5. Väljendusvabadus, tehisintellekt, algoritmilised süsteemid, profileerimine

Väljendusvabaduse põhiõiguse teostamine on järjest enam surve all seoses selliste uute tehnoloogiate nagu tehisintellekti ja algoritmiliste süsteemide kasutuselevõtmisega.

Tehisintellekt viitab süsteemidele, mis näitavad intelligentset käitumist, analüüsides keskkonda ja võttes meetmeid – teatud autonoomiaga – konkreetsete eesmärkide saavutamiseks.1 Tehisintellektil põhinevad süsteemid võivad olla puhtalt tarkvarapõhised, virtuaalmaailmas toimivad (nt häälabi rakendus, pildianalüüsi tarkvara, otsingumootorid, kõne- ja näotuvastussüsteemid) või integreeritud riistvaraseadmetesse (nt arenenud robotid, autonoomsed mootorsõidukid, droonid või nutistu ehk asjade internetirakendused).2

Tehisintellekti puhul on kõige rohkem kõlapinda tekitanud algoritmilised süsteemid ja andmetöötlustehnikad, millel on tohutu 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.3 Samal ajal dikteerivad otsingumootorite algoritmid seda, mida ja millises järjekorras kasutajad näevad, ning nendega võidakse manipuleerida sisu piiramiseks või prioriseerimiseks4 , 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.5

Otsingualgoritm võib olla kallutatud ka teatud liiki sisu või sisupakkujate suhtes, nii riskitakse sellega seotud väärtuste, näiteks meedia pluralismi ja mitmekesisuse mõjutamisega.6 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.7 Need uurimised põhinevad konkurentsiõigusel, kuid on samavõrra olulised põhiõiguste seisukohast.

Ülemaailmsetel digitaalsetel platvormidel on suur mõju nii üksikisikute kui ka ühiskondade teabekeskkondadele, 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 reaalajas ja ülemaailmsel 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.8 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 märkimisväärseid 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.9

5.2. Algoritmilised otsused

Sotsiaalmeediaplatvormide kasutajate eelistuste algoritmilised ennustused ei juhi mitte ainult seda, milliseid reklaame inimestele näidatakse, vaid nende kaudu isikupärastatakse ka otsingutulemusi ja dikteeritakse, kuidas sotsiaalmeediakanalid, sealhulgas uudislehed, on korraldatud. Arvestades selliste platvormide suurust, nende kesksust paljude internetikogemuste jaoks poolavaliku sfäärina10 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.11

Andmepõhise infokeskkondade isikupärastamine kasutajate profileerimise kaudu toob kaasa võimalused manipuleerida inimestega peenel, kuid väga tõhusal viisil.12 Individuaalsel tasandil võib manipuleerimine ohustada isiklikku autonoomiat ja tekkivat õigust kognitiivsele suveräänsusele.13 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.14

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.[15] 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.”[16]

Algoritmiliste süsteemide hankimine, loomine, arendamine ja kasutuselevõtt on nii Euroopa Nõukogu[17] kui ka Euroopa Komisjoni[18] kümnete õigusintrumentide ese. Samas riigi tasandil seadusandjad alles kaaluvad, milline on õige ja tõhusaim õigusraamistik ja poliitika, et tagada inimõiguste kaitse, takistamata samas tehnoloogia arengut.

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.[19]

Selliste nähtude vastu on riigil vähe võimalusi meetmeid rakendada: 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.[20] Euroopa Inimõiguste Kohus on leidnud, et olukorras, kus riik otsustas teatud ebasoovitava sisu blokeerida, kuid sellega kaasnes ka õiguspärase sisuga veebilehtede blokeerimine, tõi see kaasa mõju paljudele internetikasutajatele ja seeläbi piirati omavoliliselt ka kaebaja sõnavabadust.[21] 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.

- 1Tehisintellekti legaaldefineerimises ei ole eksperdid kokkuleppele jõudnud ning see definitsioon on Euroopa Komisjoni tehtud legaaldefinitsiooni ettepanek. High Level Expert Group on AI, A Definition of AI: Main Capabilities and Disciplines. – European Commission 08.04.2019.
- 2Ibid.
- 3Recommendation 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.
- 4ÜRO arvamus- ja sõnavabaduse edendamise ja kaitse eriraportööri David Kaye’ 2016. aasta aruanne inimõiguste nõukogu 32. istungjärgul (A/HRC/32/38).
- 5Maruste, R., Turk, K. Paragrahv 45. – Madise, Ü. (toim). et al. Eesti Vabariigi põhiseadus. Kommenteeritud väljaanne. 2020, p 10. − https://pohiseadus.ee/sisu/3514p 49; vt ka Saxena, R. The social media „echo chamber“ is real. − Ars Technica 2017/3. – https://arstechnica.com/science/2017/03/the-social-media-echo-chamber-is-real/ (25.09.2020).
- 6UNESCO. World Trends in Freedom of Expression and Media Development. – http://www.unesco.org/new/en/world-media-trends (25.09.2020).
- 7Euroopa 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_a (13.09.2021).
- 8Wagner, 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.
- 9Mitmed 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.

- 10York, J. C. Policing Content in the Quasi-Public Sphere. MA: Open Net Initiative Bulletin. Berkman Center. – Boston: Harvard University 2010.
- 11Maruste, R., Turk, K. Paragrahv 45. – Madise, Ü. (toim). et al. Eesti Vabariigi põhiseadus. Kommenteeritud väljaanne. 2020, p 10. − https://pohiseadus.ee/sisu/3514p 49; p 49; 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.
- 12Yeung, 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.
- 13Teatavat 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.
- 14Gorton, 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).
- 15Yeung, K. Hypernudge: Big Data as a mode of regulation by design. – Information, Communication & Society 2016, lk 1–19.
- 16Korff, 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).

- 17Euroopa Nõukogu ministrite komitee soovitus liikmesriikidele algoritmiliste süsteemide mõjust inimõigustele. 08.04.2020. – CM/Rec(2020)1.
- 18Euroopa Komisjoni kõrgetasemeline tehisintellekti eksperdirühm. Eetikasuunised usaldusväärse tehisintellekti arendamiseks, 2019. –https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/JURI/DV/20 06/Ethics-guidelines-AI_ET.pdf (13.09.2021).
- 19Horowitz, 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.
- 20Tackling Online Disinformation: A European Approach, COM(2018) 236 final, Euroopa Komisjon, 26.04.2018, lk 2.
- 21EIK, 3111/10, Ahmet Yildirim vs. Türgi, 18.12.2012.