

25. Tehnoloogia ja inimõigused

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 digitaalseid 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 saadetud 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 eraettevõtetega. Mitmed tehnoloogilised 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 kaamerate 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 sagenenud 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 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 uute tehnoloogiate – nagu näiteks tehisintellekt ja algoritmiliste süsteemid – kasutuselevõtmisega. Tehisintellekti puhul on enim kõlapinda tekitanud otsimootorite, algoritmilise ennustamise ja isikupärastamise (profileerimine), algoritmilise modereerimise ja algoritmide poolt sisu loomisega seonduvad tehnoloogiad ja nende kasutamise. Arusaadavalt on ülemaailmsetel digitaalsetel platvormidel ning uutel tehnoloogiatel suur mõju nii üksikisikute kui ka ühiskondade teabekeskondadele, 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 massjälgimine 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 peatükis analüüsimegi, kuidas inimõiguste standardeid austades eespool nimetatud väljakutsetega rinda pista.

- [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, aktiivsusemonitorid 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. (toim). Eesti Vabariigi põhiseadus. Kommenteeritud väljaanne. 2020, p 10. – <https://pohiseadus.ee/sisu/3514>.
- [6](#)Näiteks võimaldab Tor võrk kasutada internetti 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. Vt 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 selfie (selfi) või ka laiemalt 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.
- [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.