiseportaaali artikli juurde jäetud kommentaaride kohta leidis Euroopa Inimõiguste Kohus, et vastutuse tunnistamine ei riku selliste portaali väljendusvabadust, juhul kui portaal ei võta meetmeid selgelt õigusvastaste kommentaaride viivitamatuks kõrvaldamiseks, isegi kui väidetav ohver või kolmandad isikud pole neist teavitanud.¹¹⁶

Hilisemates lahendites on Euroopa Inimõiguste Kohus leidnud, et kohustus filtreerida või eemaldada teatud tüüpi kasutajate sisu veebiplatvormidelt paneb operaatoritele „ülemäärase ja teostamatu“ koormuse ning võib sundida neid paigaldama seiresüsteemi, „mis võib kahjustada õigust edastada teavet internetis“.¹¹⁷ Euroopa Inimõiguste Kohtu praktika võib võtta kokku selliselt, et platvormi vastutuse hindamisel tuleb lähtuda järgmistest kriteeriumidest: 1) kasutaja loodud postituse või kommentaari kontekst ning sisu on üheselt ja selgelt õigusvastane, mitte vaieldavalt ebakohane või väär (nt vaenuõhutus); 2) riigi tasandil on esmalt kaalutud kasutajate endi vastutust; 3) mistahes vastutuse jaotamise korral on vaagitud, et vastutus ei ohusta platvormi alles jäämist; 4) tuleb tuvastada, kas platvorm on kasutusele võtnud piisavalt hoolsusmeetmeid; 5) arvesse tuleb võtta platvormi suurust ja võimekust, sest platvormide kadumine oleks ohuks demokraatiale; 6) kannatanu peaks suutma näidata, et talle tekitati tegelikku ja olulist kahju.

Euroopa Liidu tasandil on juhiseks Euroopa Komisjoni teatis võitlusest ebaseadusliku veebis sisuga¹¹⁸, mis lähtub järgmisest arusaamast:

„[...] platvormidel, mis vahendavad infosisu kättesaadavust enamikule internetikasutajatele, lasub oluline ühiskondlik vastutus: nad peavad kaitsma kasutajaid ja laiemalt kogu ühiskonda ning ei tohi lasta kurjategijatel ja teistel veebis rikkumisi toime panevatel isikutel oma teenuseid ära kasutada. Platvormide loodav avatud digiruum ei tohi muutuda terrorismi, ebaseadusliku vaenuõhutuse, laste väärkohtlemise või inimkaubanduse kasvulavaks ega kohaks, kus ei kehti õigusriigi põhimõte. On ilmselge, et ebaseadusliku infosisu levik veebis võib õõnestada

¹¹⁵ EIK, 64569/09, Delfi AS vs. Eesti, 16.06.2015; EIK, 22947/13, Magyar Tartalomszolgáltatók Egyesülete ja Index.hu Zrt vs. Ungari, 02.02.2016; EIK, 74742/14 M, Pihl vs. Rootsi, 07.02.2017.

¹¹⁶ EIK, 64569/09, Delfi AS vs. Eesti, 16.06.2015.

¹¹⁷ EIK, 22947/13, Magyar Tartalomszolgáltatók Egyesülete ja Index.hu Zrt vs. Ungari, 02.02.2016.

¹¹⁸ Komisjoni teatis Euroopa Parlamendile, nõukogule, Euroopa Majandus- ja Sotsiaalkomiteele ning Regioonide Komiteele. Euroopa Komisjon. 28.09.2017. COM(2017)555, kättesaadav: <https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX%3A52017DC0555> (viimati külastatud 18.10.2021).

kodanike usaldust digitaalse keskkonna vastu ja sellega seotud kindlustunnet, kuid ühtlasi võib see ohtu seada ka platvormikeskkondade ja digitaalse ühtse turu majandusliku arengu. Veebiplatvormide keskne koht ühiskonnas tähendab vastutust ja ühe osana sellest peaksid need platvormid otsustavalt tõhustama oma tegevust kirjeldatud probleemi lahendamiseks.“¹¹⁹

Euroopa Komisjoni teatise kohaselt nõutakse erasektorilt selgemaid „teavitamise ja meetmete võtmise“ menetlusi. Selle järgi peaksid veebiplatvormid kehtestama lihtsad ja läbipaistvad eeskirjad ebaseaduslikust infosist teavitamiseks, sealhulgas kiirmenetlused „usaldusväärsete märguandjate“ jaoks. Sisuteenuse pakkujaid tuleks teavitada sellistest otsustest ja neil peaks olema võimalus neid vaidlustada, et vältida seadusliku sisu tahtmatut eemaldamist. Teatise järgi on nõutud ka tõhusamad vahendid ja ennetavad tehnoloogiad. See tähendab, et ettevõtted peaksid kehtestama kasutajate jaoks selged teavitussüsteemid. Neil peaksid olema ennetavad vahendid ebaseadusliku sisu tuvastamiseks ja eemaldamiseks, eelkõige terrorismi ja muu sellise sisu puhul, mida ei ole vaja kontekstuaalselt määratleda, et seda ebaseaduslikuks pidada (näiteks materjalid laste seksuaalse kuritarvitamise kohta või võltsitud kaubad).

Meie hinnangul on selline suundumus üks võimalus ebaseadusliku veebisisuga võitlemiseks, kuid seoses sellega kerkib üles ka olulisi põhiseaduslikke küsimusi. Platvormide tehtavad otsused pole sageli läbipaistvad ja nendega ei kaasne aruandekohustust, mis tekitab ülemäärase sõnavabadusse sekkumise ohu, ning need kätkevad riski kvalifitseeruda õiguskaitsekohustuste üleandmiseks riikidelt eraettevõtetele. Riigi õiguskord, mis nõuab, et digitaalsed vahendajad piiraksid juurdepääsu sisule, mis põhineb ebamäärastel mõistetel, nagu *ekstremism*, *soovimatu sisu* ja *kahjustav sisu*, kohustab vahendajaid jälgima kogu veebipõhist suhtlust, et avastada ebaseaduslikku sisu. Nii rikutakse põhimõtet, et vahendajad ei peaks olema kohustatud tegema üldist järelevalvet, eelkõige just võimaliku nn jahutava mõju tõttu sõnavabadusele¹²⁰, aga ka seetõttu, et küsitav on, kas platvormid suudavad ise otsustada, kas tegemist on õigusvastase sisuga. Seetõttu jääb platvormide poolt sisu kõrvaldamisel küsimus: kuna vahendid ja meetmed, mille abil tuvastamis- ja eemaldamisotsused tehakse, on eraõiguslike teenuseosutajate otsustada, ning kui nende meetmete suhtes ei kohaldata sisulist ja tõhusat riiklikku järelevalvet, võib see ületada seadusega ja põhiseadusega ette nähtud piire, rikkudes seeläbi õigusriigi põhimõtet.¹²¹

Avatud interneti kui väärtust tagavad mitmed rahvusvahelised õigusaktid, näiteks need, mis käsitlevad internetisisu ja sellele juurdepääsu filtreerimist ja blokeerimist.¹²² Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikli 10 kohaselt peavad kõik meetmed, mis blokeerivad juurdepääsu sisule filtreerimise või sisu eemaldamise teel, olema seadusega ette nähtud, järgima üht artikli 10 lõikes 2 ette nähtud õiguspärastest eesmärkidest ning olema

¹¹⁹ *Ibid.*

¹²⁰ See põhimõte on sätestatud nii Euroopa Liidu (nt e-kaubanduse direktiivis) kui ka Euroopa Nõukogu mitmes soovituses, nt Ministrite Komitee soovitus liikmesriikidele seoses interneti teenuse vahendajate rollide ja vastutusega. 07.03.2018. CM/Rec(2018)2.

¹²¹ Mitmed riigid on võtnud vastu seadusi, mis puudutavad kahjuliku internetisisu levikut. Näiteks Saksamaa võttis vastu sotsiaalvõrgustikes õiguste teostamist käsitleva seaduse (NetzDG) aastal 2017. Selle seaduse kohaselt peavad veebiplatvormid, millel on Saksamaal rohkem kui kaks miljonit registreeritud kasutajat, eemaldama „ilmselgelt ebaseadusliku“ sisu 24 tunni jooksul alates teate või kaebuse saamisest ning kõrvaldama kogu muu „ebaseadusliku“ sisu seitsme päeva jooksul alates teatamisest. Ebaseadusliku sisu all on mõeldud internetisisu, mis on vastuolus Saksamaa kriminaalkoodeksi konkreetsete elementidega, nagu holokausti eitamine ja vaenuõhutus. Nõuete täitmata jätmisega kaasneb kuni 50 miljoni euro suurune trahv. Seadus on pälvinud märkimisväärselt kriitikat, kuna see piirab väljendusvabadust.

¹²² Ministrite Komitee soovitus liikmesriikidele seoses vaba, piiriülese informatsiooni liikumisega Internetis. 1.04.2015. CM/Rec(2015)6.

demokraatlikus ühiskonnas vajalikud. Euroopa Inimõiguste Kohtu praktikat arvestades peavad sõnavabaduse piirangud vastama „tungivale sotsiaalsele vajadusele“ ja olema proportsionaalsed taotletavate õiguspäraste eesmärkidega.

Seoses internetisisu blokeerimisega on Euroopa Inimõiguste Kohus leidnud, et internet on ka ligipääsuvahend, mis võimaldab teostada väljendusvabadust. Kohtuasja Ahmet Yildirim vs. Türgi kohaselt oli kaebajal veebisait teenuses Google Sites. Türgi kohtu taotlusel blokeeriti igasugune juurdepääs Google Sites'i teenustele, selleks et blokeerida juurdepääs osale selles talletatavatest õigusvastastest veebisaitidest. Seetõttu ei saanud kaebaja enam juurdepääsu ka oma veebisaidile. Euroopa Inimõiguste Kohus selgitas, et Google Sites on Google'i teenus, mille eesmärk on hõlbustada veebisaitide loomist ja jagamist grupisiseselt, ning on seega vahend sõnavabaduse kasutamiseks. Niisiis ei ole juurdepääsu piiramine kogu Google Sites'i teenusele proportsionaalne ning inimõigusi austav. Euroopa Inimõiguste Kohus märkis:

„[...] eelnevatele piirangutele omased ohud on sellised, et need nõuavad kohtult kõige hoolikamat kontrolli, [...] sest uudised on kiiresti riknev kaup ja selle avaldamise edasilükkamine isegi lühikeseks ajaks võib selle väärtuse ära võtta. Seetõttu nõuab internetile juurdepääsu blokeerimine või veebisisu eemaldamine õigusraamistikku, „tagades nii range kontrolli keeldude ulatuse üle kui ka tõhusa kohtuliku kontrolli, et vältida võimu kuritarvitamist. [...] Sellega seoses on sellise meetme kohtulik kontroll, mis põhineb konkureerivate huvide kaalumisel ja mille eesmärk on saavutada nende vahel tasakaal, mõeldamatu ilma raamistikuta, millega kehtestatakse täpsed ja konkreetsed eeskirjad sõnavabaduse ennetuslike piirangute kohaldamise kohta.“¹²³

Nagu märgitud, on Euroopa Inimõiguste Kohus pidanud tõlgendama ka ajakirjandusliku sisu kustutamist internetist. Asjas Wegrzynowski ja Smolczewski vs. Poola rõhutas kohus, et internetiarhiividel on oluline roll uudiste ja informatsiooni säilitamisel ja kättesaadavaks tegemisel. Ka märgitud lahendist tuleneb, et kuigi meedia esmaülesanne demokraatias on olla valvekoer, on tal ka teisene funktsioon: talletada ning teha avalikele arhiividele kättesaadavaks uudislööd, mis on eelnevalt avalikult kajastatud.¹²⁴

5. Väljendusvabadus, tehisintellekt, algoritmilised süsteemid, profileerimine

Väljendusvabaduse põhiõiguse teostamine on järjest enam surve all seoses uute tehnoloogiate – nagu näiteks tehisintellekti ja algoritmiliste süsteemid – kasutuselevõtmisega.

Tehisintellekt viitab süsteemidele, mis näitavad intelligentset käitumist, analüüsides keskkonda ja võttes meetmeid – teatud autonoomiaga – konkreetsete eesmärkide saavutamiseks.¹²⁵ Tehisintellektil põhinevad süsteemid võivad olla puhtalt tarkvarapõhised, virtuaalmaailmas toimivad (nt häälabi rakendus, pildianalüüsi tarkvara, otsingumootorid, kõne- ja näotuvastussüsteemid) või integreeritud riistvaraseadmetesse (nt arenenud robotid,

¹²³ EIK, 3111/10, Yildirim vs. Türgi, 18.03.2013.

¹²⁴ EIK, 33846/07, Wegrzynowski ja Smolczewski vs. Poola, 16.10.2013. Ka Riigikohus on leidnud, et artikli eemaldamine ei ole proportsionaalne meede, kui hagiavaldusest ei nähtu, nagu koosneks kogu artikkel ainult valedest faktiväidetest ja kohatutest väärtushinnangutest (vt RKTk, 3-2-1-147-16, 08.02.2017).

¹²⁵ Tehisintellekti legaalseadistamises ei ole eksperdid kokkuleppele jõudnud ning see definitsioon on Euroopa Komisjoni tehtud legaalseadistamise ettepanek. High Level Expert Group on AI, A Definition of AI: Main Capabilities and Disciplines. – European Commission 08.04.2019.

autonoomsed mootorsõidukid, droonid või nutistu ehk asjade internetirakendused).¹²⁶

Tehisintellekti puhul on kõige rohkem kõlapinda tekitanud algoritmilised süsteemid ja andmetöötlustehnikad, millel on tohtu mõju sõnavabadusele, seda nii otsimootorite, algoritmilise ennustamise ja isikupärastamise (profileerimine), algoritmilise modereerimise ja algoritmide poolt sisu loomise kaudu. Nendel küsimustel peatume selles alapeatükis.

5.1. Otsingualgoritmid

Otsingualgoritmid ja otsingumootorid võimaldavad rahvusvahelisel üldsusel otsida, vastu võtta ja edastada teavet ja ideid ning muud sisu, eelkõige teadmiste omandamiseks ning aruteludes ja demokraatlikes protsessides osalemiseks.¹²⁷ Samal ajal dikteerivad otsingumootorite algoritmid seda, mida ja millises järjekorras kasutajad näevad, ning nendega võidakse manipuleerida sisu piiramiseks või prioriseerimiseks¹²⁸, mistõttu võivad need kahjustada üksikisikute, kogukondade ja tervete elanikerühmade teabe- ja sõnavabadust. See ei seostu mitte ainult individuaalse õigusega sõnavabadusele, vaid ka artikli 10 eesmärgiga luua pluralistlikuks aruteluks soodne keskkond, mis on kõigile võrdselt kättesaadav ja kaasav.

Otsingumootorid toimivad oluliste väravavahtidena kõigi jaoks, kes soovivad teavet otsida, vastu võtta või edastada. Sisu, mida otsingualgoritm ei indekseeri ega hinda kõrgelt, jõuab väiksema vaatajaskonnani või on üldse nähtamatu. Selle tulemusena võib algoritmide kasutamine viia avaliku sfääri killustumiseni ja nn kajakambrite loomiseni, mis soodustavad ainult teatud tüüpi infokanaleid, suurendades seeläbi polariseerumist ühiskonnas – see omakorda võib tõsiselt ohustada sotsiaalset ühtekuuluvust.¹²⁹

Otsingualgoritm võib olla kallutatud ka teatud liiki sisu või sisupakkujate suhtes, nii riskitakse sellega seotud väärtuste, näiteks meedia pluralismi ja mitmekesisuse mõjutamisega.¹³⁰ Internetis info võrdne kohtlemine tagab kõigi ja igaühe võrdsed võimalused. Näiteks Euroopa Komisjon on alustanud arvukalt uurimisi seoses Google'i toodete ja teenustega alates otsimootorist ja lõpetades Androidi operatsioonisüsteemiga, mille puhul komisjon leidis, et Google pärssis valikuvõimalusi ja innovatsiooni mitmesuguste mobiilirakenduste ja -teenuste puhul, kuna Google järgis mobiilsete seadmete puhul üldist strateegiat, mille eesmärk oli kaitsta ja laiendada oma turgu valitsevat seisundit interneti üldotsingute valdkonnas.¹³¹ Need uurimised põhinevad konkurentsioigusel, kuid on samavõrra olulised põhiõiguste seisukohast.

Ülemaailmsel digitaalsetel platvormidel on suur mõju nii üksikisikute kui ka ühiskondade teabekeskondadele, kus automatiseeritud algoritmid otsustavad, kuidas käsitleda, prioriseerida, levitada ja kustutada või eemaldada kolmanda osapoole sisu veebis, sealhulgas poliitiliste ja valimiskampaaniate ajal. Platvormide suutlikkus levitada sõnumeid reaalsajas ja

¹²⁶ *Ibid.*

¹²⁷ Recommendation to member States on the protection of human rights with regard to search engines. Committee of Ministers. 04.04.2012. CM/Rec(2012)3, p 1.

¹²⁸ ÜRO arvamus- ja sõnavabaduse edendamise ja kaitse eriraportööri David Kaye' 2016. aasta aruanne inimõiguste nõukogu 32. istungjärgul (A/HRC/32/ 38).

¹²⁹ Maruste, R., Turk, K. Paragrahv 45. – Eesti Vabariigi põhiseadus. Kommenteeritud väljaanne, p 10. – <https://pohiseadus.ee/sisu/3514> p 49; vt ka Saxena, R. The social media „echo chamber“ is real. – Ars Technica 03.2017. – <https://arstechnica.com/science/2017/03/the-social-media-echo-chamber-is-real/> (25.09.2020).

¹³⁰ UNESCO. World Trends in Freedom of Expression and Media Development. – <http://www.unesco.org/new/en/world-media-trends> (25.09.2020).

¹³¹ Euroopa Komisjon, konkurentsipoliitika, otsused Google'i suhtes, nt otsus nr 39740, Google Search (Shopping). – https://ec.europa.eu/competition/elojade/isef/index.cfm?fuseaction=dsp_result&policy_area_id=1&case_title=Google (13.09.2021).

ülemailmsel tasandil on suurendanud oluliselt õigusvastase sisu ulatust ja seega ka mõju, mistõttu püüavad ka seadusandjad rakendada algoritme sellise sisu filtreerimiseks, blokeerimiseks ja eemaldamiseks.

Pöördumine automaatsete lähenemisviiside poole veebisisu filtreerimisel toob esile teravad vastutusprobleemid, mida tekitab suurenev sõltuvus algoritmilistest süsteemidest. Kuigi need süsteemid pakuvad oma mastaabi, kiiruse ja tõhususe tõttu suuremat kasu kui inimeste otsuste tegemine, on inimeste järelevalve vajalik, ehkki mastaabi tõttu ebapiisav.¹³² Veebiplatvormid on üha suurema surve all, et võidelda aktiivselt veebipõhise õigusvastase sisu vastu automatiseeritud tehnika abil. Kuigi vaieldamatult tuleb otsustavalt tegutseda vaenuõhutuse leviku ja rassistlikele õigusrikkumistele õhutamise vastu, tekitab see märkimisväärsed probleeme seoses sõnavabadusse sekkumise seaduslikkusega. Äärmuslikku sisu või vägivalda õhutavat materjali on sageli raske tuvastada isegi koolitatud inimesel, sest keeruline on eristada selliseid tegureid nagu kultuuriline kontekst ja huumor. Algoritmid ei suuda tänapäeval tuvastada irooniat ega kriitilist analüüsi, karikatuure ega nalju. Euroopa Inimõiguste Kohtu pikaajalise praktika kohaselt kaitseb artikkel 10 ka šokeerivat, solvavat või häirivat sisu, mistõttu seistakse kahjuliku sisu kõrvaldamiseks rakendatava algoritmilise filtreerimise korral silmitsi üleblokeerimise ja õiguspärase sisu eemaldamise ohuga.¹³³

5.2. Algoritmilised otsused

Sotsiaalmeediaplatformide kasutajate eelistuste algoritmilised ennustused ei juhi mitte ainult seda, milliseid reklaame inimestele näidatakse, vaid nende kaudu isikupärastatakse ka otsingutulemused ja dikteeritakse, kuidas sotsiaalmeediakanalid, sealhulgas uudislehed, on korraldatud. Arvestades selliste platformide suurust, nende kesksust paljude internetikogemuste jaoks poolavaliku sfäärina¹³⁴ ja nende võimet teatud hääli võimendada ning nende võimekust isikupärastada sisu kasutajate eeldatavate eelistuste ja huvide alusel, on loodud nn filtrimullid ja kõlakojad, mis mõjutavad seda, kuidas on teave kättesaadav.¹³⁵

Andmepõhise infokeskkondade isikupärastamine kasutajate profileerimise kaudu toob kaasa võimalused manipuleerida inimestega peenel, kuid väga tõhusal viisil.¹³⁶ Individuaalsel tasandil võib manipuleerimine ohustada isiklikku autonoomiat ja tekkivat õigust kogitiivsele

¹³² Wagner, B., Schulz, W., Turk, K *et al.* Study On The Human Rights Dimensions of Automated Data Processing Techniques (In Particular Algorithms) And Possible Regulatory Implications. 2016. Council of Europe, Committee of Experts on internet intermediaries (MSI-NET). – <https://rm.coe.int/study-hrdimension-of-automated-data-processing-incl-algorithms/168075b94a> (01.04.2021); Yeung, K. Responsibility and AI: A study of the implications of advanced digital technologies (including AI systems) for the concept of responsibility within a human rights framework. Council of Europe study. DGI(2019)05, lk 31.

¹³³ Mitmed Euroopa Inimõiguste Kohtu otsused, mis käsitlesid küsimust, kas teatud avaldust võiks või tuleks kvalifitseerida kuritegelikuks vaenuõhutuseks, andsid tulemuseks jagatud hääled, vt näiteks EIK, 21279/02 ja 36448/02, Lindon, Otchakovsky-Laurens ja Juuli vs. Prantsusmaa, 22.10.2007; EIK, 15615/07, Féret vs. Belgia, 16.07.2009; EIK, 27510/08, Perinçek vs. Šveits, 15.10.2015; EIK, 1813/07, Vejdeland jt vs. Rootsi, 09.02.2012.

¹³⁴ York, J. C. Policing Content in the Quasi-Public Sphere. MA: Open Net Initiative Bulletin. Berkman Center. – Boston: Harvard University 2010.

¹³⁵ Maruste, R., Turk, K. Paragrahv 45. – Madise, Ü. *et al.* (toim). Eesti Vabariigi põhiseadus. Kommenteeritud väljaanne, p 10. – <https://pohiseadus.ee/sisu/3514>; vt ka Bucher, T. Want to Be on the Top? Algorithmic Power and the Threat of Invisibility on Facebook. – New Media & Society 08.04.2012.

¹³⁶ Yeung, K. Hypernudge: Big Data as a mode of regulation by design. – Information, Communication & Society 22.05.2016, lk 1–19. Näiteks analüüsiti Norra tarbijanõukogu hiljutises uuringus Facebooki, Google'i ja Windows 10 seadete valimit ning näidati, kuidas kasutajatega manipuleerimiseks mõeldud vaikeseadeid ja mustreid, tehnikaid ja funktsioone kasutatakse teatud valikute suunas: Norwegian Consumer Council. Deceived by Design. – ForbrukerRadet 27.06.2018.

suveräänsusele.¹³⁷ Samas näitavad mitmed andmepõhise manipuleerimise globaalsed juhtumid (nt Cambridge Analytica skandaal USA 2016. aasta valimiste ja Brexiti referendumi eel), et kui poliitilise mikrosihtmärgistamise eesmärgil püütakse mastaapselt manipuleerida hääletamiskäitumisega (mis võib hõlmata sotsiaalmeedia veebisaitidel tegutsevate automatiseeritud *bot*'ide kasutamist), võib see ohustada nii igaühe õigust mõtte, sõna- ja teabevabadusele kui ka tõsiselt kahjustada demokraatia korralduse aluseid. Nii rikutakse Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikli 3 protokolli nr 1 alusel kaitstud õigust vabadele valimistele.¹³⁸

Digitehnoloogial põhinevat manipuleerimist võib mõista kui artiklite 8 ja 10 alusel kaitstud õigustesse sekkumist, kuna seda kasutatakse automaatselt (ja pidevalt ümber konfigureerides) inimeste informatsioonilise valiku ja keskkonna kohandamiseks andmepõhise profiilianalüüsi abil, et ennustada mastaapselt (sageli suure täpsusega) üksikisikute käitumist, huve, eelistusi ja haavatavust. Neid rakendusi saab kasutada inimestega manipuleerimiseks ja nende petmiseks, mis riivab seega nii privaatsusõigust kui ka väljendusvabadust.¹³⁹ Oxfordi teadlased prof Douwe Korff ja dr Ian Brown on järeldanud:

„Profiilianalüüs kujutab endast tõsist ohtu kafkalikule maailmale, kus võimsad korporatsioonid ja riigiasutused võtavad vastu otsuseid, mis mõjutavad oluliselt nende kliente ja kodanikke, ilma et need otsustajad saaksid või oleksid valmis selgitama nende otsuste aluseks olevaid põhjendusi ning kus klientidele ja kodanikele ei võimaldata tõhusaid individuaalseid või kollektiivseid õiguskaitsevahendeid. Nii tõsine on profileerimise küsimus: see kujutab endast fundamentaalset ohtu õigusriigi kõige põhilisematele põhimõtetele ning võimu ja üksiksiku suhetele demokraatlikus ühiskonnas.”¹⁴⁰

Algoritmiliste süsteemide hankimine, loomine, arendamine ja kasutuselevõtt on nii Euroopa Nõukogu¹⁴¹ kui Euroopa Komisjoni¹⁴² kümnete õigusinstrumentide ese. Samas riigi tasandil seadusandjad alles kaaluvad, milline on õige ja tõhusaim õigusraamistik ja poliitika, et tagada inimõiguste kaitse, takistamata samas tehnoloogia arengut.

¹³⁷ Teatavat akadeemilist toetust uue õiguse tunnustamisele kognitiivse suveräänsuse suhtes, mille eesmärk on pakkuda üksikisikutele õigustel põhinevat kaitset manipuleerimise ja pettuse vormide eest, mida digitehnoloogia edendamine üha enam võimaldab, et tagada üksikisikutele suveräänsuse lävitase oma vaimu ja meele üle (vt Bublitz, J. C. My mind is mine!? Cognitive liberty as a legal concept in Cognitive Enhancement: An Interdisciplinary Perspective. – Hildt, E., Franke, A. G. (toim). – Dordrecht. Springer 2013, lk 233–264). Kuigi see võib olla iseseisev õigus, on ka võimalik, et sellist õigust võib tunnustada Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikli 9 lõike 1 alla kuuluvana, mis sätestab õiguse mõtte-, südametunnistuse- ja usuvabadusele.

¹³⁸ Gorton, W. A. Manipulating Citizens: How Political Campaigns' Use of Behavioral Social Science Harms Democracy'. – New Political Science 2016/38 (1), lk 61–80; Gorton, W. A. Manipulating Citizens: How Political Campaigns' Use of Behavioral Social Science Harms Democracy. – New Political Science: 2016/38 (1).

¹³⁹ Yeung, K. Hypernudge: Big Data as a mode of regulation by design. – Information, Communication & Society 2016, lk 1–19.

¹⁴⁰ Korff, D., Browne, I. The use of the Internet & related services, private life & data protection: trends, technologies, threats and implications. Council of Europe, T-PD(2013)07, 2013, lk 21. – <https://ssrn.com/abstract=2356797> (01.04.2021).

¹⁴¹ Ministrite Komitee soovitus liikmesriikidele algoritmiliste süsteemide mõjust inimõigustele. 08.04.2020. – CM/Rec(2020)1.

¹⁴² Euroopa Komisjoni kõrgetasemeline tehisintellekti eksperdirühm. Etikasuunised usaldusväärse tehisintellekti arendamiseks, 2019. – https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/JURI/DV/2019/11-06/Ethics-guidelines-AI_ET.pdf (13.09.2021).

5.3. Algoritmiline sisuloome

Tehisintellekt (eelkõige algoritmid) on tehnoloogiliselt võimeline sisu looma. Selline sisu võib olla nii õige ja korrektse teabe vormis kui ka libauudise, desinformatsiooni, süvavõltsingute ja *bot*'ide vormis, mis hinnanguliselt moodustavad vähemalt poole kogu internetiliiklusest.¹⁴³

Selliste nähtude vastu on riigil vähe võimalusi meetmeid võtta: iga piirang peab olema rakendatud seaduse alusel, sellel peab olema seaduspärane eesmärk ning see peab olema proportsionaalne, eelkõige vajalik demokraatlikus ühiskonnas. Võimalike meetmetega filtreerimise ja blokeerimise kaudu võib kaasneda mõju, mis ei vastaks Euroopa inimõiguste standardile.¹⁴⁴ Euroopa Inimõiguste Kohus on leidnud, et olukorras, kus riik otsustas teatud ebasoovitava sisu blokeerida, kuid sellega kaasnes ka õiguspärase sisuga veebilehtede blokeerimine, kaasnes mõju paljudele internetikasutajatele ja seeläbi piirati omavoliliselt ka kaebaja sõnavabadust.¹⁴⁵ Riikliku sekkumise kõrval peetakse lahenduseks pigem digiteadlikkuse suurendamist ning tehnoloogia kasutamist sellise teabe tuvastamiseks. Iga lähenemine eraldiseisvalt kätkeb endas nii võimalusi, piiratust kui ka ohte, millest anname ülevaate siinses peatükis.

6. Kogunemis- ja ühinemisvabadus ning tehnoloogia

Euroopa Inimõiguste Kohus on märkinud, et terminitel *kogunemine* ja *ühingud* on Euroopa inimõiguste ja põhivabaduste kaitse konventsioonis sätestatud tingimustel (artikkel 11) iseseisev tähendus, mis ei sõltu riigisisest õigusest.¹⁴⁶ Kogunemistele viitas kohus kui „määramata arvu isikute kogunemisele, kellel on tuvastatav kavatsus osaleda kommunikatiivses protsessis“. Kohus on veel öelnud, et kogunemisvabadus hõlmab nii erakohtumisi kui ka kohtumisi avalikel koosolekutel, samuti staatilisi koosolekuid ja avalikke rongkäike ning et seda inimõigust võivad kasutada nii üksikosalejad kui ka kogunemist korraldavad isikud.¹⁴⁷

Ühingute kohta on Euroopa inimõiguste ja põhivabaduste kaitse konventsioonis sedastatud, et „võime asutada juriidiline isik kollektiivseks tegutsemiseks vastastikust huvi pakkuvast valdkonnas on ühinemisvabaduse üks olulisemaid aspekte“. Kuigi konventsiooni artiklis 11 on sõnaselgelt nimetatud ainult üht liiki ühingu (st ametiühingud) ning asjakohane Euroopa Inimõiguste Kohtu praktika viitab erakondadele, on mõistel *ühendus* laiem tähendus, sest „ühendused, mis on moodustatud muudel eesmärkidel, sealhulgas need, mis kaitsevad kultuuri- või vaimset pärandit, järgivad erinevaid sotsiaal-majanduslikke eesmärke, kuulutavad või õpetavad religiooni, otsivad etnilist identiteeti või kinnitavad vähemusteadvust, on samuti olulised demokraatia nõuetekohaseks toimimiseks. [...] On täiesti loomulik, et kui kodanikuühiskond toimib, saavutatakse kodanike osalemine demokraatlikus

¹⁴³ Horowitz, M. et al. Artificial Intelligence and International Security, Center for a New American Security, 10.07.2018. – <https://www.cnas.org/publications/reports/artificial-intelligence-and-international-security>.

¹⁴⁴ Tackling Online Disinformation: A European Approach, COM(2018) 236 final, Euroopa Komisjon, 26.04.2018, lk 2.

¹⁴⁵ EIK, 3111/10, Ahmet Yildirim vs. Türgi, 18.12.2012.

¹⁴⁶ EIK, 25088/94, Chassagnou jt vs. Prantsusmaa, 29.04.1999, p 100.

¹⁴⁷ EIK, 26005/08, Tatár ja Fáber vs. Ungari, 12.06.2012, p 38; Sergei Kuznetsov vs. Venemaa, 23.10.2008, p 35; samuti EIK, 33689/96, Andersonid jt vs. Ühendkuningriik, 27.10.1997.

¹⁴⁸ EIK, 44158/98, Gorzelik jt vs. Poola, 17.02.2004, p 88.

protsessis suures osas ühendustesse kuulumise kaudu, kus nad võivad üksteisega integreeruda ja koos ühiseid eesmärke saavutada“.¹⁴⁹

Nii Euroopa inimõiguste konventsioon kui ka Eesti põhiseaduse § 47 toetab vaid rahumeelse kogunemise õigust. Mitmetes riikides on mõiste tõlgendus olnud ülemäära kitsas, piirates lubamatult õiguse ulatust. Kuigi mõistet *rahumeelne* on Euroopa Inimõiguste Kohtu praktikas kohaldatud peamiselt võrguühenduseta kogunemiste suhtes, on võrguühenduseta ja veebimaailmade tarbeks õiguse ristrakendamine ühe sujuvam. Digitehnoloogiat võivad kasutada kõik meelevaldustel osalevad sidusrühmad alates ajakirjandusest kuni politsei ja meelevaldajateni.

Kogunemis- ja ühinemisvabadus on tehnoloogianeutraalne põhivabadus, mistõttu see kohaldub ühetaoliselt nii võrguühenduseta maailmas kui ka infoühiskonnas. Internet, infoühiskonnas toimivad muud võrgustikud ja eelkõige sotsiaalsõrgustikud on olulised vahendid, mis võimaldavad teostada põhiseaduse §-s 47 sätestatud õigust kogunemis- ja koosolekuvabadusele, pakkudes võimalusi suurendada üksikisikute osalemist poliitilises, sotsiaalses ja kultuurielus¹⁵⁰. Seega on võimalik tehnoloogiat kasutada nii vabaduse teostamise koha kui ka vahendina. Kogunemise võib organiseerida sisuliselt mõne tunni jooksul, ilma et peaks teiste korraldajatega kohtuma (kui need on olemas), sest kogu teabevahetus võib toimuda veebis. Samamoodi saab luua ühise eesmärgiga üksikisikute rühma ja koguda sotsiaalmeedia kaudu mõne tunni jooksul tuhandeid toetajaid, ilma et sellel rühmal oleks struktuuri, põhikirja või et seda peaks registreerima. Neid võib pidada mitteametlikeks ühendusteks, millel on suur organisatsiooniline potentsiaal oma liikmete ühise eesmärgi saavutamiseks. Mitteametlikud ühendused on alati olemas olnud, kuid internet on hõlbustanud nende loomist ja teavitustööd ning igapäevast tegutsemist.¹⁵¹

Vabadus kasutada internetiplatvorme, näiteks sotsiaalmeediat, et asutada ühendusi ja organiseerida rahumeelseid kogunemisi ja proteste, on kogu maailmas saanud oluliseks kodanikuühiskonna aktivistide ja meelevaldajate seas.¹⁵² Kogunemiste ja meelevalduste ajal ja pärast seda saab internetti kasutada mitmel eesmärgil: avalikustamiseks (eriti kui üritus ei leia traditsioonilises meedias piisavalt kajastamist), et mõista hukka politsei liigne jõukasutamine, jagada ajakohast teavet (näiteks kust leida meditsiinilist abi haiguspuhangute korral), väljendada toetust nende poolt, kes ei saa üritusel viibida, küsida või pakkuda abi, suhelda pere ja sõpradega. Samuti loob ühingu- ja kogunemisvabadus internetis võimalused ülemaailmseteks liikumisteks¹⁵³, kodanikuühiskonna kaasamiseks¹⁵⁴, avalike debattide

¹⁴⁹ EIK, 44158/98, Gorzelik jt vs. Poola, 17.02.2004, p 88.

¹⁵⁰ Euroopa Nõukogu internetivabaduse komitee. Freedom of assembly and association on the Internet. MSI-INT (2014)08, 2015.

¹⁵¹ *Ibid.*

¹⁵² Recommendation to member States on the protection of human rights with regard to social networking services. Committee of Ministers. 04.04.2012. CM/Rec(2012)4; Recommendation to member States on Internet freedom. Committee of Ministers. 13.04.2016. CM/Rec(2016)5; Recommendation to member States on a Guide to human rights for Internet users. Committee of Ministers. 16.04.2014. CM/Rec(2014)6; Barberá, P., Metzger, M. Tweeting the Revolution: Social Media Use and the #Euromaidan Protests. – HuffPost 21.02.2014; Tufekci, Z. Twitter and Tear Gas: The Power and Fragility of Networked Protest. Yale University Press 2017.

¹⁵³ Näiteks talgud „Teeme ära“, mis said alguse 2008. aastal ja milles esimesel aastal osales Eestis vaid 50 000 inimest, on nüüdseks saanud 180 riiki hõlmavaks liikumiseks, millesse on kaasatud miljoneid inimesi üle maailma. – <http://www.letsdoitworld.org>.

¹⁵⁴ Näiteks Euroopa kodanikualgatus, mis võimaldab EL-i kodanikel otseselt osaleda EL-i poliitika väljatöötamises ja kutsub Euroopa Komisjoni üles esitama seadusandlikku ettepanekut. – https://europa.eu/citizens-initiative/home_et.

algatamiseks¹⁵⁵, petitsioonide koostamiseks ja ühishankimiseks (*crowdsourcing*) ning digitaalses keskkonnas toimuvateks lokaalseteks, regionaalseteks¹⁵⁶ või globaalseteks¹⁵⁷ protestideks.

Nagu kõiki teisi vahendeid saab ka internetti ja teisi võrgutööriistu kasutada ka õigusvastastel eesmärkidel, näiteks vaenu või vägivalda õhutamiseks. Terroristlikud rühmitused võivad internetti ja teisi info- ja kommunikatsioonitehnoloogiaid kasutada oma ideoloogia edastamiseks, oma tegevuse kohta juhiste andmiseks, värbamiseks või piltide edastamiseks.¹⁵⁸ Sellise tegevusega seotud väljendusvormid ei kuulu Euroopa inimõiguste konventsiooni kaitse alla, neid vaagiks Euroopa Inimõiguste Kohus vaenuõhutuse konventsiooni artikli 17 alusel.

Põhiseaduse § 47 ja Euroopa inimõiguste konventsiooni artikli 11 kohaselt peavad kõik rahumeelse kogunemise vabaduse ja ühinemisvabaduse piirangud olema seadusega ette nähtud, taotlema õiguspärast eesmärki ja olema demokraatlikus ühiskonnas vajalikud. Euroopa Kohus on tavapäraste kogunemisvabaduse riivetena nimetanud kogunemiskeeldu; ennetavaid kinnipidamisi ning kogunemise kohale ligipääsu piiramist; jõuga kogunemise laialiajamist ning kogunemisjärgseid karistusi. Ennetava meetmena info jagamise blokeerimise kohta on Euroopa Inimõiguste Kohus teinud otsuse asjas *Kablis vs. Venemaa*, milles kohus leidis, et sotsiaalvõrgustike konto ja kolme blogikande blokeerimine põhjendusega, et need sisaldasid üleskutseid osaleda avalikul üritusel, mille asukohta linnavalitsus ei olnud heaks kiitnud, kujutas endast sõnavabaduse õiguse riivamist. Tegemist on üheselt ka kogunemisvabaduse riivega.¹⁵⁹

Euroopa Inimõiguste Kohus on andnud hinnangu ka üleskutsele osaleda rahumeelsel protestil, mis tõi kaasa üleskutsuja arreteerimise ja karistamise. Küsimus kerkis esile kohtuasjas *Elvira Dmitriyeva vs. Venemaa*. Dmitriyeva kutsus sotsiaalmeedias inimesi üles osalema üritusel, mis pidi toimuma asukohas, mida ametivõimud ei olnud heaks kiitnud. Euroopa Inimõiguste Kohus leidis, et kuna avalike ürituste korraldamise menetluse rikkumine oli väike, ei tekitatud tegelikku avaliku korra rikkumise või kuriteo ohtu ega kahjustatud potentsiaalselt avalikku julgeolekut ega inimeste õigusi, ei olnud hagejale trahvi määramine õigustatud. Muu hulgas rõhutas kohus otsuses, et avalikeks kogunemisteks eelloa puudumine ja sellest lähtuv tegevuste n-ö õigusvastasus ei anna ametiasutustele *carte blanche*'i ning piiravate meetmete rakendamisel tuleb lähtuda ka proportsionaalsuse nõudest (art 11). Sellest järeldub, et asjaolu,

¹⁵⁵ Näiteks erinevate tähiste kasutamine, millest populaarseim on teemaviite # kasutamine, mida nimetatakse *hashtag*'i aktivismiks. Hea näide on #metoo liikumine erinevate sotsiaalplatvormide kaudu; vt nt Zacharek, S. *The Silence Breakers*. – *Time Magazine*, 6.12.2017.

¹⁵⁶ Näiteks autoriõiguste direktiivi vastased protestid enne selle vastuvõtmist Euroopa Parlamendis, kus paljud veebilehed n-ö pandi kinni 24 tunniks; vt Evdokimova, T. *Online Protests Sweep European Internet Ahead of Copyright Law Vote*. – *Slate* 21.03.2019.

¹⁵⁷ Näiteks 2018. aastal alguse saanud #metoo liikumine, mille kohta ÜRO inimõiguste raportöörid ja eksperdid avaldasid teatise: „Avaldame austust vapratele naistele, kes on rääkinud seksuaalse ahistamise ja muude seksuaalse vägivalda vormide vastu, mille ohvriks on langenud kuritarvitavate meeste tõttu, kes on jäänud karistamata, kuna selline vägivald on ühiskonnas normaliseeritud. Oma julgete tegudega on need naised algatanud ülemaailmse liikumise, mille käigus on naised murdnud vaikuse müüri seksuaalse ahistamise ja kõigi teiste seksuaalse vägivalda vormide ees.“ – *International Women's Day Statement by United Nations Women's Human Rights Experts*. – OHCHR 06.03.2018.

¹⁵⁸ Brookingsi Instituudi uuringus hinnati, et 2014. aasta septembrist detsembrini kasutasid vähemalt 46 000 Twitteri kontot Da'eshi toetajad, terrorirühmitus, mis nimetab end Islamiriigiks; vt Berger, J. M., Morgan, J. *The ISIS Twitter census: Defining and describing the population of ISIS supporters on Twitter*, Brookings Paper, 2015. a märts.

¹⁵⁹ EIK, 48310/16, *Kablis vs. Venemaa*, 30.04.2019.

et hageja rikkus seadusega kehtestatud keeldu, kutsudes üles osalema avalikul üritusel, mida ei olnud nõuetekohaselt heaks kiidetud, ei ole iseenesest piisav, et õigustada sekkumist tema sõnavabadusse.¹⁶⁰

Info- ja kommunikatsioonitehnoloogia kaudu kogunemis- ja ühinemisvabaduse kasutamisel on suhteliselt lihtne tuvastada üritusel osalevaid isikuid ja selle organiseerijaid, samuti on lihtne jälgida ühinemise või meeleavalduse kulgemist. Just massjälgimine ja teised inimeste eraellu sekkumised, mida tehakse seoses õiguskaitse ja riikliku julgeolekuga ning teenuse osutaja poolt, on saamas ühinemis- ja kogunemisvabaduse proovikiviks. Endine ÜRO eriraportöör Martin Scheinin on inimõiguste ja põhivabaduste edendamise ja kaitse kohta öelnud:

„Massjälgimine ohustab ka ühinemis- ja kogunemisvabadust. Need vabadused nõuavad sageli erakohtumisi ja teabevahetust, et võimaldada inimestel organiseeruda valitsuste või teiste võimukandjate palge ees. Laiendatud jälitusvolitused on mõnikord viinud „pädevuste ekstsessini“, kui politsei või luureagentuurid on nimetanud rühmitusi terroristlikeks, et saaks kasutada jälitusvolitusi, mis anti ainult terrorismivastaseks võitluseks. Ameerika Ühendriikides kandis Marylandi osariigi politsei enne New Yorgi ja Denveri poliitilisi meeleavaldusi terroristide jälgimisnimekirjadesse keskkonnahoiu eest seisvad ja muud rahumeelsed meeleavaldajad. Ühendkuningriigis säilitatakse poliitilistel protestiüritustel tehtud valvekaamera pilte andmebaasis. Ühendkuningriigis hiljuti tehtud küsitlusest selgus, et kolmandik inimesi ei soovi meeleavaldustel osaleda, kuna nad on mures oma privaatsuse pärast.“¹⁶¹

Paljudes riikides on rakendatud nn interneti sulgemist: näiteks takistatakse avalike meeleavalduste ajal juurdepääsu interneti- ja sideteenustele. Nii piiratakse inimeste kogunemis- ja ühinemisvabadust. Nii-öelda interneti sulgemine toimub siis, kui häiritakse tahtlikult internetiühendust või mobiilirakendusi, et kontrollida, mida inimesed ütlevad või teevad. Interneti sulgemisi nimetatakse mõnikord ka katkestusteks või tapmislülititeks. Teabe vaba liikumine on tsiviilrahutuste ajal hädavajalik, kuid interneti sulgemine takistab osalejatel omavahel suhelda ning meedial kohapealsest olukorrast aru anda. Ajakirjanikke võidakse takistada oma allikatega rääkimast ning julgeolekujõudude toime pandud vägivalda ja inimõiguste rikkumisi kajastamast.¹⁶² Euroopa Inimõiguste Kohus on öelnud, et liiga laialdasi piiranguid või blokeerimiskorraldusi, mis takistavad juurdepääsu veebiteenustele või internetiühendusele, ei saa pidada proportsionaalseteks piiranguteks.¹⁶³

Algoritmide toimimist sotsiaalmeediaplatformidel ja suurt hulka kättesaadavaid isikuandmeid saab kasutada ka inimeste jälgimiseks ja tuvastamiseks, sealhulgas kogunemiskutseteks, millel võib olla oluline negatiivne mõju kogunemisvabadusele.¹⁶⁴ Rahvusvahelise õiguse,

¹⁶⁰ EIK, 60921/17, *Elvira Dmitriyeva vs. Venemaa*, 30.04.2019, p 84.

¹⁶¹ ÜRO resolutsioon A/HRC/13/37, p 36.

¹⁶² Näiteks #IAmTheSudanRevolution demonstratsioonid 2019. aasta juunis. Nädala jooksul pärast Sudaani interneti sulgemist tapeti 100 inimest, üle 700 sai vigastada ja vähemalt 70 vägistati. Interneti sulgemise tõttu oli ajakirjanikel äärmiselt keeruline kajastada kogu nädala jooksul toime pandud inimõiguste rikkumisi. Vt Access Now. #IAmTheSudanRevolution: There's a direct link between internet shutdowns and human rights violations in Sudan! 2019.

¹⁶³ EIK, 3111/10, *Yildirim vs. Turkey*, 18.03.2013.

¹⁶⁴ Näitena võib tuua tehisintellekti idufirma Dataminr, millel on reaajas juurdepääs kõigile Twitteri säutsudele. Firma pääseb ligi protestide korraldajate ja neil osalejate säutsudele ja asukohaandmetele. Twitterit kasutavad need inimesed oma tegevuse koordineerimiseks ja avalikustamiseks. 2020. a suvel avastati, et Dataminr müüs

eelkõige ÜRO äritegevuse ja inimõiguste juhtpõhimõtete kohaselt on ettevõtetel eriline kohustus austada kõiki inimõigusi, sealhulgas järgida diskrimineerimiskeeldu. Tehnoloogiaettevõtete poliitika ja tavad, sealhulgas nende võim otsustada, kelle häält võimendatakse ja keda vaigistatakse, mõjutavad otseselt rahumeelse kogunemise ja ühinemise õigust. Nende probleemidega seisavad järgmistel aastakümnetel silmitsi kõik riigid .

Kokkuvõte

Tehnoloogia mõju inimõigustele võib olla väga positiivne, sest tehnilised lahendused võimaldavad kaitsta sõnavabadust, kindlustada sõnumisaladust, levitada ideid või leida soovitud informatsiooni. Laialdase tehnoloogia kasutuse ja andmete rohkusega on aga seotud ka hulgaliselt probleeme, mis kõik mõjutavad suuremal või vähemal määral üksikisiku õiguste kaitset. Eriti problemaatiline on nende riikide praktika, kus tehnoloogiat kasutatakse elanikkonna lausjälgimiseks, profileerimiseks ning muude demokraatlikku ühiskonda iseloomustavate õiguste ebaproportsionaalseks kitsendamiseks.

Siinses peatükis keskendusime inimõiguste kaitse ning tehnoloogiaga seotud peamistele probleemidele. Privaatsuse ning isikuandmete kaitse valdkonnas on õiguslikke probleeme palju ning väärib kriitilist arutelu, kas tänapäeval tehnoloogiaajastul on privaatsus vaid illusioon või õnnestub meil siiski säilitada oma privaatne sfäär, ükskõik kui õbluke. On tõsi, et privaatsuse tähendus on juba ühe põlvkonna jooksul väga palju muutunud ning täpsustub ka edaspidi meie igapäevaste harjumuste kujunemise käigus. Sellele vaatamata tuleb privaatsust hinnata ja kaitsta ning meile kõigile tuleks kasuks, kui teeksime aeg-ajalt n-ö privaatsuse inventuuri ja analüüsiksime, kes ja kuidas meie andmetele ligi pääseb ning kes neid kasutab. Samuti tuleb tähelepanu pöörata sellele, kuidas laialdane tehnoloogia kasutamine on muutnud meie eraelu ning kodu kaitset.

Privaatsusega seotud probleemide kõrval vaatlesime peatükis ka õigus- ja praktilist raamistikku, mis reguleerib digimaailmas toimetamist, kui soovime oma seisukohta väljendada, infot leida, jagada või hoopis toetuda meid iga päev abistavatele uutele nutistu ja teistele tehisintellekti tehnoloogiatele. Näiteks on tehnoloogia selgelt võimendanud väljendusvabaduse mõju, sest teave levib internetis kiiresti ja ulatuslikult ning võib jääda ringlema ka siis, kui selle sisu pole enam asjakohane. Samamoodi võib internetis kerge vaevaga levitada libauudiseid ja valeinfot, mille looja võib olla nii inimene kui ka tehisintellekt. Kogunemis- ja ühinemisvabaduse kasutamisel võimaldab aga tehnoloogia suhteliselt kergesti tuvastada üritustel osalevaid isikuid ning jälgida ühinemise või meeleavalduse kulgemist, mida võib omakorda õigusvastastel eesmärkidel ära kasutada.

Riikide õiguste ja kohustuste kõrval tuleb rõhutada ka tehnoloogiaid arendavate ning kasutavate ettevõtete vastutust. Muret teeb see, et ei ole piisavalt läbipaistev, kuidas tehnoloogiafirmad koguvad ja kasutavad isikuandmeid või mil määral vastutab digitaalne platvorm kasutajate loodud sisu eest. Samamoodi nagu riikidel on ka tehnoloogiaettevõtetel kohustus ja vastutus austada, kaitsta, järgida ja viia ellu inimõigusi.

Kuigi praeguseks on õiguspõhimõttena fikseeritud, et virtuaalmaailmas kohalduvad õigused samamoodi nagu pärismaailmas, on kahjuks selge, et info- ja kommunikatsioonitehnoloogiat

USA õiguskaitseorganitele juurdepääsu liikumise Black Lives Matter protestiürituste andmetele (pärast George Floyd'i mõrva), sealhulgas rahumeelsete meeleavaldajate asukohaandmetele. Vt lähemalt Biddle, S. The Intercept. Police Surveilled George Floyd protests with help from Twitter-affiliated startup Dataminr. – The Intercept 09.07.2020.

aktiivselt kasutaval inimesel on aina keerulisem virtuaalruumis oma õigusi teostada. Seega on oluline suurendada teadlikkust sellest, mil määral tehnoloogiate kasutamine mõjutab meie õiguste kaitset, kuidas kasutavad tehnoloogiat riigid ja ettevõtted ning mida saame oma õiguste kaitseks ette võtta. See teema on eriti oluline sellisele riigile nagu Eesti, mille toimimine on üles ehitatud digilahendustele, mis töötlevad inimeste isikuandmeid, ning mille kodanikel on suur usaldus e-teenuste vastu. E-riigina peaks Eesti olema teistele riikidele eeskujuks ka õiguskindluse ja läbipaistvuse, seadusandluse päevakohasuse ning üksikisiku kaitse tagamisel.