TARTU ÜLIKOOL

ÕIGUSTEADUSKOND

Avaliku õiguse osakond

Omar Kõiv

SÜVAVÕLTSINGUTE LOOMISE JA LEVITAMISEGA SEONDUVAD OHUD NING NENDE MAANDAMINE KEHTIVA ÕIGUSLIKU RAAMISTIKU ABIL

Magistritöö

Juhendaja

dr. *iur*. Mario Rosentau

Tartu

2025

SISUKORD

SISSEJUHATUS

Viimaste aastate jooksul on generatiivse tehisintellekti (edaspidi: TI) valdkonnas toimunud märkimisväärne areng, mis on kaasa toonud hulgaliselt innovaatilisi lahendusi ning mõjutanud olulisel määral majandust ja ühiskonda. Kuigi TI täpsete mõjude hindamine on selle tehnoloogilise uudsuse tõttu hetkel keeruline, valitseb ekspertide seas üldine konsensus, mille kohaselt TI rakendamisest tulenev mõju on vähemalt majanduslikus mõttes valdavalt positiivne. Näiteks prognoosib Goldman Sachs, et tulenevalt laialdasest TI kasutusest võib oodata järgneva kümne aasta jooksul kuni 7% suurust (ligikaudu 7 triljonit USA dollarit) globaalset SKP kasvu ning USA tootlikkuse aastast kasvu 1,5% ulatuses.[1] Sarnast optimistlikku hinnangut jagab ka McKinsey & Company, kelle arvutuste kohaselt võib generatiivse TI potentsiaalne kasu maailmamajandusele ulatuda kuni 25,6 triljoni dollarini, mis tähendaks arenenud riikide aastase SKP kasvu suurenemist 1,5–3,4% võrra.[2] Siiski leidub ka konservatiivsemaid hinnanguid, näiteks MIT professor Daron Acemoglu on arvamusel, et USA-s jääb tootlikkuse kasv järgmisel kümnendil ligikaudu 0,66% juurde aastas.[3] Kokkuvõtvalt võib siiski nentida, et laialdaselt peetakse TI-tehnoloogia kasutuselevõttu oluliseks teguriks majanduskasvu, tootlikkuse ja innovatsiooni edendamisel erinevates sektorites.

Üha laiemale avalikkusele kättesaadavaks muutunud generatiivsed TI-süsteemid võimaldavad luua teksti ning realistlikuna näivat heli-, pildi- ja videomaterjali. Selliste tehnoloogiate hulka kuuluvad ka süvavõltsingud (ingl *deepfakes*), mis on süvaõppe- ja TI-mudelite rakendamisel loodud realistlikud võltsingud.[4] Avalikkus puutus süvavõltsingutega esmakordselt kokku 2017. aastal, mil Redditi kasutaja nimega deepfakes avaldas esimesed laiemalt tuntud näited süvavõltsingute abil loodud pornograafilistest videotest.[5] Sellest ajast on süvavõltsingute tehnoloogia muutunud kättesaadavamaks, tõhusamaks ja realistlikumaks ning on leidnud ka mitmeid kasulikke rakendusi. Näiteks filminduses kasutatakse süvavõltsingute tehnoloogiat

[1] Acemoglu, D. The simple macroeconomics of AI. – Economic Policy 2025/40 (121), lk 16. https://doi.org/10.1093/epolic/eiae042 (23.03.2025).
[2] *Ibidem*.
[3] *Ibidem*, lk 54.
[4] Das, M.K., *et al*. Deepfake Creation Using Gans and Autoencoder and Deepfake detection. – 2nd International Conference on Vision Towards Emerging Trends in Communication and Networking Technologies (ViTECoN), Vision Towards Emerging Trends in Communication and Networking Technologies (ViTECoN), 2023 2nd International Conference On 05.2023, lk 1. https://ieeexplore-ieee-org.ezproxy.utlib.ut.ee/stamp/stamp.jsp?tp=&arnumber=10157962 (25.04.2025).
[5] Somers, M. Deepfakes, explained. – MIT Management 21.07.2020. https://mitsloan.mit.edu/ideas-made-to-matter/deepfakes-explained (23.03.2025).

selleks, et näitlejaid digitaalselt noorendada[6], parandada nende kõne dubleerimist teistesse keeltesse[7] või tuua surnud näitlejaid uuesti kinoekraanile[8]. Samuti on leidnud süvavõltsingute tehnoloogia laialdast kasutust kunstilistes ja satiirilistes projektides.[9] Kuigi TI-süsteemide laialdased positiivsed rakendused on märkimisväärsed ja igati teretulnud, ei tohi ühiskond lasta end pimestada üksnes nende tehnoloogiate kasudest. Nagu tehnoloogia arengule tavaks, näitab ka süvavõltsingute tehnoloogia areng, et igal uuendusel võib olla varjukülg, mistõttu peab pöörama tähelepanu tehnoloogiaga kaasnevatele riskidele ning võimalikele kuritarvitustele.

Käesoleva magistritöö eesmärk on uurida ja kaardistada süvavõltsingutega seotud ohte ning analüüsida, mil määral võimaldab kehtiv õiguslik raamistik nendele ohtudele reageerida ja neid maandada. Eestis on süvavõltsingute temaatikat seni käsitletud vaid üksikutes analüüsides, näiteks kunsti[10] ja kriminaalmenetluse tõendamisaspektide[11] kontekstis. Käesoleva magistritöö uudsus seisneb süvavõltsingutega seotud ohtude senisest laiapõhjalisemas käsitlemises ning ohtudega seotud maandamis- ja reageerimismeetmete põhjalikus analüüsimises.

Probleemi aktuaalsus tuleneb süvavõltsingute üha laialdasemast väärkasutamisest, mis mõjutab otseselt nii üksikisikuid kui ka ühiskonda tervikuna. Eriti teravalt on esile kerkinud nende pahatahtlik kasutamine naiste- ja lastevastase seksuaalse väärkohtlemise vahendina. Süvavõltsingute tehnoloogia ohud ilmnevad ka demokraatlike protsesside ja avaliku infovälja kahjustamises. Lisaks kujutavad süvavõltsingud üha tõsisemat ohtu finantskuritegevuses. Süvavõltsingute realistlikkus ja kättesaadavus muudavad ehtsa ja võltsitud sisu eristamise järjest keerulisemaks, mis võib viia ulatusliku ühiskondliku usalduskriisini.

---

[6] Vilenkin, R. How De-aging Technology is Changing Hollywood & the Future of Film-making. – Respeecher 27.01.2021. https://www.respeecher.com/blog/de-aging-technology-changing-hollywood-future-film-making (23.03.2025).

[7] Felipe, R. M. Generative AI and deepfakes: a human rights approach to tackling harmful content. – International Review of Law, Computers & Technology 2024/38 (3), lk 299. https://www-tandfonline-com.ezproxy.utlib.ut.ee/doi/pdf/10.1080/13600869.2024.2324540 (24.04.2025).

[8] Chesney, B., Citron, D. Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security. California Law Review 2019/107 (6), lk 1770. https://heinonline-org.ezproxy.utlib.ut.ee/HOL/Page?collection=journals&handle=hein.journals/calr107&id=1806&men_tab=srchresults (24.04.2025).

[9] Ajder, H., Glick, J. Deepfakes, Satire, and the Politics of Synthetic Media. – Just Joking! The collaboration between Co-Creation Studio at MIT Open Documentary Lab and the human rights, video and technology network WITNESS 12.2021. https://cocreationstudio.mit.edu/just-joking/ (23.03.2025).

[10] Vt nt: Kinks, L. Loova tehisintellekti kasutamise võimalik mõju kujutava kunsti valdkonnale Eesti näitel. Magistritöö. Juhendaja Kadri Asmer. Tartu: Tartu Ülikool 2024. https://dspace.ut.ee/server/api/core/bitstreams/38937763-6937-4d75-a9b2-f43f67bc60aa/content (23.04.2025).

[11] Vt nt: Vahkal, H. Infotehnoloogia ja digivormi kasutamise perspektiivid tõendamisel kriminaalmenetluses. Magistritöö. Juhendaja Mario Rosentau. Tartu: Tartu Ülikool 2022. https://dspace.ut.ee/server/api/core/bitstreams/c5b8ec07-46de-4bc8-847a-61a432a1bfd6/content (23.04.2025).

Magistritöö raames otsitakse seega vastuseid järgmistele küsimustele: kuidas mõjutab süvavõltsingute tehnoloogia naiste- ja lastevastast seksuaalset väärkohtlemist; kuidas mõjutab see poliitilist manipulatsiooni ja desinformatsiooni levikut; kuidas mõjutab see finantskuritegevust ning mil määral suudab Eestis ja Euroopa Liidus kehtiv õiguslik raamistik süvavõltsingutest tulenevaid ohte maandada ja neile reageerida.

Magistritöö tugineb välismaistele ja Eesti allikatele, sealhulgas teadusartiklitele, uuringutele, kohtupraktikale, õigusaktidele ja ajakirjanduslikele materjalidele. Allikate analüüsimisel keskendutakse sellele, kuidas süvavõltsingud mõjutavad üksikisikuid ja ühiskonda laiemalt, milliseid võimalusi need pahatahtlikele isikutele loovad, ning millised on võimalused ohtudele reageerimiseks ja nende maandamiseks. Süvavõltsingutega seotud ohte illustreeritakse juhtuminäidetega, mis toovad välja süvavõltsingute tehnoloogia kuritarvitamise võimalused erinevates õiguslikes ja ühiskondlikes kontekstides.

Magistritöö esimene peatükk avab süvavõltsingute olemust, tutvustades nende kujunemislugu ning eripära võrreldes varasemate digitaalsete manipulatsioonitehnoloogiatega. Teises peatükis analüüsitakse süvavõltsingutest tulenevaid ohte kolmes eelnimetatud valdkonnas. Esiteks käsitletakse naiste- ja lastevastase seksuaalse väärkohtlemise ohtu, rõhutades süvavõltsingute rolli sihipärases kahjustavas käitumises. Teiseks analüüsitakse süvavõltsingute mõju demokraatlikele protsessidele ja avalikule infoväljale, keskendudes poliitilisele manipulatsioonile ning desinformatsiooni levikule. Kolmandaks vaadeldakse süvavõltsingute kasutamist finantskuritegevuses, mis ohustab nii ettevõtete kui ka üksikisikute majanduslikku turvalisust. Kolmandas peatükis analüüsitakse, mil määral suudab Eestis ja Euroopa Liidus kehtiv õiguslik raamistik maandada süvavõltsingutega seotud ohte ja neile reageerida.

Tööd iseloomustavad järgmised märksõnad: võltsingud, seksuaalne väärkohtlemine, lastepornograafia, desinformatsioon, pettus.

1. SÜVAVÕLTSINGUTE TEHNOLOOGIA ALUSED, AJALUGU NING ERISUSED VÕRRELDES VARASEMATE TEHNOLOOGIATEGA

Käesoleva peatüki eesmärk on käsitleda süvavõltsingute tehnoloogia aluspõhimõtteid ja toimemehhanisme, anda ülevaade selle kujunemisloost ning analüüsida, mil viisil erineb see varasematest sisumanipulatsiooni meetoditest.

1.1. Süvavõltsingute tehnoloogia alused

Süvavõltsing on audiovisuaalne esitus, millel kujutatu või kuuldu ei vasta tegelikkusele ja mis on loodud TI- ja süvaõppemudelite abil.[12] Tavapäraselt mõistetakse selle all manipuleeritud videot, pilti või helisalvestist, kus isiku nägu või keha on realistlikult asendatud teise isiku omaga, või kellegi hääl on tehislikult genereeritud nii, et ta näib ütlevat midagi, mida ta tegelikult öelnud ei ole. Termin *deepfake* tuleneb sõnadest *deep learning* (süvaõpe) ja *fake* (võlts).[13] Süvavõltsingute loomisel kasutatakse mitmeid tehnoloogiad. Levinumateks neist on vastandgeneratiivsed võrgud (ingl *generative adversarial network*, edaspidi: GAN), difusioonmudelid ja autokooderid.[14]

GAN on generatiivne mudel, mis koosneb kahest tehisnärvivõrgust: üks genereerib pilte juhuslike arvude põhjal (generatiivne võrk), teine aga hindab, kas pildid on ehtsad või tehislikult loodud (diskriminatiivne võrk). Generatiivset võrku treenitakse looma järjest realistlikumaid pilte, mida diskriminatiivne võrk ei suudaks pärisandmetest eristada. Samal ajal areneb ka diskriminatiivne võrk, muutudes osavamaks võltsingute äratundmisel. Pidev vastastikune treenimine viib lõpuks selleni, et generatiivne võrk suudab toota üha veenvamaid pilte.[15] Vastandgeneratiivseid võrke kasutatakse pildi-, kõne- ja tekstisünteesis.[16]

---

[12] Das, M.K., *et al*., lk 1.
[13] Mengesha, S., *et al*. Protecting Against Sexual Violence Linked to Deepfake Technology. – The Regulatory Review 13.04.2024. https://www.theregreview.org/2024/04/13/protecting-against-sexual-violence-linked-to-deepfake-technology/ (23.03.2025).
[14] Phipps, B., *et al*. AI image generation technology in ophthalmology: Use, misuse and future applications. – Progress in Retinal and Eye Research 2025/106, lk 3. https://www-sciencedirect-com.ezproxy.utlib.ut.ee/science/article/pii/S1350946225000266 (25.04.2025).
[15] Tampuu, A. Piltide genereerimine. Tehisintellekti Algkursus 2019/20. – Tartu Ülikool. Arvutiteaduse instituut. https://courses.cs.ut.ee/2020/Tehisintellekti_algkursus/Main/PARTIIIGen (23.03.2025).
[16] Bogdanov, D., *et al*. Tehisintellekti ja masinõppe tehnoloogia riskide ja nende leevendamise võimaluste uuring. Aruanne. – Riigi Infosüsteemi Amet ja Cybernetica AS 27.02.2024, lk 20. https://www.ria.ee/sites/default/files/documents/2024-03/Tehisintellekti-masinoppe-tehnoloogia-riskide-uuring-2024.pdf (23.03.2025).

Difusioonmudel on generatiivne mudel, mis koosneb pärisuunalisest protsessist, kus pärisandmetele lisatakse müra, ja vastassuunalisest protsessist, kus algset sisendit üritatakse müra eemaldades taasluua.[17] Difusioonmudeleid kasutatakse mudelites nagu DALL-E 3 ja Stable Diffusion, mis võimaldavad tekstiliste juhiste (ingl *prompt*) alusel pilte genereerida.[18] Stable Diffusion erineb DALL-E-st eelkõige seetõttu, et tegemist on avatud lähtekoodiga süsteemiga, mis võimaldab kasutajatel ise mudeleid treenida, sealhulgas süvavõltsingute loomiseks. DALL-E on suletud süsteem, mis on suunatud piiratud pildigeneratsioonile.[19] On aga leitud, et nii DALL-E kui ka Stable Diffusion on treenitud alaealiseid seksuaalsetes olukordades kujutaval materjalil.[20] Difusioonmudelid on GAN-idest uuem tehnoloogia, mille kasutamine süvavõltsingute loomisel muutub tõenäoliselt üha olulisemaks.[21] Kirjanduses on leitud, et teatud juhtudel on difusioonmudelid GAN-idest tõhusamad.[22] Samuti võib neid olla lihtsam treenida kui GAN-e.[23]

Autokooder on juhendamata tehisneurovõrk, mis koosneb kooderist ja dekooderist. Kooder saab sisendi ja transformeerib selle teisele kujule ja dekooder üritab transformeeritud sisendist esialgse sisendi taasluua. Treenitud kooderit saab kasutada sisendandmete mõõdete vähendamiseks, dekooderit aga andmete genereerimiseks. Üldiselt on autokooderi generatiivsed võimed piiratud, sest dekooderi sisendite lähedus ei garanteeri väljundi sarnasust.[24] Andmete genereerimiseks kasutatakse variatsioonilisi autokoodereid (ingl *variational autoencoder*, edaspidi: VAE). VAE-d suudavad anda lähedaste sisendite korral sarnaseid väljundeid.[25] VAE-d on leidnud rakendust realistlike piltide genereerimisel.[26]

Nagu iga tehnoloogia, muutuvad ka GAN-id, difusioonmudelid ja autokooderid ajas üha tõhusamaks, toetudes suurenevatele andmehulkadele ja kasvavale arvutusvõimsusele. Areng kiirendab sisuloomeprotsesse, vähendab kulusid ning muudab süvavõltsingute loomise

[17] Bogdanov, D., *et al*., lk 20.
[18] Swatton, P., Leblanc, M. What are deepfakes and how can we detect them? The science behind the tech that's transforming the online world. – The Alan Turing Institute 07.06.2024. https://www.turing.ac.uk/blog/what-are-deepfakes-and-how-can-we-detect-them (23.03.2025).
[19] Balarabe, T. Stable Diffusion Deepfakes: Creation and Detection. – Medium 10.12.2024. https://medium.com/@tahirbalarabe2/stable-diffusion-deepfakes-creation-and-detection-15103f99f55d (13.04.2025).
[20] Felipe, R. M., lk 299–300; 305.
[21] Swatton, P., Leblanc, M.
[22] Amerini, I., *et al*. Deepfake Media Forensics: Status and Future Challenges. – Journal of Imaging 2025/11 (3), lk 6–7. https://www.researchgate.net/publication/389456404 (23.03.2025).
[23] Swatton, P., Leblanc, M.
[24] Bogdanov, D., *et al*., lk 19.
[25] *Ibidem*, lk 19–20.
[26] Phipps, B., *et al*., lk 5.

lihtsamaks ja kättesaadavamaks.[27] Tulemuseks on üha realistlikumad võltsingud, mida on keerulisem eristada ehtsast sisust. Ei saa välistada ka uute tehnoloogiate esilekerkimist, mis võivad muuta süvavõltsingute tuvastamise veelgi keerulisemaks ning tuua kaasa nii uusi positiivseid kasutusvõimalusi kui ka riske.

1.2. Süvavõltsingute ajalugu

Süvavõltsingute tehnoloogia esimesi ilminguid võis täheldada juba 2010. aastatel.[28] Olulisemaks verstapostiks peetakse aga 2017. aastat, mil kasutaja nimega deepfakes jagas Reddit platvormil arvutiga genereeritud realistlikke võltsvideoid, milles tuntud naisnäitlejate näod olid paigutatud pornograafilise sisuga videoklippidele.[29] Platvormile loodi ka eraldi lehekülg r/deepfakes, mis oli pühendatud just süvavõltsingute jagamisele.[30] Sellest juhtumist pärineb mõiste „*deepfake*“, mis oli võltsingute looja kasutajanimi, ning mis kujunes sarnasel tehnoloogial põhinevate võltsingute üldtähiseks.[31]

2018. aastal pälvisid süvavõltsingud avalikkuse tähelepanu, kui uudisteportaal BuzzFeed, koostöös näitlejaga Jordan Peele, avaldas realistliku võltsvideo endisest USA presidendist Barack Obamast. Video eesmärk oli juhtida ühiskonna tähelepanu süvavõltsingute tehnoloogia väärkasutuse riskidele.[32] Samal perioodil muutus süvavõltsingute loomine ka tehniliselt lihtsamaks. Turule ilmusid esimesed kasutajasõbralikumad rakendused, näiteks FakeApp, mis võimaldasid süvavõltsinguid luua ka isikutel, kellel puudusid süvatehnilised oskused.[33] Esialgsed tulemused olid ebatäiuslikud: tehislikult loodud kujutised erinesid tegelikust inimesest ebaloomulike näoilmete, liigutuste või hääle poolest. Süvavõltsingute tehnoloogia on aga ajas märkimisväärselt arenenud, muutes võltsingud ehtsast materjalist üha raskemini

[27] Cybersecurity Information Sheet. Contextualising Deepfake Threats to Organizations. – National Security Agency, Federal Bureau of Investigation, Cybersecurity and Infrastructure Security Agency 12.09.2023, lk 10. https://media.defense.gov/2023/Sep/12/2003298925/-1/-1/0/CSI-DEEPFAKE-THREATS.PDF (21.04.2025).
[28] Łabuz, M. A Teleological Interpretation of the Definition of Deep Fakes in the EU Artificial Intelligence Act– A Purpose-Based Approach to Potential Problems With the Word “Existing”. – Policy & Internet 2024/17 (1), lk 3. https://doi-org.ezproxy.utlib.ut.ee/10.1002/poi3.435 (24.04.2025).
[29] Masood, M., *et al*. Deepfakes Generation and Detection: State-of-the-art, open challenges, countermeasures, and way forward. – arXiv 23.11.2021, lk 5. https://arxiv.org/pdf/2103.00484 (25.04.2025).
[30] Cole, S. Reddit Just Shut Down the Deepfakes Subreddit. – Vice 07.02.2018. https://www.vice.com/en/article/reddit-shuts-down-deepfakes/ (14.04.2025).
[31] Somers, M.
[32] Silverman, C. How To Spot A Deepfake Like The Barack Obama–Jordan Peele Video. – BuzzFeed 17.04.2018. https://www.buzzfeed.com/craigsilverman/obama-jordan-peele-deepfake-video-debunk-buzzfeed (23.03.2025).
[33] Conrad, L. Can deepfake technology be used for good? – Launched Tech News 31.05.2019. https://tbtech.co/news/can-deepfake-technology-be-used-for-good/ (25.04.2025).

tuvastatavaks. Lisaks visuaalsetele süvavõltsingutele on oluliselt arenenud ka inimhääle süvavõltsingud (ingl *voice deepfakes*).[34] Autentse kõlaga häälvõltsingu loomiseks piisab lühikesest helisalvestisest, mille põhjal suudab algoritm realistlikult matkida teise isiku häält.[35]

Süvavõltsingute levik on seejuures eksponentsiaalne. 2019. aasta alguses DeepTrace Labs poolt läbi viidud uuringus tuvastati internetist umbes 8000 süvavõltsinguvideot, kuid aasta lõpuks oli arv kasvanud peaaegu 15 000-ni, mis tähendab ligikaudu 100% kasvu.[36] Levik jätkus kiirenevas tempos: perioodil 2019–2020 teatati veebis leiduvate süvavõltsingute arvu suurenemisest 900% võrra.[37] On leitud, et 2023. aastal võis internetis levida 500 000 süvavõltsitud video- või heliklippi. Täiendavate prognooside kohaselt võib 2025. aastaks ulatuda internetis ringlevate süvavõltsingute arv 8 miljonini.[38] Tasub märkida, et eksponentsiaalne kasv ei tule üksnes pahatahtlike võltsingute arvelt. Internetis levivad ka meelelahutuslikud süvavõltsingud: näiteks süvavõltsitud Tom Cruise videod TikTokis, mis on loodud pigem naljaviljuks.[39] Kokkuvõtlikult võib öelda, et süvavõltsingud on lühikese ajaga kujunenud nišitehnoloogiast laialdaselt levinud nähtuseks.

[34] Ilmestamise eesmärgil on autor varasemalt loonud süvavõltsingu, milles Donald Trump näib rääkivat küberkiusamise ohtudest. Tegemist on tekstist kõneks sünteesitud võltsinguga, mille loomine võttis aega vaid poolteist minutit, ent mille hääl kõlab ehtsana. Kättesaadav: https://www.tryparrotai.com/video?id=xm5Ezv3di5cg (25.04.2025).

[35] Leffer, L. AI Audio Deepfakes Are Quickly Outpacing Detection. – Scientific American 26.01.2024. https://www.scientificamerican.com/article/ai-audio-deepfakes-are-quickly-outpacing-detection/ (23.03.2025).

[36] Ajder, H., *et al*. The State of Deepfakes: Landscape, Threats, and Impact. – Deeptrace 09.2019, lk 1. https://regmedia.co.uk/2019/10/08/deepfake_report.pdf (23.03.2025).

[37] Bueermann. G., Perucica, N. How can we combat the worrying rise in the use of deepfakes in cybercrime? – World Economic Forum 19.05.2023. https://www.weforum.org/stories/2023/05/how-can-we-combat-the-worrying-rise-in-deepfake-content/ (23.03.2025).

[38] Accelerated Capability Environment. Case Study. Innovating to detect deepfakes and protect the public. – GOV.UK 05.02.2025. https://www.gov.uk/government/case-studies/innovating-to-detect-deepfakes-and-protect-the-public (15.04.2025).

[39] Metz, R. How a deepfake Tom Cruise on TikTok turned into a very real AI company. – CNN Business 06.08.2021. https://edition.cnn.com/2021/08/06/tech/tom-cruise-deepfake-tiktok-company (23.03.2025).

1.3. Süvavõltsingute tehnoloogia erisused võrreldes varasemate tehnoloogiatega

Visuaalse ja auditiivse materjali tahtlik manipuleerimine ei ole iseenesest uus nähtus. Juba foto- ja filmitehnoloogia algusaegadest teatakse juhtumeid, kus pilte lavastati või töödeldi propagandistlikel ja poliitilistel eesmärkidel.[40] Autoritaarsed režiimid on kasutanud fotomanipulatsioone, et eemaldada fotodelt soovimatuid isikuid või levitada propagandat.[41] Digiajastu tõi kaasa tööriistad nagu Photoshop, mis muutsid visuaalse sisu manipuleerimise avalikkusele kättesaadavamaks. Tuleb aga toonitada, et süvavõltsingud erinevad oluliselt varasematest sisu manipuleerimise vahenditest.

Esiteks iseloomustab süvavõltsinguid erakordselt kõrge realismitase nii heli-, foto- kui ka videomaterjalis, mis muudab need raskesti eristatavaks ehtsast sisust.[42] Teiseks, kui varasemad tööriistad nõudsid teatud määral ikkagi tehnilisi oskusi ja aeganõudvat sisu käsitsi töötlemist, siis süvavõltsingute loomine toimub suures osas automatiseeritult. Selle tulemusel saavad ka vähese tehnilise pädevusega isikud luua veenvat manipuleeritud sisu, kasutades selleks vabalt kättesaadavaid rakendusi.[43] Kolmandaks, süvavõltsingute tehnoloogia võimaldab lühikese ajaga toota võltsitud sisu massiliselt, samas kui varasemate tööriistade abil loodi pigem üksikuid võltsinguid. See loob täiesti uue ulatusega manipuleerimisvõimalused, mida varasemad meetodid ei võimaldanud.[44] Security Hero 2023. aasta uuringu kohaselt kulus näiteks tasuta 60-sekundilise pornograafilise sisuga süvavõltsingu loomiseks alla 25 minuti.[45]

Süvavõltsingute tuvastamiseks on küll loodud erinevaid detektoreid, kuid ka need jäävad süvavõltsingute tehnoloogia arengule alla. Kirjanduses on leitud, et käesoleva põlvkonna detektorid ei ole levivate süvavõltsingute ühtlustatud tuvastamiseks piisavalt tõhusad.[46] Sisuliselt on tegemist pideva võidujooksuga, kus vähemalt hetkel on süvavõltsingute loomise tehnoloogia detektoreid võitmas. Kui isegi detektoritel on raskusi süvavõltsingute

[40] Deepfake Technology: A Brief History Worth Knowing. – European Identity Theft Observatory System 15.05.2024. https://eithos.eu/deepfake-technology-1-history-useful-to-know/ (23.03.2025).
[41] How Stalin's propaganda machine erased people from photographs, 1922-1953. – Rare Historical Photos 07.12.2021. https://rarehistoricalphotos.com/stalin-photo-manipulation-1922-1953/ (21.04.2025).
[42] Westerlund, M. The Emergence of Deepfake Technology: A Review. – Technology Innovation Management Review 2019/9 (11), lk 39. https://timreview.ca/sites/default/files/article_PDF/TIMReview_November2019%20-%20D%20-%20Final.pdf (21.04.2025).
[43] Chesney, R., Citron, D. K., lk 1762–1763.
[44] National Security Agency, Federal Bureau of Investigation, Cybersecurity and Infrastructure Security Agency, lk 10.
[45] 2023 State of Deepfakes. Realities, Threats, and Impact. – Security Hero 2023. https://www.securityhero.io/state-of-deepfakes/ (23.03.2025).
[46] Le, Binh M., *et al*. SoK: Systematization and Benchmarking of Deepfake Detectors in a Unified Framework. – arXiv 02.03.2025, lk 12. https://arxiv.org/pdf/2401.04364 (16.04.2025).

tuvastamisega, siis tavainimeste võimalused on veelgi piiratumad: neil puuduvad sageli nii vajalikud teadmised süvavõltsingute olemusest kui ka võimekus süvavõltsingute tuvastamiseks.[47] Realistlike süvavõltsingute massiline levik võib tõsiselt õõnestada avalikkuse usaldust digitaalsete materjalide vastu ja viia ühiskonna uude tõejärgsesse ajastusse, kus audiovisuaalne materjal ei ole enam usaldusväärne.

[47] Hancock, J. T., Bailenson, J. N. The Social Impact of Deepfakes. – Cyberpsychology, Behaviour, and Social Networking 2021/24 (3), lk 149. https://par.nsf.gov/servlets/purl/10233906 (23.03.2025).

2. SÜVAVÕLTSINGUTE LOOMISE JA LEVITAMISEGA SEONDUVAD OHUD

Käesoleva peatüki eesmärk on välja selgitada süvavõltsingute loomise ja levitamisega seotud peamised ohud naiste- ja lastevastase seksuaalse väärkohtlemise, poliitilise manipulatsiooni ja desinformatsiooni ning finantskuritegevuse kontekstis.

2.1. Süvavõltsingute loomine ja levitamine naiste- ja lastevastase seksuaalse väärkohtlemise kontekstis

Eelnevalt kirjeldatust ilmneb, et esimene valdkond, kus süvavõltsingute tehnoloogiat laialdaselt kuritarvitama hakati, oli pornograafilise sisuga materjalide tootmine ja levitamine. Õiguslikult on selliseid süvavõltsinguid hakatud mõistma kui pildipõhist seksuaalset väärkohtlemist (ingl *image-based sexual abuse*).[48] Eksperdid võrdlevad seda ka kättemaksupornoga (ingl *revenge porn*).[49] Uuringud kinnitavad, et enamik internetis levivatest süvavõltsingutest täidavad jätkuvalt just pornograafilist eesmärki. Deeptrace Labs 2019. aasta uuringust ilmnes, et ligi 96% tuvastatud süvavõltsingutest olid pornograafilise sisuga, kusjuures kõikidel juhtudel olid ohvriteks just naised.[50] Süvavõltsingute hulk internetis on viimastel aastatel järsult tõusnud: näiteks tuvastati Security Hero 2023. aasta uuringus ligikaudu 96 000 süvavõltsitud videot, millest 98% olid pornograafilise iseloomuga ning 99% juhtudest kujutati neis naisi.[51] Seega tasub märkida, et kuigi süvavõltsingute kontekstis räägitakse tihti poliitilistest ohtudest, viitavad uuringud sellele, et süvavõltsingute peamine oht avaldub eelkõige soopõhise ja seksuaalse väärkohtlemise vahendina.

Süvavõltsingute ohvriteks on avalikkusele teadaolevalt sattunud eeskätt naissoost avaliku elu tegelased. Tuntuimaks näiteks saab pidada lauljat Taylor Swift, kellest 2024. aastal loodud alandava sisuga süvavõltsingud kogusid ligikaudu 47 miljonit vaatamist.[52] Ent viimaste aastate jooksul on märgata selget tendentsi, mille kohaselt satuvad süvavõltsingute sihtmärgiks üha

[48] Briefing Paper: Deepfake Image-Based Sexual Abuse, Tech-Facilitated Sexual Exploitation and the Law. – Equality Now 17.01.2024, lk 4. https://audri.org/wp-content/uploads/2024/01/EN-AUDRi-Briefing-paper-deepfake-06.pdf (23.03.2025).
[49] Kelleher, K. Revenge Porn and Deep Fake Technology: The Latest Iteration of Online Abuse. – Boston University School of Law 10.08.2023. https://sites.bu.edu/dome/2023/08/10/revenge-porn-and-deep-fake-technology-the-latest-iteration-of-online-abuse/ (15.04.2025).
[50] Ajder, H., *et al*. 2019, lk 1–2.
[51] Security Hero.
[52] Contreras, B. Tougher AI Policies Could Protect Taylor Swift–And Everyone Else–From Deepfakes. – Scientific American 26.01.2024. https://www.scientificamerican.com/article/tougher-ai-policies-could-protect-taylor-swift-and-everyone-else-from-deepfakes/ (23.03.2025).

enam ka tavaisikud, kellest luuakse pornograafilise sisuga võltsinguid näiteks vaigistamise või ahistamise eesmärgil.[53] 2025. aasta seisuga võib seega praktiliselt iga isik – eriti naised, kes on ebaproportsionaalselt sagedamini sellise tegevuse sihtmärgiks – sattuda süvavõltsingute kaudu aset leidva seksuaalse vägivalla ohvriks, misläbi on probleem omandanud suured ühiskondlikud mõõtmed. 2021. aastal nimetas ÜRO naistevastase vägivalla eriraportöör pildipõhist seksuaalset väärkohtlemist varipandeemiaks, rõhutades probleemi laialdast levikut ning selle varjatust avaliku tähelepanu ees.[54]

Süvavõltsingute tehnoloogiatel põhinev digitaalne väärkohtlemine, mille aluseks on eelkõige jätkuvalt laialt levinud misogüünsed hoiakud, kujutab endast seega uut ja eriti ohtlikku relvaliiki naistevastase väärkohtlemise arsenalis. Olukorra muudab eriti tõsiseks asjaolu, et süvavõltsingute tehnoloogia puhul on tegemist sisuliselt piiramatu kasutuspotentsiaaliga vahendiga, millele pääseb ligi iga isik. Sellest tulenevalt on süvavõltsingud muutunud tõsiseks ja raskesti kontrollitavaks ohuks naiste põhiõigustele. Tehnoloogia võimaldab pahatahtlikel isikutel lihtsasti ja ilma ohvri nõusolekuta luua ning levitada intiimset või pornograafilist laadi süvavõltsinguid. Eesti Vabariigi põhiseaduse[55] (PS) tähenduses rikutakse sellise tegevusega mitmeid põhiõigusi, sealhulgas õigust au ja hea nime kaitsele (PS § 17), inimväärikusele (PS § 18), vabale eneseteostusele (PS § 19), eraelu puutumatusele (PS § 26) ja tervisele (PS § 28).

Oluline on rõhutada, et ohvrite seisukohast ei oma sisulist tähendust, kas levitatud materjal on ehtne või tehislikult loodud: psühholoogiline, emotsionaalne ja sotsiaalne kahju on sageli samaväärselt ränk.[56] Kirjanduses on selgitatud, et ohvril võib tekkida posttraumaatiline stressihäire, suitsidaalsus, ärevus, depressioon, usaldus- ja kontrollitunde kadumine. Kaasneda võivad ka kahjulikud toimetulekumehhanismid, nagu liigne alkoholi tarvitamine.[57] Lisaks võib ohvreid tabada märkimisväärne mainekahju, eriti kui süvavõltsingutega puutuvad kokku tööandjad, pereliikmed või teised ühiskondlikud sidusrühmad, mis võib omakorda viia ohvri sotsiaalse marginaliseerumiseni ning piirata tema tööalaseid ja ühiskondlikke võimalusi.[58]

---

[53] Dunn, S. Women, Not Politicians, Are Targeted Most Often by Deepfake Videos. – Centre for International Governance Innovation 03.03.2021. https://www.cigionline.org/articles/women-not-politicians-are-targeted-most-often-deepfake-videos/ (23.03.2025).
[54] Mengesha, S., *et al*.
[55] Eesti Vabariigi põhiseadus. – RT I, 15.05.2015, 2.
[56] Dunn, S. Legal Definitions of Intimate Images in the Age of Sexual Deepfakes and Generative AI. – McGill Law Journal 2024/69, lk 6. https://ssrn.com/abstract=4813941 (23.04.2025).
[57] McGlynn, C., *et al*. 'It's Torture for the Soul': The Harms of Image-Based Sexual Abuse. – Social & Legal Studies 2023/30 (4), lk 544. https://journals.sagepub.com/doi/pdf/10.1177/0964663920947791 (23.04.2025).
[58] Rigotti, C., McGlynn, C. Towards an EU criminal law on violence against women: The ambitions and limitations of the Commission's proposal to criminalise image-based sexual abuse. – New Journal of European Criminal Law 2022/13 (4), lk 459. https://journals.sagepub.com/doi/epub/10.1177/20322844221140713 (23.03.2025).

Kirjanduse kohaselt on sellise sisu levitajateks peamiselt mehed, kelle peamisteks motiivideks on võimu- ja kontrollivajadus, misogüünsed hoiakud, seksuaalne rahuldus, väidetav naljatlemine, ohvri alandamine ja sotsiaalse kapitali suurendamine.[59] Käitumise aluseks on sügavalt juurdunud struktuurne sooline ebavõrdsus, mis väljendub eriti selgelt nn „kollektsioneerimiskultuuris“, kus mehed süstemaatiliselt jagavad ja levitavad ilma nõusolekuta naiste intiimseid kujutisi nii avalikes veebikeskkondades kui ka kinnistes gruppides.[60]

Lisaks individuaalsetele mõjudele on täheldatav laiem ühiskondlik negatiivne mõju. Naised võivad hakata vältima aktiivset osalemist avalikus elus ja sotsiaalmeedias hirmust, et nende pilte kasutatakse süvavõltsingute loomisel. 2021. aastal läbi viidud uuringu kohaselt kardab ligikaudu 30% EL naistest, et neist võidakse levitada nõusolekuta loodud intiimse sisuga võltsinguid.[61] 2024. aastal teostatud uuring näitas, et koguni kaks kolmandikku naistest väljendavad tõsist muret võimaliku süvavõltsingute ohvriks langemise pärast.[62] Laiaulatuslik ja mõistetav hirm võib aga osutada naiste väljendusvabadust piiravaks ning ohustada naiste õigust võrdsele ühiskondlikule eneseteostusele, mis kujutab omakorda tõsist soolist ebavõrdsust süvendavat probleemi. Soolise ebavõrdsuse süvenemisele on juhtinud tähelepanu ka naiste õiguste ekspert Rangita de Silva de Alwis, kes on toonud esile, et sooline kübervägivald (sh süvavõltsingute loomine ja levitamine) pärsib naiste väljendusvabadust ja osalust avalikus elus, tekitades eriti naisajakirjanike ja naisaktivistide seas hirmu oma turvalisuse pärast.[63]

Süvavõltsingute tehnoloogia väärkasutamine ei piirdu üksnes täiskasvanutega. Üha enam ilmneb juhtumeid, kus on loodud lapspornograafiat kujutavaid süvavõltsinguid. Tegemist on laste seksuaalset väärkohtlemist kujutava materjaliga (ingl *Child Sexual Abuse Material*, edaspidi: CSAM). CSAM-i loomine on ekspertide hinnangul kujunenud üheks peamiseks süvavõltsingute kuritegelikuks kasutusviisiks. Kahetsusväärselt on tegemist kasvava trendiga,

[59] *Ibidem*, lk 458.
[60] *Ibidem*, lk 459–460.
[61] *Ibidem*, lk 457.
[62] Nearly two-thirds of women worry about being a victim of deepfake pornography, ESET UK Research reveals. – ESET 20.03.2024. https://www.eset.com/uk/about/newsroom/press-releases/nearly-two-thirds-of-women-worry-about-being-a-victim-of-deepfake-pornography-eset-uk-research-reveals/ (23.03.2025).
[63] Silva de Alwis, R., Vialle, E. Is AI-Facilitated Gender-Based Violence the Next Pandemic? – The Regulatory Review 06.05.2024. https://www.theregreview.org/2024/05/06/de-silva-de-alwis-vialle-is-ai-facilitated-gender-based-violence-the-next-pandemic/ (23.03.2025).

mis raugemise märke ei näita.[64] 2023. aasta Internet Watch Foundation (edaspidi: IWF) uuringus leiti, et 30-päevasel perioodil postitati ühele tumeneti foorumile 2978 TI abil loodud CSAM-i kujutist.[65] IWF 2024. aasta uuringus leiti, et samas ajavahemikus postitati 3512 kujutist.[66] Ohvriteks ei ole seejuures vaid lapse- ja teismeealised. Nähtub, et luuakse ka imikuid kujutavat CSAM-i.[67] Lisaks interneti süvakihtidele leidub CSAM-i ka avalikel veebilehtedel.[68] IWF raport näitab sedagi, et süvavõltsingute loomisel kasutatakse mudeleid, mida on treenitud nii reaalsel täiskasvanuid kujutaval kui ka reaalsel laste seksuaalset väärkohtlemist kujutaval materjalil.[69] Täiendavalt esineb üha enam videomaterjali, mis algselt kujutas täiskasvanuid, kuid mis on süvavõltsingutega muudetud alaealisi kujutavaks.[70] Olemuslikult võib selliseid süvavõltsinguid käsitada pseudo-pornograafilise materjalina, kus reaalse isiku nägu monteeritakse teise keha külge, luues näiliselt autentset, kuid tegelikkuses fabritseeritud pornograafilist sisu.[71] Süvavõltsingute tehnoloogia pidev treenimine reaalsel materjalil tähendab aga seda, et süvavõltsingud muutuvad aja möödudes üha autentsemaks, misläbi muutub üha keerukamaks eristada pärismaterjali fiktiivsest.[72]

Õiguslikult on niisugune tegevus enamikes riikides ühemõtteliselt kriminaalne. Ka pseudo-lapspornot käsitatakse samaväärselt reaalse laste seksuaalset väärkohtlemist kujutava materjaliga (näiteks Ühendkuningriigis on seadused, mis keelavad ebasündsa lapsepildi loomise, levitamise ja omamise, hõlmates ka pseudofotograafilisi ja täiesti fiktiivseid kujutisi).[73] Selliste süvavõltsingute kriminaliseerimisel on ka eluliselt mõistetav põhjendus. CSAM-i laiaulatuslik loomine ja levitamine ning selle kättesaadavus võib soodustada pedofiilide üleminekut reaalse laste seksuaalse väärkohtlemiseni. Seega, sõltumata sellest, et

---

[64] Dearden, L. AI increasingly used for sextortion, scams and child abuse, says senior UK police chief. – The Guardian 24.11.2024. https://www.theguardian.com/technology/2024/nov/24/ai-increasingly-used-for-sextortion-scams-and-child-abuse-says-senior-uk-police-chief (23.03.2025).

[65] How AI is being abused to create child sexual abuse imagery. Prompt: from fantasy to photo-realistic reality. – Internet Watch Foundation 10.2023, lk 27. https://www.iwf.org.uk/media/q4zll2ya/iwf-ai-csam-report_public-oct23v1.pdf (21.04.2025).

[66] AI CSAM REPORT UPDATE in conjunction with our Oct 23 report. What has changed in the AI CSAM landscape? Prompt: from fantasy to photo-realistic reality. – Internet Watch Foundation 07.2024, lk 20. https://www.iwf.org.uk/media/nadlcb1z/iwf-ai-csam-report_update-public-jul24v13.pdf (21.04.2025).

[67] Crawford, A., Smith, T. Illegal trade in AI child sex abuse images exposed. – BBC News 28.06.2023. https://www.bbc.com/news/uk-65932372 (23.03.2025).

[68] Internet Watch Foundation 2023, lk 10; 25.

[69] Internet Watch Foundation 2024, lk 17–18.

[70] *Ibidem*, lk 15.

[71] Nair. A. Real porn and pseudo porn: The regulatory road. – International Review of Law, Computers & Technology 2010/24 (3), lk 224. https://www-tandfonline-com.ezproxy.utlib.ut.ee/doi/epdf/10.1080/13600869.2010.523611 (21.04.2025).

[72] Dearden, L.

[73] Internet Watch Foundation 2024, lk 20.

süvavõltsingute abil loodud CSAM-is ei pruugi alati olla kujutatud tegelikke isikud (kuigi sageli on) võivad need süvendada pedofiilide kuritegelikku kalduvust ning tekitada seeläbi ühiskonda uusi ohvreid. Sellega seonduvalt on märgitud, et väär on argumentatsioon, mille kohaselt ei põhjusta TI abil loodud materjal kellelegi kahju.[74]

Kui varem tähendas lapspornograafia peamiselt reaalse väärkohtlemise dokumenteerimist ja levitamist, siis süvavõltsingute tehnoloogia võimaldab nüüd luua piiramatus koguses sünteetilist materjali. Selline sisu võib taasohvristada seksuaalset väärkohtlemist kogenud lapsi ning samal ajal süvendada, normaliseerida ja isegi julgustada pedofiilsete üksikisikute ning võrgustike tegevust. Näiteks on toodud IWF raportis esile juhtum, kus last väärkoheldi ajal, mil ta oli 3–8-aastane. Laps küll päästeti väärkohtleja käest, kuid temast toona tehtud pornograafilise sisuga pilte kasutatakse kurjategijate poolt tänase päevani. Seejuures kasutatakse temast loodud pilte, et luua uue sisuga CSAM-i, kus last kujutatakse uutes pornograafilistes situatsioonides, mida pedofiilsetes võrgustikes levitatakse.[75] Kurjategijad kasutavad süvavõltsingute loomiseks ka avalikult kättesaadavat materjali, seejuures näiteks sotsiaalmeediasse postitatud video- ja fotomaterjali. Sellega tehakse ohvriteks ka lapsed, keda pole kunagi reaalselt väärkoheldud.

2.1.1. Juhtuminäide: Almendralejo kaasus

2023. aasta septembris tuli Almendralejo linnas ilmsiks šokeeriv juhtum, kus teismelised poisid kasutasid nutitelefoni rakendust, et luua oma koolikaaslastest tüdrukute alastipilte. Rakendus ClothOff võimaldas ühe klikiga eemaldada fotodel olevatelt isikutelt riided. Poisid laadisid rakendusse üle 20 tüdruku Instagramist pärit süütud fotod (tüdrukud olid algmaterjalis kujutatud riietes) ning genereerisid nendest fotodest versioonid, kus tüdrukud olid alasti. Seejärel jagati pilte suhtlusrakendustes nagu WhatsApp. Juhtum põhjustas kogukonnas suurt nördimust. Tüdrukud, kellest mõned olid vaid 11-aastased, tundsid end alandatuna ja kartsid, et süvavõltsingud võivadki internetti ringlema jääda. Kerkis ka küsimus, kas seaduse silmis oli toime pandud kuritegu. Ühiskondlikult tõstatus nõudmine, et õigusraamistik peaks selliseid tegusid karistama.[76] Juhtum andis ka ainest aruteluks vanematele: kuivõrd peaks jälgima noorte

[74] Crawford, A., Smith, T.
[75] Internet Watch Foundation 2024, lk 3; 18.
[76] Llach, L. Naked deepfake images of teenage girls shock Spanish town: But is it an AI crime? – Euro News 24.09.2023. https://www.euronews.com/next/2023/09/24/spanish-teens-received-deepfake-ai-nudes-of-themselves-but-is-it-a-crime (23.03.2025).

nutitelefoni kasutust ja milliseid rakendusi on üldse lubatud alla laadida. Badajozi noortekohus mõistis 15 koolipoisile aastase tingimisi vangistuse, leides, et poisid olid loonud laste seksuaalset väärkohtlemist kujutavat materjali ning kahjustanud ohvrite moraalset terviklikkust.[77] Juhtum ilmestab, et lisaks seaduste ajakohastamisele vajadusele on tehnoloogia jõudnud tasemini, kus süvavõltsingute loomine pole vaid tehnoloogiaekspertide pärusmaa. Isegi lapsed suudavad seda lihtsate rakenduste abil teha. Seetõttu on kriitilise tähtsusega ennetustöö, et kujundada väärtushinnanguid noorte seas ja takistada selliste trendide normaliseerumist.

2.1.2. Avalikkuse teadlikkuse puudujäägid

Süvavõltsingutest tulenevatele ohtudele naiste- ja lastevastases seksuaalses väärkohtlemises on mõnel määral tähelepanu juhitud ka Eesti meedias. 10.03.2025 avaldatud Õhtulehe artiklis juhtis politseikapten Maarja Punak tähelepanu sellele, et TI abil loodud intiimseid kujutisi (alastipilte) on Eestis genereeritud juba aastaid ning et selliseid materjale kasutatakse sageli inimeste häbistamiseks, kiusamiseks või muul pahatahtlikul eesmärgil mõjutamiseks. Tema sõnul on Politsei- ja Piirivalveamet saanud korduvalt teateid, et selliseid kujutisi on loodud ning levitatud. Samas toonitas Punak, et kuigi igas vanuses isikust digitaalsete kujutiste loomine ise ei pruugi olla süüteona karistatav, on kahjustatud isikul võimalik pöörduda kohtusse isikukujutise loata kasutamise eest tuleneva kahju hüvitamiseks ja õigusrikkumise lõpetamiseks. Punak rõhutas, et digitaalsete kujutiste genereerimine on kriminaalkorras karistatav, kui loodud kujutis kujutab alla 18-aastast isikut pornograafilises poosis või alla 14-aastast isikut erootilises poosis. Selline tegevus on kooskõlas Eesti karistusseadustikus[78] (KarS) sätestatud lapspornograafiat keelavate normidega (KarS § 178). Lisaks tõi Punak esile, et alastipiltide levitamisega kaasneb ka väljapressimine, kus ohvritelt nõutakse raha, et pilte ei levitataks.[79] Tasub toonitada, et kui varasemas praktikas kasutati väljapressimiseks sageli just ohvri enda saadetud autentseid pilte (nt endisele elukaaslasele), siis süvavõltsingute

[77] Spain: Court punishes schoolboys for spreading AI deepfakes of girls. Scottish Legal News 10.07.2024. https://www.scottishlegal.com/articles/spain-court-punishes-schoolboys-for-spreading-ai-deepfakes-of-girls (21.04.2025).
[78] Karistusseadustik. – RT I, 12.12.2024, 6.
[79] Jõerand, R. DIGITAALNE ÕUDUS LEVIB! Süvavõltsitud alastifotod tekitavad ohvrites paanikahooge. – Õhtuleht 10.03.2025. https://www.ohtuleht.ee/1126142/digitaalne-oudus-levib-suvavoltsitud-alastifotod-tekitavad-ohvrites-paanikahooge? (23.03.2025).

tehnoloogia levikuga on muutunud tõenäolisemaks olukord, kus väljapressijad loovad võltsitud kujutised ise ning nõuavad ohvrilt raha, et kujutisi ei levitataks.

Märkimisväärne probleem seisneb ka asjaolus, et avalikkus ei mõista sageli, kui tõsiseid ja pikaajalisi tagajärgi võib digitaalne väärkohtlemine ohvritele põhjustada. Sageli alahinnatakse süvavõltsingute mõju võrreldes ehtsa materjali levitamisega. Internetifoorumites ja meediakommentaarides esineb seisukohti, et kuna süvavõltsingud on kunstlikult loodud ega kujuta endast ehtsat jäädvustust, ei tohiks need ohvrile põhjustada tõsist mõju ega emotsionaalset reaktsiooni. Näiteks on M. Punaku artikli all kasutanud kommentaator väljendit: „Kui on võltsing, mis seal siis pabistada?“[80] Teine kommenteerija rõhutas, et süvavõltsingud on lihtsalt järjekordne tehnoloogiline uuendus ega erine oluliselt Photoshop-tarkvaraga loodud manipulatsioonidest.[81] Kommenteerija soovitus oli, et endast ei tohiks ühtegi pilti üles laadida. Sarnaseid kommentaare leidus ka 2023. aasta artikli „Juristid hoiatavad: tehisaru avab küberkiusajatele uued horisondid. Üha enam asetatakse tüdrukute nägusid pornovideosse“ all avaldatud kommentaarides.[82] Nii leidis kommenteerija, et „no siis tuleb õppida elama, nii nagu päris pornostaarid õpivad elama oma loomingu taustal. ei ole võimalik võidelda tehnoloogilise progressiga.“ Kommentaar leidis ka toetust. Näiteks avaldati: „Ma toetan mõtet, et sellega ei saa võidelda ja tuleb õppida sellega elama. Mu nooruses tehti nii Brežnevile kui kinokangelastele ja lauljatele plakatitel ikka vuntsid ette ja algul oli „oi kui solvav“ aga see läks ruttu üle.“ Esile toodi seegi, et sisuliselt ei ole mingit erisust näiteks Photoshopiga töödeldud materjalil: „Üks asi et tuuleveskitega võitlemine ei maksa ja teine asi, et ega tegelikult probleemi olemus pole tehniline /.../. Ega AI videode, piltide, photoshoppide jms kõige muuga sisuliselt sama olukord, tõde ei puutugi üldse asjasse.“[83]

Kommentaarid, mille kohaselt süvavõltsingud ei põhjusta ohvritele tõsist kahju ega erine oluliselt näiteks Photoshopiga loodud manipulatsioonidest, on ekslikud ning põhinevad süvavõltsingute tehnoloogia olemuse ja mõju vääral mõistmisel. Erinevalt Photoshopist, mis nõuab tehnilisi oskusi ja ajakulu, võimaldab süvavõltsingute tehnoloogia peaaegu igaühel kiiresti, automatiseeritult ja massiliselt luua ning levitada realistlikku kahju tekitavat materjali. Just tehniline lihtsus, leviku kiirus ja kontrollimatus muudavad süvavõltsingud varasematest

[80] *Ibidem*.
[81] *Ibidem*.
[82] Kõiv, O., Ilves, M. Juristid hoiatavad: tehisaru avab küberkiusajatele uued horisondid. Üha enam asetatakse tüdrukute nägusid pornovideosse. – Eesti Päevaleht 04.11.2023. https://epl.delfi.ee/artikkel/120244858/juristid-hoiatavad-tehisaru-avab-kuberkiusajatele-uued-horisondid-uha-enam-asetatakse-tudrukute-nagusid-pornovideosse (23.03.2025).
[83] *Ibidem.*

sisumanipulatsioonidest oluliselt ohtlikumaks. Ka väide, et „kui tegemist on võltsinguga, pole põhjust muretseda“, eirab täielikult digitaalse väärkohtlemise reaalset mõju ohvrite vaimsele tervisele ja sotsiaalsele staatusele. Uuringud näitavad, et mittenõusolekul loodud intiimsed süvavõltsingud põhjustavad ohvritele emotsionaalset traumat, sotsiaalset tõrjutust ning pikaajalisi kahjusid era- ja tööelus. Seega ei ole küsimus materjali ehtsuses, vaid selles, kuidas ohver seda isiklikult tajub ning millist kahju see talle põhjustab. Samuti on väär seisukoht, et tehnoloogiliste arengutega pole mõtet võidelda. Selline seisukoht ignoreerib tõsiasja, et õiguslik regulatsioon ja ühiskondlikud normid ei ole staatilised, vaid peavad pidevalt kohanduma tehnoloogiliste muutustega, tagamaks inimeste põhiõiguste kaitset. Süvavõltsingute väärkasutus ei ründa üksnes üksikisikuid, vaid õõnestab ka ühiskonna toimimise aluseid. Sellised kommentaarid kajastavad paraku laiemat teadlikkuse puudulikkust süvavõltsingute tegelikust ohust.

2.1.3. Vahekokkuvõte

Süvavõltsingud kujutavad endast uut digitaalset vägivallavormi, mille kaudu kanduvad soopõhised ja seksuaalse väärkohtlemise ohud tehnoloogilisse keskkonda, võimendades seniseid probleeme raskemini tuvastataval viisil. Tegemist on uue relvaga naiste- ja lastevastases väärkohtlemises, mis ei ole võrreldav varasemate tööriistadega. Süvavõltsingute tehnoloogia võimaldab kiiresti ja vähese vaevaga luua väga realistlikku kahjustavat materjali, mida saab massiliselt levitada. Arvestades sotsiaalmeedia mõju, levib selline sisu laialdaselt, süvendades hirmu ja umbusaldust ning pärssides naiste avalikku ja sotsiaalset aktiivsust. Naised võivad peljata oma pilte jagada või arvamust avaldada, kartes sattuda väärkasutuse ohvriks. Laste puhul on tagajärjed veelgi rängemad, suurendades püsiva trauma ja taasohvristamise riski. Uuringud ja meediakajastused näitavad, et avalikkuse teadlikkus süvavõltsingute tegelikust mõjust on endiselt madal. Paljud alahindavad ohvrite kannatusi, mis on võrreldavad ehtsa materjali levitamisest põhjustatud kahjuga. Süvavõltsingute kättesaadavus ja visuaalne veenvus koos vähese teadlikkusega võivad aidata kaasa virtuaalse väärkohtlemise normaliseerumisele, näiteks naiste objektistamisele või laste seksualiseerimisele.

2.2. Süvavõltsingute loomine ja levitamine poliitilise manipulatsiooni ja desinformatsiooni kontekstis

Süvavõltsingute loomine ja levitamine võib kujutada ohtu demokraatlikule ühiskonnale, mille toimimise alusteks on usaldusväärne teave, teadlikud valijad ja faktidel põhinev avalik arutelu. Kodanikud langetavad poliitilisi otsuseid eeldusel, et neile esitatav info, sealhulgas näiteks avalikud debatid, mida vahendatakse televisiooni ja interneti kaudu, on autentne ning kajastab tõepäraselt poliitikute seisukohti ja tegevust. Süvavõltsingute tehnoloogia võimaldab aga luua võltsinguid, mis võivad moonutada tegelikku pilti poliitilistest sündmustest või poliitikutest. Näiteks 2023. aastal läbi viidud küsitluses väljendas 85% USA kodanikest muret, et süvavõltsingute levik võib kahjustada demokraatlikke protsesse.[84] Eriti ohtlikud on süvavõltsingud valimiste kontekstis, kus vahetult enne hääletust võib avalikkuseni jõuda veenev süvavõltsing, mis kujutab kandidaati kompromiteerivalt. Selline materjal võib sotsiaalmeedias kiiresti levida ja mõjutada avalikku arvamust enne, kui suudetakse tõendada selle võltsitud olemust.

Kuna inimesed omandavad suure osa teadmistest audiovisuaalsest materjalist, on autentne audiovisuaalne sisu kujunenud nn informatsiooni kuldstandardiks.[85] Selle standardi õõnestamine süvavõltsingute abil võib põhjustada tõsise üldise usalduskriisi, mille tulemuseks on ka demokraatlike protsesside ja avaliku diskursuse tõsine kahjustumine. Lisaks võimaldavad süvavõltsingud ära kasutada inimeste loomulikku kalduvust kinnistada oma olemasolevaid uskumusi.[86] Näiteks on võimalik luua süvavõltsinguid, milles poliitik või ekspert näiliselt kinnitab mingi grupi maailmavaatelisi stereotüüpe või eelarvamusi, tugevdades sellega ühiskonnas olemasolevaid konflikte ja polariseerumist. Kirjanduses on leitud, et näiteks poliitikut kujutava süvavõltsitud materjali nägemine, mõjutab negatiivselt võltsingut näinud isikute suhtumist kujutatud isikusse.[87] Veelgi enam, kui süvavõltsingut näidata kindlale sihtrühmale, keda sisu tõenäoliselt šokeerib (nt näidata religioossetele

[84] Goldstein, J. A., Lohn, A. Deepfakes, Elections, and Shrinking the Liar's Dividend. – Brennan Center for Justice 23.01.2024. – https://www.brennancenter.org/our-work/research-reports/deepfakes-elections-and-shrinking-liars-dividend (23.03.2025).
[85] Hancock, J. T., Bailenson, J. N., lk 150.
[86] Lovato, J., *et al*. Diverse misinformation: impacts of human biases on detection of deepfakes on networks. – npj Complexity 2024/5, lk 2. https://www.nature.com/articles/s44260-024-00006-y (25.04.2025).
[87] Hancock, J. T., Bailenson, J. N., lk 150.

inimestele poliitikut teotamas pühadusi), siis negatiivne mõju poliitiku mainele on veelgi suurem.[88]

Tasub märkida, et uuringud virtuaalreaalsuse kohta on näidanud, et realistlikud võltselamused võivad muuta mälestusi või isegi sisendada valemälestusi sündmustest, mida tegelikult pole toimunud.[89] Eeltoodu pinnalt võib seega väita, et süvavõltsingud võivad printsiibis mõjutada pikaajaliselt ka ühiskonna kollektiivset mälu ning ajaloolist tõde, tekitades valemälestusi, mida inimesed peavad autentseks. Ka olukorras, kus isikud ei lase end otseselt süvavõltsingutest petta, tekitab nende nägemine neis üldist ebakindlust meediatõdede vastu ning vähendab usaldust uudiste vastu.[90] Usk, et kõik meedias nähtav on niikuinii manipulatsioon, võib inimesed muuta vastuvõtlikumaks vandenõuteooriatele või vähendada osalust demokraatlikes protsessides. Eeltoodu võib omakorda luua soodsa pinnase autoritaarsetele tendentsidele ja ühiskonna killustumisele.[91]

Oluline aspekt süvavõltsingute mõjus demokraatiale seisneb nn „valetaja dividendi" (ingl *liar's dividend*) efektis. Õigusteadlased on ka hoiatanud, et avalikkuse teadlikkus süvavõltsingutest võib anda ebaausatele avaliku elu tegelastele võimaluse karistamatult valetada: kui avalikkus on teadlik süvavõltsingutest, võib neid olla lihtsam veenda, et ka ehtne materjal on tegelikult võltsitud.[92] Seega võimaldaks valetaja dividend avaliku elu tegelastel, keda on tabatud kompromiteerivates olukordades, vastutust vältida, väites, et tegemist on süvavõltsinguga.[93] Selline praktika raskendab aga oluliselt tõe tuvastamist ning õigusliku ja poliitilise vastutuse tagamist. Kirjanduses on siiski leitud, et valetaja dividendi rakendamine ei pruugi videomaterjali puhul anda soovitud tulemust. Seevastu näiteks väide, et poliitiku kohta kirjutatud artikli puhul on tegemist väärinfoga (ingl nn *fake news*), saavutab paremat efekti.[94]

Süvavõltsingud on muutunud oluliseks tööriistaks ka rahvusvahelises informatsioonisõjas. See on selgelt nähtav Venemaa Föderatsiooni poolt Ukraina vastu peetavas sõjas, kus süvavõltsinguid on kasutatud Ukraina presidendi diskrediteerimiseks ning ühiskondliku

[88] *Ibidem*.
[89] *Ibidem*, lk 149.
[90] *Ibidem*, lk 150.
[91] Nadal, D., Jančárik, P. Beyond the deepfake hype: AI, democracy, and "the Slovak case". – Harvard Kennedy School Misinformation Review 2024/5 (4), lk 3. https://misinforeview.hks.harvard.edu/article/beyond-the-deepfake-hype-ai-democracy-and-the-slovak-case/ (25.04.2025).
[92] Goldstein, J. A., Lohn.
[93] Chesney, B., Citron, D., lk 1785.
[94] Schiff, K. J., *et al*. The Liar's Dividend: Can Politicians Claim Misinformation to Evade Accountability? – American Political Science Review 2025/119 (1), lk 87. https://isps.yale.edu/research/publications/isps24-07 (23.03.2025).

moraali õõnestamiseks.[95] Informatsioonisõjas on oluline roll väärinfo massilisel levitamisel ning selle kulutõhususel pahatahtliku riigi jaoks. Just selles kontekstis pakuvad süvavõltsingud soodsat võimalust, kuna nende loomine on odav, tehniliselt lihtne ja neid on võimalik kiiresti ning laialdaselt levitada.[96] Rahvusvahelisel tasandil tunnistatakse süvavõltsingute probleemi üha laiemalt kui hübriidohtu, mis võib ohustada rahvusvahelist julgeolekut ja diplomaatilist stabiilsust. Ka Kaitsepolitseiameti 2024–2025 aastaraamatus on süvavõltsingute ohule tähelepanu juhitud ning märgitud, et sotsiaalmeedias nähtub üha enam süvavõltsinguid, mida võidakse kasutada valeinfo tootmiseks ja levitamiseks.[97] NATO on 2024. aastal oma strateegilistes dokumentides toonitanud, et süvavõltsinguid võidakse kasutada ühiskondade destabiliseerimiseks ja riikide vaheliste suhete pingestamiseks.[98] Seetõttu on välja pakutud ka rahvusvahelisi õiguslikke algatusi, näiteks ÜRO tasandil globaalseid leppeid, mis keelaksid süvavõltsingute kasutamise riikide poliitilise stabiilsuse ja julgeoleku kahjustamiseks.[99] Ei saa välistada ka seda, et arvestades süvavõltsingute kõrget realismitaset, võib kriisiolukorras tekkida olukord, kus otsustajad peavad tegutsema kiiresti, tuginedes teabele, mis osutub hiljem süvavõltsinguks.

2.2.1. Juhtuminäide: Keir Starmeri häälvõltsing (2023)

2023. aastal langes tänane Ühendkuningriigi peaminister Keir Starmer süvavõltsingul põhineva sihitud rünnaku ohvriks. Temast loodi häälvõltsing, mis kujutas teda ropendamas ja agressiivselt oma alluvatesse suhtumas. Poliitikud andsid pühapäeval avalikkusele hoiatuse sellise võltsingu leviku kohta, kuid juba esmaspäeva pärastlõunaks oli salvestist vaadatud X

[95] Williamson, E. Q&A: With Zelenskyy Surrender Hoax, the Feared Future of Deepfakes Is Here. – UVA Today 17.03.2022. https://news.virginia.edu/content/qa-zelenskyy-surrender-hoax-feared-future-deepfakes-here (23.03.2025).
[96] Smith, H., Mansted, K. Weaponised Deep Fakes: National Security and Democracy. – Australian Strategic Policy Institute 2020, lk 11–12. https://www.jstor.org/stable/resrep25129.7?seq=1 (21.04.2025).
[97] Aastaraamat 2024-2025. – Kaitsepolitseiamet 14.04.2025, lk 4; 43. https://kapo.ee/sites/default/files/content_page_attachments/aastaraamat-2024-2025_0.pdf (21.04.2025).
[98] Bjola, C. Algorithmic invasions: How information warfare threatens NATO's eastern flank. – Nato Review 07.02.2025. https://www.nato.int/docu/review/articles/2025/02/07/algorithmic-invasions-how-information-warfare-threatens-nato-s-eastern-flank/index.html (23.03.2025).
[99] Byman, D. L., *et al*. Deepfakes and International Conflict. – Foreign Policy at BROOKINGS 02.2023, lk 11. https://www.brookings.edu/wp-content/uploads/2023/01/FP_20230105_deepfakes_international_conflict.pdf (23.03.2025).

platvormil (endine Twitter) üle 1,5 miljoni korra.[100] Seega, isegi kui avalikkust suudetakse võltsingust kiiresti teavitada, levib manipuleeritud sisu sotsiaalmeedias kiiresti ja laialdaselt.

2.2.2. Juhtuminäide: Slovakkia häälvõltsingud (2023)

2023. aastal toimus Slovakkias juhtum, kus Progressiivse Slovakkia erakonna juhi kohta levis kaks häälvõltsingut. Esimeses kujutati juhti korrumpeerununa. Võltsingust kõlas, et juht kiitles valimispettuste läbiviimisega, mis haakus Slovakkias levitatava venemeelse desinformatsiooniga.[101] Teisest võltsingust kõlas, et plaanitakse tõsta õlle hinda.[102] Progressiivne Slovakkia kaotas valimised, kuid ei ole teada, kui suurt mõju süvavõltsingud valimistulemustele omasid.[103] Juhtub illustreerib ilmekalt, kuidas süvavõltsinguid saab kasutada poliitilise kandidaadi maine kahjustamiseks.

2.2.3. Juhtuminäide: Gaboni poliitiline kriis (2019)

Gaboni juhtum on üks esimesi maailmas, kus pelk kahtlus süvavõltsingu kasutamisest tõi kaasa reaalse poliitilise kriisi. Pärast president Ali Bongo salapärast kadumist insuldi tõttu avaldati video, mis pidi kinnitama tema elusolekut, kuid mille ebatavaline sisu tekitas ühiskonnas kahtlusi võltsimise kohta. Kuigi video ei osutunud tõestatult süvavõltsinguks, vallandas just selle tajutud võltslikkus 2019. aasta alguses riigipöördekatse.[104] Juhtum illustreerib süvavõltsingutega seotud infokindluse kriisi. Ainuüksi oletus manipuleeritud materjalist võib õõnestada riigi poliitilist stabiilsust ja julgeolekut.

[100] Bristow, T. Keir Starmer suffers UK politics' first deepfake moment. It won't be the last. – Politico 09.10.2023. https://www.politico.eu/article/uk-keir-starmer-labour-party-deepfake-ai-politics-elections/ (23.03.2025).
[101] Berthier, V. As the investigation into a Slovak journalist Monika Tódová's "deepfake" is reopened, RSF is calling for this type of attack to be criminalised. – Reporters Without Borders 06.03.2024. https://rsf.org/en/investigation-slovak-journalist-monika-t%C3%B3dov%C3%A1-s-deepfake-reopened-rsf-calling-type-attack-be (25.04.2025).
[102] Devine, C., *et al*. A fake recording of a candidate saying he'd rigged the election went viral. Experts say it's only the beginning. – CNN Politics 01.02.2024. https://edition.cnn.com/2024/02/01/politics/election-deepfake-threats-invs/index.html (25.04.2025).
[103] Nadal, D., Jančárik, P., lk 5.
[104] Ajder, H., *et al*. 2019, lk 10.

2.2.4. Juhtuminäide: Malaisia seksiskandaal (2019)

Malaisias levis seksuaalse sisuga video, milles figureeris toonane Malaisia majandusminister Mohamed Azmin Ali koos meessoost partneriga (Malaisias on homoseksuaalsed suhted kriminaliseeritud). Minister tugines väitele, et tegemist on süvavõltsinguga.[105] Hoolimata ekspertide järeldustest ja meessoost abi kinnitusest, et video ei olnud manipuleeritud, jäi avalikkus lõhestatuks ning poliitiline kahju piirdus maineplekkidega.[106] Juhtum peegeldab valetaja dividendi mõju: juba ainuüksi võimalus väita, et tegu on süvavõltsinguga, andis poliitikule võimaluse skandaalist osaliselt pääseda. Juhtum ilmestab, kuidas süvavõltsingute väitele tuginedes on võimalik luua ühiskondlikku segadust, ning näitab, kuidas tehnoloogia areng võimaldab süüdistusi ümber lükata ka ilma faktipõhise aluseta.

2.2.5. Juhtuminäide: Volodõmõr Zelenskõi süvavõltsing (2022)

2022. aasta märtsis, vahetult pärast Venemaa Föderatsiooni invasiooni Ukrainasse, levis internetis süvavõltsing, milles president Volodõmõr Zelenskõi näis kutsuvat ukrainlasi üles relvi maha panema ja alistuma. Video ilmus hetkeks isegi Ukraina telekanali otseülekandes ning ringlemine sotsiaalmeedias viitas selle levitamisele osana Venemaa infosõja strateegiast. Kuigi Zelenskõi reageeris kiiresti ehtsa vastuvideoga ja platvormid eemaldasid võltsingu, ilmus samal päeval ka vastureaktsioonina võltsitud video Venemaa Föderatsiooni presidendist Vladimir Putinist. Mõlemad videod olid tehniliselt nõrgad, mis võimaldas võltsituse kiiret tuvastust, kuid need tähistavad esimesi dokumenteeritud juhtumeid, kus süvavõltsingut kasutati käimasoleva sõjalise konflikti mõjutamise eesmärgil.[107] Juhtum näitab, et süvavõltsingud on muutunud relvaks kaasaegses infosõjas, võimaldades vaenulikul poolel sihipäraselt mõjutada avalikku arvamust ja külvata segadust ka sõjaolukorras. Isegi kui võltsingud on tuvastatavad, võib nende mõju olla reaalajas levides märkimisväärne.[108] Selliste

[105] *Ibidem*.
[106] Zainul, E. No prosecution – Ag. – The Edge Malaysia 10.01.2020. https://theedgemalaysia.com/article/no-prosecution-%E2%80%94-ag (21.04.2025).
[107] Holroyd, M., Olorunselu, F. Deepfake Zelenskyy surrender video is the 'first intentionally used' in Ukraine war. – Euro News 16.03.2022. https://www.euronews.com/my-europe/2022/03/16/deepfake-zelenskyy-surrender-video-is-the-first-intentionally-used-in-ukraine-war (23.03.2025).
[108] *Ibidem*.

süvavõltsingutega püütakse murendada Ukraina ühiskondlikku moraali ja vähendada liitlasriikide toetust.

2.2.6. Vahekokkuvõte

Süvavõltsingud kujutavad demokraatiale ohtu kolmel tasandil. Esiteks võimaldab süvavõltsingute tehnoloogia levitada valeinfot, mis õõnestab valimiste ja poliitiliste otsuste usaldusväärsust. 2023. aasta juhtumid Ühendkuningriigis ja Slovakkias näitasid, kui kiiresti poliitikuid kahjustavad süvavõltsingud võivad levida ja avalikku arvamust mõjutada. Teiseks võib süvavõltsingute olemasolu soodustada valetaja dividendi efekti, kus ka tõeseid materjale võidakse pidada võltsinguteks, võimaldades poliitikutel vältida vastutust. Malaisia skandaal näitas, kuidas süvavõltsingu väide võib vähendada poliitilist vastutust ja süvendada ühiskondlikku lõhet. Kolmandaks avalduvad süvavõltsingute ohud kriisi- ja julgeolekusituatsioonides, nagu ilmnes Ukraina presidendi juhtumis. Samuti võivad süvavõltsingud pikemas perspektiivis moonutada kollektiivset mälu ja ajaloolist tõde, õõnestades usaldust meedia ja demokraatlike institutsioonide vastu ning suurendades haavatavust vandenõuteooriate ja autoritaarsete tendentside ees.

2.3. Süvavõltsingute loomine ja levitamine finantskuritegevuse kontekstis

Süvavõltsingud kujutavad üha suuremat ohtu ka finantskuritegevuses. Süvavõltsingute realistlikkuse kasv, tehnoloogia kättesaadavus ja madalad loomekulud loovad soodsa pinnase pettusteks, kus juba üks edukas skeem võib korvata kõik varasemad ebaõnnestumised ning tuua kuritegelikele võrgustikele märkimisväärset kasumit. Mida veenvamaks muutub võltsitud sisu, seda suurem on petuskeemide õnnestumise tõenäosus ja seeläbi ka motivatsioon investeerida üha keerukamatesse lahendustesse. Erakordselt realistlikud süvavõltsingud võimaldavad kurjategijatel kehastuda ettevõtete juhtideks, ametnikeks või muudeks autoriteetseteks isikuteks, luues olukordi, mis võivad viia majandusliku kahju tekkimiseni. Näiteks

Resemble.AI uuringu andmetel ulatus 2025. aasta esimeses kvartalis süvavõltsingutega seotud pettustest põhjustatud majanduslik kahju üle 200 miljoni USA dollari.[109]

2024. aasta uuringud näitavad, et 50% ettevõtetest on vähemalt korra kokku puutunud süvavõltsingutel põhinevate pettustega ning 66% finantsettevõtete juhtidest näevad tehnoloogias reaalset ohtu.[110] Hääle- ja videosüvavõltsingute juhtumite arv kasvab kiiresti – vastavalt 12% ja 20% võrreldes 2022. aastaga – mis näitab selgelt vajadust ennetus- ja tuvastusmeetmete arendamiseks.[111] Paraku on uuringute põhjal vastumeetmete tõhusus veel piiratud ning seniks jääb oluliseks ühiskondliku teadlikkuse tõstmine.[112] Tasub märkida, et süvavõltsingute tehnoloogiat kasutatakse ka petukõnede tegemiseks.[113]

Olulise ohukategooriana tuleb esile tuua ka finantsturgude manipuleerimine. Näiteks 2013. aastal põhjustas Associated Pressi kompromiteeritud Twitteri konto kaudu levitatud valeinfo USA presidendi vigastamisest aktsiaturgude lühiajalise, ent märkimisväärse languse.[114] Kuigi tegemist ei olnud süvavõltsinguga, näitab juhtum, kui tundlikud on finantsturud eksitava info suhtes.[115] Ei ole välistatud seegi, et süvavõltsingu tehnoloogia võimaldaks veenvate võltsingutega finantsturgu veelgi tugevamalt destabiliseerida.[116]

Süvavõltsingute levik kahjustab ka üldist usaldust finantssüsteemi vastu, eriti digitaalse panganduse ja autentimissüsteemide kontekstis. Hääle- ja näotuvastusel põhinevad kaitsemehhanismid võivad olla haavatavad, kui neid petetakse TI-l põhinevate võltsingutega. Näiteks on kasutatud kolmemõõtmelisi näorenderdusi ehk 3D-stiilis digitaalseid kujutisi, mis matkivad maskitaoliste visuaalide abil kellegi välimust ning võimaldavad eksitada

[109] Solberg, M. Q1 2025 Deepfake Incident Report: Mapping Deepfake Incidents. – Resemble.AI 04.2025, lk 2. https://www.resemble.ai/wp-content/uploads/2025/04/ResembleAI-Q1-Deepfake-Threats.pdf (22.04.2025).
[110] Deepfake Trends 2024. – Regula 2024, lk 5; 16. https://static-content.regulaforensics.com/PDF-files/0831-Regula-Deepfake-Research-Report-Final-version.pdf? (22.04.2025).
[111] *Ibidem*, lk 8.
[112] Deepfakes in the Financial Sector: Understanding the Threats, Managing the Risks. A Report by the FS-ISAC Artificial Intelligence Risk Working Group. – Financial Services Information Sharing and Analysis Center 10.2024, lk 15. https://www.fsisac.com/hubfs/Knowledge/AI/DeepfakesInTheFinancialSector-UnderstandingTheThreatsManagingTheRisks.pdf? (22.04.2025).
[113] Deep-Fake Audio and Video Links Make Robocalls and Scam Texts Harder to Spot. – Federal Communications Commission 08.06.2024. https://www.fcc.gov/consumers/guides/deep-fake-audio-and-video-links-make-robocalls-and-scam-texts-harder-spot (25.04.2025).
[114] Smith, H., Mansted, K., lk 11.
[115] *Ibidem*.
[116] *Ibidem.*

biomeetrilisi tuvastussüsteeme.[117] Selliste võltsingute abil on võimalik saada ligipääs finantsteenustele või konfidentsiaalsetele andmetele.

Süvavõltsingutest tulenevate ohtude majanduslik mõju on seejuures märkimisväärne. Prognooside kohaselt võib küberkuritegevusest, sealhulgas pettustest, põhjustatud kahju ulatuda 2025. aastaks üle 10 triljoni USA dollari aastas.[118] Prognoositud kahju suurus peegeldab tendentsi, et kuritegelikud skeemid muutuvad tehnoloogilise arengu toel järjest tõhusamaks ja laiahaardelisemaks, kasvatades oluliselt potentsiaalsete ohvrite hulka. Kuigi süvavõltsingud ei ole selle trendi kujunemisel ainus faktor, on need siiski oluliseks osaks kiirelt arenevas tehnoloogiapõhises kelmuste arsenalis. Nagu rõhutas USA Föderaalse Kaubanduskomisjoni (FTC) esinaine Lina Khan 2023. aastal, „TI turbolaeb (ingl *turbo-charges*) pettusi" – viidates sellele, kuidas uued tehnoloogiad suurendavad pettuseskeemide mõjuulatust, tõetruudust ja levimiskiirust.[119]

2.3.1. Juhtuminäide: Ühendkuningriigi häälkõne (2019)

2019. aastal Ühendkuningriigis aset leidnud juhtum, kus kurjategijad kasutasid tõenäoliselt süvavõltsitud häält, et petta ühe ettevõtte juhilt välja ligikaudu 220 000 eurot, oli esimene laialdaselt kajastatud äripettus, kus kasutati TI abil genereeritud häält.[120] Kuigi juhtumi detailid jäid osaliselt konfidentsiaalseks ning ettevõtte nime ei avalikustatud, kinnitas toimunut kindlustusfirma, kes märkis, et tegemist oli just süvavõltsitud häälega.[121] Juhtum tõi esile seni alahinnatud haavatavuse: ka telefonikõned, mida juhid olid seni pidanud usaldusväärseteks (hääl, aktsent ja intonatsioon), võivad olla tehnoloogia arengu tõttu ebaturvalised. Juhtum ilmestab, et tehnoloogia kiire areng eeldab finantskuritegevuse tõkestamisel proaktiivset lähenemist ja pidevat valmisolekut täiustada turvaprotsesse vastavalt uutele ohtudele. Realistlikud süvavõltsingud võivad eksitada isegi kõrgetasemelisi otsustajaid, mis rõhutab

[117] Sancho, D., Ciancaglini V. Surging Hype An Update on the Rising Abuse of GenAI. – Trend Micro 30.07.2024. https://www.trendmicro.com/vinfo/es/security/news/cybercrime-and-digital-threats/surging-hype-an-update-on-the-rising-abuse-of-genai (22.04.2025).
[118] Morgan, S. Cybercrime Facts and Statistics. 2021 REPORT: CYBERWARFARE IN THE C-SUITE. CYBERSECURITY VENTURES 21.01.2021, lk 1. https://cybersecurityventures.com/wp-content/uploads/2021/01/Cyberwarfare-2021-Report.pdf (22.04.2025).
[119] Ahmed, N., *et al*. Money scams: Deepfakes, AI will drive $10 trn in financial fraud, crime. – Business Standard 22.08.2023. https://www.business-standard.com/world-news/money-scams-deepfakes-ai-will-drive-10-trn-in-financial-fraud-crime-123082200083_1.html (23.03.2025).
[120] Somers, M.
[121] *Ibidem*.

vajadust tugevdada teadlikkust ning autentimis- ja kontrollimehhanisme kogu organisatsioonilises hierarhias.

2.3.2. Juhtuminäide: Hongkongi häälkõne (2020)

2020. aasta alguses sai Hongkongis tegutseva Jaapani ettevõtte harukontori juht telefonikõne isikult, kelle häält pidas ta oma emafirma direktoriks. Kõnes paluti kiireloomulise ülevõtmistehingu raames kanda määratud kontodele 35 miljonit USA dollarit. Kõnele järgnesid ka e-kirjad direktorilt ja isikult, kes esitles end tehingut koordineeriva advokaadina. Kuna kõik näis usutav – nii hääl, e-kirjad kui detailid –, kandis juht raha üle. Kuna pettus mõjutas ka Araabia Ühendemiraatides tegutsevaid isikuid, alustas juhtumi uurimist Dubai prokuratuur. Uurimise käigus tuvastati 17 kahtlusalust ning selgus, et raha liikus mitmetesse riikidesse.[122] Juhtum toob esile süvavõltsingutel põhinevate finantskuritegude rahvusvahelise mõõtme ja järjest keerukama iseloomu. Isikud kasutasid mitte ainult realistlikku häälvõltsingut, vaid sidusid selle koordineeritud e-kirjade ja usutava stsenaariumiga, mis harujuhti veenvalt eksitas. Seejuures ilmestab juhtum, et kui tegu pannakse toime mitme isiku poolt ja sellel on rahvusvaheline ulatus, muutuvad menetlused paratamatult keerukamaks, mis omakorda rõhutab vajadust tõhusa rahvusvahelise koostöö järele.

2.3.3. Juhtuminäide: Arup videokõne (2024)

2024. aasta alguses osales Hongkongis tegutseva Briti inseneriifirma Arup töötaja videokõnes, kus ekraanil kujutatud isikud näisid olevat ettevõtte kõrgemad juhid. Kõnes esitati usutav selgitus, mille alusel paluti töötajal kanda 200 miljonit Hongkongi dollarit (umbes 22,5 miljonit eurot) viiele erinevale pangakontole. Hiljem selgus, et tegemist oli keeruka süvavõltsingul põhineva pettusega, kus kasutati nii TI abil loodud hääli kui ka manipuleeritud pilti, et jätta mulje reaalsest videokoosolekust.[123] Juhtum ilmestab, kui ohtlikuks võivad süvavõltsingud

[122] Brewster, T. Fraudsters Cloned Company Director's Voice In $35 Million Heist, Police Find. – Forbes 02.05.2023. https://www.forbes.com/sites/thomasbrewster/2021/10/14/huge-bank-fraud-uses-deep-fake-voice-tech-to-steal-millions/ (22.04.2025).
[123] Milmo, D. UK engineering firm Arup falls victim to £20m deepfake scam. – The Guardian. https://www.theguardian.com/technology/article/2024/may/17/uk-engineering-arup-deepfake-scam-hong-kong-ai-video (22.04.2025).

kujuneda ärikeskkonnas, kus otsuseid tehakse virtuaalsuhtluse teel. Realistlikult lavastatud videokõne, milles kasutati nii manipuleeritud kujutisi kui ka häälvõltsingut, näitab, et ka kogenud töötajad võivad eksida, kui visuaalne ja auditiivne sisu jätab usaldusväärse mulje.

2.3.4. Vahekokkuvõte

Kokkuvõtvalt võib järeldada, et süvavõltsingute tehnoloogia kiire areng ja kasvav kasutus finantskuritegudes kujutab endast tõsist ja süvenevat ohtu. Realistlikkuse kasv, madalad loomekulud ja tehnoloogiline kättesaadavus soodustavad pettusi, kus juba üks edukas skeem võib tuua kuritegelikele võrgustikele märkimisväärset kasumit. Mida veenvamaks muutub võltsitud sisu, seda suurem on skeemide õnnestumise tõenäosus ja motivatsioon investeerida keerukamatesse lahendustesse. Finantssektor on süvavõltsingute suhtes eriti haavatav, sest tagajärjed ei piirdu üksnes rahalise kahjuga, vaid õõnestavad ka usaldust autentimissüsteemide vastu. Süvavõltsingutel põhinevad kuriteod hõlmavad veenvalt manipuleeritud heli- ja videomaterjali, millega eksitatakse juhte ja töötajaid. Seetõttu peavad õiguskaitseorganid ja finantsasutused kiiresti uuendama oma turvamehhanisme ja ennetusstrateegiaid, eeskätt hõlmab see teadlikkuse tõstmist. Arvestada tuleb ka, et süvavõltsingupettustel on sageli rahvusvaheline mõõde, mis muudab nende menetlemise keeruliseks ja kulukaks. Üks tõhusamaid viise nende mõju vähendamiseks on avalikkuse teadlikkuse tõstmine. Süsteemne ja järjepidev teavitustöö peab olema osa laiemast ennetusstrateegiast, tugevdades ühiskonna vastupanuvõimet digiajastu üha keerukamatele kuritegevuse vormidele.

3. KEHTIV ÕIGUSLIK RAAMISTIK EESTIS JA EUROOPA LIIDUS

Süvavõltsingute õiguslik raamistik on alles kujunemas. Seadusandjate ees seisab keeruline ülesanne: kuidas kaitsta ohvreid ja ühiskonda, ilma et see piiraks liigselt sõnavabadust, pidurdaks innovatsiooni või takistaks tehnoloogia kasulikku kasutamist. Käesoleva peatüki eesmärk on välja selgitada, mil määral suudab Eesti ja Euroopa Liidu õiguslik raamistik süvavõltsingutest tulenevaid ohte maandada ja neile reageerida. Tasub märkida, et EL on kujunenud süvavõltsingute regulatsiooni eestvedajaks, võttes selge suuna õiguslike lahenduste väljatöötamisele, mis arvestavad nii tehnoloogia kiire arenguga kui ka kaasnevate ühiskondlike ohtudega. EL-i käsitlus ei ole piirdunud pelgalt üldsõnaliste hoiatustega, vaid on asutud kehtestama konkreetseid ja kohustavaid norme, mis reguleerivad süvavõltsingute loomist, levitamist ning mõju ühiskonnale. Eestvedaja staatus on eriti oluline olukorras, kus mitmed maailma piirkonnad alles otsivad sobivat tasakaalu innovatsiooni ja kaitsemeetmete vahel.

3.1. Süvavõltsingute reguleerimise keerukus

Süvavõltsingute reguleerimine on keeruline, kuna tegemist on mitmeotstarbelise kasutusega tehnoloogiaga. Seda saab kasutada nii positiivsetel kui ka negatiivsetel eesmärkidel ning nagu eelnevates peatükkides selgitatud, hõlmavad ka kahjulikud kasutusviisid mitmeid erinevaid vorme. Tehnoloogia kiire areng tähendab, et uued riskid võivad esile kerkida ootamatult. Seega ei saa piirduda ühe regulatiivse lahendusega: vaja on paindlikku ja mitmekihilist lähenemist, mis suudaks kiiresti muutuva olukorraga kohaneda. Üheks keskseks küsimuseks on see, kelle tegevust tuleks reguleerida. Süvavõltsingute elutsükkel hõlmab mitmeid osapooli: tehnoloogia arendajaid, võltsingute loojaid ja võltsingute levitajaid (sealhulgas sotsiaalmeediaplatvorme), võltsingute vaatajaid ja edasilevitajaid ning võltsingute tõttu kannatavaid ohvreid. Tõhus regulatsioon eeldab, et iga osapoole roll ja vastutus oleks selgelt määratletud. Ainult nii on võimalik vältida olukordi, kus ülereguleerimine pärsib innovatsiooni, samal ajal kui regulatiivsed lüngad jätavad ohvrid kaitseta.

Õigusliku sekkumise keerukus seisneb muu hulgas selles, et süvavõltsingute loomise ja levitamise reguleerimisel tuleb pöörata tähelepanu ka süvavõltsingute elutsüklis osalevate subjektide õigustele ning kaaluda ja põhjendada õiguste riiveid. Kuna süvavõltsinguid luuakse peamiselt isikuandmete – näiteks isikut kujutavate fotode, videote ja helisalvestiste – alusel,

tõstatab see küsimuse, kas ja millistel tingimustel on selliste andmete töötlemine õiguspärane. Isikuandmete kaitse üldmäärus[124] (edaspidi: IKÜM) art 6 sätestab isikuandmete töötlemise seaduslikkuse tingimused, millest on täpsemalt räägitud alapeatükis 3.4.2.

Reguleerimisel on oluline hinnata, kas süvavõltsingutega seotud riske – eriti nõusolekuta intiimse sisu loomist ja levitamist – tuleks maandada eraõiguslike või karistusõiguslike meetmetega. Intiimsete süvavõltsingute levitamine rikub ohvri põhiõigusi ja põhjustab tõsist moraalset ja mainelist kahju. Eraõiguslikud meetmed ei pruugi üksi pakkuda piisavat heidutust ega taastada õiglustunnet. Seetõttu võiks oluline roll olla karistusõiguslikel meetmetel, mille rakendamine võib omada olulist preventiivset mõju ning ründaja kriminaalvastutusele võtmise korral rahuldada ohvri õiglustunnet. Kuigi Eestis puuduvad praegu süvavõltsinguid käsitlevad karistusnormid, on nende kehtestamine tekitatava kahju valguses põhjendatud ja vältimatult vajalik. Konkreetselt süvavõltsingutele suunatud karistusõiguslikud meetmed täiendaksid olemasolevaid eraõiguslikke meetmeid ning tagaksid ohvritele tõhusama kaitse ja pidurdaksid pahatahtlike süvavõltsingute levikut. Selles suunas on Eesti kohustatud ka liikuma. Euroopa Parlamendi ja nõukogu direktiivis (EL) 2024/1385[125] tuuakse esmakordselt süüteona esile nõusolekuta intiimse sisuga süvavõltsingute loomine ja levitamine. Tasub märkida, et sarnast lähenemist on asutud rakendama ka teatud USA osariikides.[126] Siiski kehtivad juba praegu Eestis karistusnormid, mida saab teatud juhtudel süvavõltsingutega seotud juhtumitele kohaldada. Täpsem käsitlus järgneb alapeatükis 3.3.2.

Kuna süvavõltsingute tehnoloogia on otseselt seotud generatiivsete TI-süsteemidega, on need kaks valdkonda tihedalt põimunud. Seega pole üllatav, et lisaks direktiivile 2024/1385, sisaldub otseseid viiteid süvavõltsingutele ka näiteks 2024. aastal jõustunud tehisintellekti määruses.[127] Otseselt süvavõltsingutele viitav regulatsioon näitab EL-i valmidust tunnistada süvavõltsinguid mitte üksnes uudse tehnoloogilise arenguna, vaid väga konkreetse sotsiaalse ja teatud juhtudel kriminaalse probleemina, mis nõuab sihitud õiguslikku reguleerimist. Seega võib öelda, et EL

[124] 27. aprilli 2016. aasta Euroopa Parlamendi ja nõukogu määrus (EL) 2016/679, millega kehtestatakse füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus). – ELT L 119, 4.5.2016, lk 1-88.
[125] 14. mai 2024. aasta Euroopa Parlamendi ja nõukogu direktiiv (EL) 2024/1385, mis käsitleb naistevastase vägivalla ja perevägivalla tõkestamist. – ELT L, 2024/1385, 24.5.2024.
[126] Graham, M. M. Deepfakes: Federal and state regulation aims to curb a growing threat. – Thomson Reuters 26.06.2024. https://www.thomsonreuters.com/en-us/posts/government/deepfakes-federal-state-regulation/ (23.03.2025).
[127] Euroopa Parlamendi ja nõukogu määrus (EL) 2024/1689, 13. juuni 2024, millega nähakse ette tehisintellekti käsitlevad ühtlustatud õigusnormid ning muudetakse määruseid (EÜ) nr 300/2008, (EL) nr 167/2013, (EL) nr 168/2013, (EL) 2018/858, (EL) 2018/1139 ja (EL) 2019/2144 ning direktiive 2014/90/EL, (EL) 2016/797 ja (EL) 2020/1828 (tehisintellekti käsitlev määrus). – ELT L, 2024/1689, 12.7.2024.

ei käsitle süvavõltsingute probleemi kitsalt uudse tehnoloogilise nähtusena, vaid osana laiemast digitaalsest riskimaastikust. EL on loonud standardid, millel on potentsiaal kujundada globaalset lähenemist: pakkudes teistele riikidele eeskuju, kuidas reguleerida digitaalse manipuleerimise uusi vorme viisil, mis kaitseb inimõigusi, demokraatiat ja ühiskondlikku usaldust.

3.2. Avalikkuse teadlikkuse tähtsus

Süvavõltsingutega seotud ohtude tõhus maandamine eeldab mitmetasandilist lähenemist, kus lisaks regulatiivsetele meetmetele tuleb tõsta ühiskondlikku teadlikkust ja kujundada eetilisi hoiakuid. Kuigi süvavõltsingute reguleerimine peab toimuma õigusnormide kaudu, ei taga õiguslikud meetmed üksi veel soovitud tulemust. Seda eriti olukorras, kus süvavõltsingute ohtude maandamiseks puuduvad veel sihilikult süvavõltsingutele suunatud siseriiklikud õiguslikud meetmed. Seetõttu tuleb kehtivaid õigusnorme rakendada paindlikult ja sihipäraselt. Selline lähenemine eeldab mitte üksnes süvavõltsingute olemuse, vaid ka kehtivate sätete sisulise eesmärgi ja seadusandja tahte mõistmist. Õiglane ja vastutustundlik õiguse kohaldamine saab toimida vaid probleemi sisulise mõistmise korra. Probleemi mõistmine võib aidata õigusnormide tõlgendajatel – sealhulgas ohvrite esindajatel, kohtutel, prokuratuuril ja uurimisasutustel – kohaldada kehtivat regulatsiooni, mis ei ole suunatud konkreetselt süvavõltsingute reguleerimisele.

Eelnevates peatükkides esile toodud näidisjuhtumid ilmestavad, kuidas realistlik, kuid fiktiivne audiovisuaalne materjal võib põhjustada ohvritele ja ühiskonnale märkimisväärset kahju. Need juhtumid rõhutavad vajadust rakendada süvavõltsingute loojate ja levitajate suhtes tugevaid õiguslikke meetmeid. Praktilised näited aitavad teadvustada, et süvavõltsingud kujutavad endast tõsist ohtu nii üksikisikutele kui ka ühiskonnale tervikuna. Suurem teadlikkus aitab õiguse tõlgendajatel hinnata rikkumiste raskust ning langetada otsuseid, mis toetavad ohvrite kaitset. Eriti oluline on see olukordades, kus on vaja kaaluda erinevate osaliste (subjektide) huvisid. Ühiskondlik teadlikkus tähendab ka seda, et ohvrid on teadlikud enda õigustest ja võimalustest pöörduda rikkumiste korral õiguskaitseorganite poole. Samuti võib teadlikkus ja arusaam süvavõltsingute probleemist ja tagajärgedest sisendada ohvrile ka julgust enda õiguste eest seista.

Teadlikkuse tõstmisel on ka oluline ennetav mõju. Avalikkuse teadmine, et pahatahtlike süvavõltsingute loomine ja levitamine pole ühiskondlikult aktsepteeritav ega õiguslikult lubatud, võib vähendada sellise sisu loomist. Sotsiaalne surve võib heidutada isikuid, kes muidu peaksid süvavõltsinguid süütuks naljaks. Enamgi veel, nad võivad lõpuks mõista, et tegemist ei ole naljaga. Praktikas on ennetavad meetodid tõestanud end muude digitaalsete ohtude puhul, näiteks küberpettuste kontekstis, kus politsei ja teised õiguskaitseasutused hoiatavad avalikkust konkreetsete ohtude eest ning avalikustavad juhtumeid selleks, et tõsta ühiskonna valvsust ja vähendada kuritegude arvu. Ka süvavõltsingute puhul võiks analoogne strateegia aidata ennetada õigusrikkumisi. Teavitustööl on ka menetlusökonoomiline mõju: mida vähem pannakse toime õigusrikkumisi, seda vähem kulub ressursse nende menetlemiseks.

3.3. Eesti õiguslik raamistik

Nagu eelnevalt käsitletud, ei ole 2025. aasta seisuga Eestis kehtestatud eraldiseisvaid õigusnorme, mis oleksid spetsiaalselt suunatud süvavõltsingute reguleerimisele. Tasub ka märkida, et kuigi ühtegi süvavõltsinguid puudutavat õiguslikku probleemi veel Eesti kohtupraktikas lahendatud ei ole, on süvavõltsingute termin vähemalt ühel korral kohtupraktikasse jõudnud. Tallinna Ringkonnakohtu 2021. aasta määruse[128] (asjaolude kirjelduses) on märgitud järgnev: „Puudutatud isikul on osa asjade osas tekkinud kahtlus, kas need asjad on olemas või ei ole. Internetis deep fake näiteks.“ Kuigi kehtivad õigusnormid ei ole otseselt suunatud süvavõltsingutest tulenevate ohtude reguleerimisele, saab neid teatud juhtudel siiski rakendada olukordades, kus süvavõltsinguid kasutatakse teisi isikuid kahjustavalt. Sellistes olukordades võivad olemasolevad sätted pakkuda kannatanutele vajalikku õiguskaitset.

[128] TlnRnKm 30.11.2021, 2-21-16615/19, p 5.

3.3.1. Eraõiguslikud meetmed

Eesti õiguslikus raamistikus on süvavõltsingute nõusolekuta loomist ja levitamist võimalik teatud juhtudel käsitleda õigusvastase kahju tekitamisena võlaõigusseaduse[129] (VÕS) tähenduses ning ohvril on võimalik nõuda kahju hüvitamist. VÕS § 1043 sätestab, et teisele isikule (kannatanu) õigusvastaselt kahju tekitanud isik (kahju tekitaja) peab kahju hüvitama, kui ta on kahju tekitamises süüdi või vastutab kahju tekitamise eest vastavalt seadusele. Kannatanu peab tõendama objektiivse teokooseisu esinemise ning õigusvastasuse eeldused. Piisab sellest, kui tõendatakse, et teos sisaldub vähemalt üks õigusvastasuse eeldustest.[130] VÕS § 1045 lg 1 loetleb tunnused, mis lasevad eeldada, et kahju tekitaja tegu või tegevusetus, mis toob kaasa kahjuliku tagajärje tekkimise kannatanul, oli õigusvastane.[131] Seega tuleb süvavõltsingute pahatahtliku loomise ja levitamise puhul analüüsida, millised § 1045 lg-s 1 nimetatud õigusvastasuse alused võivad kohalduda.

VÕS § 1045 lg 1 p 2 sätestab, et kahju tekitamine on õigusvastane, kui see tekitati kannatanule kehavigastuse või tervisekahjustuse tekitamisega. Kirjanduses on selgitatud, et tervisekahjustus hõlmab mistahes hälvet organismi normaalsest ja tavapärasest seisundist. Seega loetakse tervisekahjustuseks ka psüühikahäireid, mis on põhjustatud vaimse heaolu halvenemisest. Tervisekahjustuse põhjustamine kui õigusvastane tegu ehk delikt võib seisneda kas aktiivse käitumise aktis või tegevusetuses. Tegude puhul, mis ei ole vahetult suunatud tervisekahjustuse põhjustamisele, on sellise kahjustuse tekitanud isiku tegu õigusvastane üksnes juhul, kui ta rikkus tegevusetusega mingit käibekohustust. Kahju võib olla põhjustatud kas tahtlikult või hooletusest.[132] Nagu eelnevalt kirjeldatud võib süvavõltsingute nõusolekuta levitamine tekitada ohvrile tõsiseid vaimseid kannatusi (stress, suitsidaalsus, ärevus, depressioon). Tõsiasi, et sisus kujutatu ei pruugi olla reaalne, ei tähenda seega, et kahju ohvrile oleks väiksem. Tasub märkida, et teatud juhtudel võib intiimse sisuga süvavõltsingute loomine ja levitamine ilma kujutatud isiku nõusolekuta ollagi tahtlik tegu, mille eesmärgiks on ohvrile kannatuste põhjustamine. Näiteks võib sellise teo taga olla endine elukaaslane või kannatanu poolt romantiliselt tõrjutud isik, kes kasutab võltsitud intiimsisu sihilikult kättemaksu

[129] Võlaõigusseadus. – RT I, 04.07.2024, 18.
[130] Käerdi, M., Tampuu, T. VÕSK § 1043/3.6. Võlaõigusseadus IV. Komm vlj. Tallinn: Juura 2020.
[131] *Ibidem*, § 1045/3.1.1.
[132] *Ibidem*, § 1045/3.3.

vahendina. Sellisel juhul võib olla tuvastatav kahju tekitaja tahtlikkus põhjustada kannatanule vaimset tervisekahju.

VÕS § 1045 lg 1 p 4 sätestab, et kahju tekitamine on õigusvastane siis, kui see tekitati kannatanu isikliku õiguse rikkumisega. Kirjanduses on selgitatud, et sätte järgi kaitstavateks isiklikeks õigusteks on § 1046 lg-s 1 toodud näidisloetelu järgi isiku au, isiku õigus oma nimele või kujutistele (eelkõige õigus välistada nende õigustamatu kasutamine) ning eraelu puutumatus. Lisaks nimetatutele on deliktiõigusega kaitstavateks isiklikeks õigusteks nt õigus väärikusele, elulookirjeldusele, õigus kehalisele puutumatusele.[133] Laimamine ja solvamine eeldavad kohtupraktika kohaselt isiku au teotamist ebaõigete faktiväidete avaldamise või häbistavate väärtushinnangute avaldamise teel.[134] Isiku au teotavateks andmeteks on mistahes faktiväited, mis kutsuvad tavapäraselt esile avalikkuse negatiivse suhtumise isikusse. Faktiväide võib olla isiku au teotav selle tõttu, et see võimaldab isiku „väärtustamist" negatiivse hinnanguga.[135]

Kirjanduse kohaselt on isikul isiklik õigus, mis välistab tema nime, kujutise või eraeluliste andmete õigustamatu, st ilma vastava isiku loata toimuva kasutamise. Isiku kujutise all mõeldakse tehniliste või kunstiliste vahendite abil jäädvustatud isiku pilti või muud kujutist (nt videolõiku), mis võimaldab isiku identifitseerimist. Eraeluliste andmete all tuleb mõista mistahes andmeid tuvastatud või tuvastatava füüsilise isiku kohta, eelkõige IKÜM art 4 p-s 1 nimetatud isikuandmeid. Andmete avaldamise õigusvastasus ei sõltu vastavate andmete õigsusest, st kuna eraeluliste andmete avaldamine on lubatud üldjuhul puudutatud isiku nõusolekul, võib selliste andmete avaldamine nõusoleku puudumisel olla õigusvastane ka juhul, kui avaldatud andmed vastavad tegelikkusele.[136] Seega, süvavõltsing, mis kujutab isikut teda tuvastataval viisil, langeb määratluse järgi isiku kujutise alla ning sellise kujutise avaldamine ilma nõusolekuta on õigusvastane, sõltumata sellest, kas kujutis vastab tegelikkusele või mitte. Eriti tundlik on olukord mõistagi siis, kui süvavõltsing on intiimse sisuga. Sellisel juhul võib tegu lisaks kujutise õiguse rikkumisele sisaldada muu hulgas ka eraelu puutumatuse rikkumist, kuna sellega tungitakse isiku privaatsfääri ning avaldatakse andmeid, mis on olemuslikult delikaatsed. Nagu kirjanduses on rõhutatud, ei sõltu eraeluliste andmete avaldamise õigusvastasus nende tõesusest. Määrav on nõusoleku puudumine.

---

[133] *Ibidem*, § 1045/3.5.
[134] Nimmo, M. Identiteedivarguse piiritlemine solvamisest ja laimamisest Eesti õigussüsteemis. – Juridica 2017/10, lk 716.
[135] Käerdi, M., Tampuu, T. VÕSK IV § 1047/3.2.
[136] *Ibidem*, § 1045/3.5.b.

Isiklike õigustesse sekkumise õigusvastasuse kindlakstegemisel tuleb lisaks VÕS § 1045 lg 1 p-le 4 kohaldada täiendavalt ka VÕS §-s 1046 toodud põhimõtteid, mis eeldavad kahju tekitajale etteheidetava teo õigusvastasuse kindlaks tegemisel ka väärtusotsustuse tegemist.[137] Kirjanduse järgi peab kohus hindama, kas isiklike õiguste rikkumise õigusvastaseks lugemine ei kahjusta ülemäära kolmandate isikute õigusi või avalikkuse huve. Õigustav motiiv võib tekkida au teotamise või eraelu puutumatuse rikkumise juhtumites, olles seotud sõna- ja ajakirjandusvabaduse või avalikkuse õigusega saada teavet avalikes huvides.[138] Süvavõltsingute kontekstis seisab vastamisi ühelt poolt isiku õigus oma aule, kujutisele, eraelule, väärikusele ja tervisele ning teiselt poolt näiteks võimalikud loojate väited sõnavabadusele ja kunstilisele eneseväljendusele. Tasub märkida, et kui isikliku õiguse rikkumine seisneb isiku kohta ebaõigete andmete avaldamises, kohaldatakse lisaks VÕS §-le 1046 ka VÕS § 1047 lg-d 1–3, mis käsitlevad ebaõigete andmete avaldamise õigusvastasuse hindamist.[139] Samas, kui tegemist on tahtliku ebaõigete andmete avaldamisega (valetamisega), siis on tegu õigusvastane juba VÕS § 1045 lg 1 p 8 järgi, mis tähendab, et sellisel juhul ei ole vaja hinnata õigusvastasust VÕS § 1047 järgi.[140]

VÕS § 1045 lg 1 p 8 sätestab, et kahju tekitamine on õigusvastane siis, kui see tekitati heade kommete vastase tahtliku käitumisega. Sätte kohaldamine eeldab teo vastuolu heade kommetega ning kahju tekitamise tahtlust.[141] Kannatanu peab tahtlust tõendama.[142] Sätte kohaldamiseks piisab ka kaudsest tahtlusest, st kui kahju tekitaja pidi aru saama, et tema tegevus võib kahjustada kannatanut ja põhjustada seeõttu õigusvastase tagajärje, ent otsustas sellegipoolest tegutseda. Seega piisab sellest, kui tahtlikult heade kommete vastaselt käitunud isik sai aru või pidi aru saama, et tema tegu võib kahjustada kannatanut ja põhjustada seetõttu õigusvastase tagajärje. Oluline ei ole aga, kas kahju tekitaja ise sai kahju tekitamise ajal aru oma tegevuse heade kommete vastasusest või mitte. Küll aga peab ta olema teadlik nendest elulistest asjaoludest, mis toovad kaasa tema käitumise vastuolu heade kommetega.[143] Süvavõltsingute levitamise puhul võiks vähemalt teatud juhtudel eeldada kaudset tahtlust. Võltsingute loomine ja levitamine on enamasti teadlik ja sihipärane tegevus, mille eesmärk on luua ohvrist moonutatud, eksitav või kahjustav kuvand. Sellise tegevuse

[137] *Ibidem*, § 1045/3.5.d.
[138] *Ibidem*, § 1046/3.1.
[139] *Ibidem*, § 1045/3.5.d.
[140] *Ibidem*, § 1047/1.
[141] *Ibidem*, § 1045/3.9.
[142] *Ibidem*, § 1043/3.6.
[143] *Ibidem*, § 1045/3.9.

motiiviks võib olla näiteks avalik häbistamine, kättemaks, maine kahjustamine või vaimse heaolu kahjustamine. Võib väita, et reeglina tegutseb süvavõltsingu looja arusaamises, et tema tegevus võib teisele isikule kahju põhjustada. Kui isik loob näiteks intiimse sisuga või kompromiteeriva võltsingu, kasutades selleks teise isiku kujutist, ning levitab seda kas sotsiaalmeedias või muudes kanalites, on tõenäoline, et ta oli teadlik nii oma tegevuse kahjustavast potentsiaalist kui ka sellest, et selline tegevus läheb vastuollu heade kommetega. Ei ole oluline, kas süvavõltsingu looja ise tajus oma teo heade kommete vastasust. Oluline on, et ta oli teadlik elulistest asjaoludest, mis selle hinnangu kaasa toovad. Näiteks teadmine, et kujutatud isik ei ole võltsingu loomiseks nõusolekut andnud, ja et tegemist on sisult kahjustava materjaliga, millel võib olla tõsine mõju ohvri vaimsele heaolule või mainele.

VÕS § 1045 lg 1 p 7 sätestab, et kahju tekitamine on õigusvastane siis, kui see tekitati seadusest tulenevat kohustust rikkuva käitumisega. Kirjanduses on selgitatud, et IKÜM ja muude õigusaktide sätete kui kaitsenormide rikkumise korral võib kannatanul tekkida VÕS § 1045 lg 1 p-st 4 tulenevale kahju hüvitamise nõudele alternatiivne kahju hüvitamise nõue VÕS § 1045 lg 1 p 7 ja lg 3 järgi.[144] Juhul kui kannatanu tahab põhjendada õigusvastasust sellega, et rikuti kaitsenormi § 1045 lg 1 p 7 mõttes, peab ta sellist rikkumist tõendama.[145] Kuna süvavõltsingute loomisel kasutatakse isikuandmeid, võib nende õigusvastane töötlemine IKÜM art 4 p 1 ja art 6 alusel sätestatud nõuete rikkumise korral anda aluse kahju hüvitamise nõudele ka võlaõigusseaduse § 1045 lg 1 p 7 tähenduses.

VÕS § 1055 annab ka kannatanule ka õiguse esitada õigusvastase tegevuse lõpetamise või sellest hoidumise nõue. Seda näiteks olukorras, kus pahatahtlik isik levitab kannatanust järjepanu süvavõltsinguid või sellega ähvardab. Lisaks annab VÕS § 1047 lg 4 kannatanule õiguse nõuda ebaõigete andmete ümberlükkamist.[146] Seejuures ei ole VÕS § 1047 lg 4 kohaldamise eelduseks ebaõigete andmete avaldamise õigusvastasuse tuvastamine. Kirjanduses on selgitatud sedagi, et ebaõigete andmete ümberlükkamist võib nõuda ka isikult, kes edastas andmed kõrvalisele isikule, sh meediaväljaandele, kui ka meediaväljaandelt.[147] See võib kohalduda näiteks olukorras, kus pahatahtlik isik on avaldanud avaliku elu tegelasest loodud süvavõltsingud mõnele uudisteportaalile, väites seejuures, et tegemist on ehtsate andmetega.

[144] *Ibidem*, § 1045/3.5.b.
[145] *Ibidem*, § 1043/3.6.
[146] *Ibidem*, § 1047/3.4.
[147] *Ibidem*, § 1047/3.5.4.

Kokkuvõtlikult võib järeldada, et süvavõltsingute pahatahtlik loomine ja levitamine võib vastata mitmele VÕS § 1045 lg-s 1 sätestatud õigusvastasuse alusele: näiteks tervisekahjustuse tekitamisele, isikliku õiguse rikkumisele, seadusest tuleneva kohustuse rikkumisele või heade kommete vastasele tahtlikule käitumisele. Seega on teatud juhtudel võimalik käsitleda süvavõltsingute loomist ja levitamist kui õigusvastase kahju tekitamist, mis koosmõjus VÕS § 1043 annab kannatanule õiguse pöörduda kohtusse ning nõuda kahju hüvitamist. Samuti on VÕS § 1055 alusel võimalik nõuda kahju tekitava käitumise lõpetamisest ja sellest hoidumist ning ebaõigete andmete ümberlükkamist VÕS § 1047 lg 4 alusel.

3.3.2. Karistusõiguslikud meetmed

Pahatahtlike süvavõltsingute loomise ja levitamise puhul on kannatanul küll võimalik toetuda kehtivale eraõiguslikule raamistikule, ent arvestades süvavõltsingute eripära – nende realistlikkust, kiiret levikut ja olulist mõju ohvritele –, ei saa üksnes eraõiguslikke vahendeid pidada piisavaks. Eelnevates peatükkides käsitletud analüüs näitab, et intiimse sisuga süvavõltsingute loomine ja levitamine võib põhjustada ohvrile samaväärset kahju kui ehtsa intiimse sisuga materjali väärkasutus. Digiajastul levivad visuaalsed materjalid kiiresti ning nende täielik eemaldamine on sageli keeruline või isegi võimatu, mis, nagu eelnevalt kirjeldatud, võib põhjustada ohvrile muu hulgas pikaajalist stressi, suitsidaalsust, ärevust ja turvatunde kaotust. Teadmatus selle üle, kus ja millises kontekstis manipuleeritud kujutisi kasutatakse, tekitab hirmu ja võib sundida ohvrit loobuma sotsiaalmeediast, avalikust elust või tööalastest ja sotsiaalsetest tegevustest.

Eraõiguslik kahjuhüvitis ei pruugi sellistes juhtumites taastada ohvri õiglustunnet ega ennetada uusi rikkumisi, sest pelgalt varalise vastutuse oht ei pruugi omada pahatahtlike süütegude puhul piisavat heidutavat mõju. Lisaks ei taga ka kahju tekitava käitumise lõpetamise nõudmine soovitud tulemust, kuna kord internetis levitatud süvavõltsingud võivad jääda püsivalt ringlema. Sellest tulenevalt on vajalik käsitleda süvavõltsingute loomist ja levitamist ka karistusõiguslikust vaatenurgast, kuna just see valdkond võimaldab rakendada tugevaimat heidutusmehhanismi. Karistusõiguslikud meetmed ei täida pelgalt tagajärjemehhanismi, vaid neil on oluline üldpreventiivne roll: mõjutada võimalikke õigusrikkujaid hoiduma süütegude toimepanemisest. Kui potentsiaalsed süvavõltsingute loojad ja levitajad teavad, et tegu võib kaasa tuua mitte ainult eraõigusliku vastutuse, vaid ka reaalse kriminaalkaristuse, võib see

panna neid kavandatavast tegevusest loobuma. Karistusõiguslike meetmete heidutav mõju on küll alati eelduslik ega ole garanteeritud, kuid võib vähemalt osaliselt hoida ära uusi rikkumisi. Juba ainuüksi üks ärahoitud juhtum tähendab märkimisväärset võitu ühiskonnale, rääkimata potentsiaalsest ohvrist.

Süvavõltsingute kontekstis on karistusmeetmete rakendamine eriti oluline olukordades, kus võltsingutega kaasneb selge soov tekitada kahju, näiteks levitades sihilikult intiimset või kahjustavat sisu. Sellise tegevuse karistusõiguslik sanktsioneerimine annaks selge signaali, et tegu ei ole tühise või naljana käsitletava pisirikkumisega, vaid süüteoga. Tasub jällegi mainida, et Eestis ei kehti praegu eraldi karistusõiguslikku sätet, mis kriminaliseeriks nõusolekuta intiimsete süvavõltsingute loomise ja levitamise. Kuid Eestis ei kehti ka sellist karistusõiguslikku sätet, mis keelaks ehtsa intiimse sisu nõusolekuta loomist ja levitamist. Selliste lünkade olemasolu õigussüsteemis võib vähendada inimeste turvatunnet, usaldust õiguskaitseorganite vastu ning jätta ohvrid kaitseta. Seetõttu tuleb analüüsida praegu kehtivaid norme, mis küll ei ole suunatud otseselt süvavõltsingutele, kuid võivad teatud juhtudel ikkagi kohalduda.

3.3.2.1. Teise isiku identideedi ebaseaduslik kasutamine KarS 157[2] tähenduses

KarS § 157[2] lg 1 kohaselt teist isikut tuvastavate või tuvastada võimaldavate isikuandmete tema nõusolekuta edastamise, nendele juurdepääsu võimaldamise või nende kasutamise eest eesmärgiga luua teise isikuna esinemise teel temast teadvalt ebaõige ettekujutus, kui sellega on tekitatud kahju teise isiku seadusega kaitstud õigustele või huvidele, või varjata kuritegu, karistatakse rahalise karistuse või kuni kolmeaastase vangistusega. Sätte eesmärk on tagada PS §-s 26 sätestatud igaüheõigus perekonna- ja eraelu puutumatusele, mis sisaldab endas ühtlasi õigust oma kujutisele ja sõnale, mida identiteedivargusega kõige otsesemalt rünnatakse.[148] Kirjanduse kohaselt on identiteedivarguse koosseisuga tagatud au ja hea nime kriminaalõiguslik kaitse, samuti informatsioonilise enesemääramise õiguse ning eraelu ja inimväärikuse kaitse.[149] Samuti on leitud, et identiteedivarguse tüüpiliste juhtumite ning ka

[148] Nõmper, A. KARSK § 157.2/1. Karistusseadustik. Komm vlj. 5. vlj. Tallinn: Juura 2021.
[149] Nimmo, M., lk 714.

laimamise ja solvamise korral on õigusvastaste tegude tagajärjeks kellegi isiklike õiguste kahjustamine.[150]

Kirjanduses on selgitatud, et objektiivne koosseis võib seisneda kolmes teos: edastamises, juurdepääsu võimaldamises ja kasutamises.[151] Edastamine tähendab andmete aktiivset teisele kättesaadavaks tegemist (nt e-postiga, serverisse üleslaadimine, andmekandjal üleandmine).[152] Juurdepääsu võimaldamine seisneb nt salasõnade või autentimisvahendite üleandmises, millega teine isik saab andmetele ligi teise isikuna esinedes.[153] Kasutamine tähendab igasugust toimingut isikuandmetega.[154] Kõik teod peavad olema toime pandud ilma andmesubjekti nõusolekuta. Oluline on hinnata, kas kannatanu oli andmete kasutamiseks tegelikult loa andnud.[155] Kui isik on andnud nõusoleku enda isikuandmete kasutamiseks, siis koosseis ei kohaldu. Teod on karistatavad vaid siis, kui nendega kaasneb kahju teise isiku seadusega kaitstud õigustele või huvidele. Samuti on teod karistatavad, kui need on toime pandud kuriteo varjamise eesmärgil. See koosseisu element on täidetud, kui isik kasutab kuritegu toime pannes teise isiku identiteeti.[156] Subjektiivne koosseis eeldab, et teo toimepanija tegutses vähemalt kaudse tahtlusega kõigi objektiivsete tunnuste suhtes. Kui isikuandmeid kasutatakse teise isikuna esinemise eesmärgil, on vajalik kavatsetus (KarS § 16 lg 2). Ebaõige ettekujutuse tekitamine võib puudutada kannatanu vaateid, välimust, andmeid jms: määrav pole avaldatu tõepärasus, vaid see, et seda ei ole avaldanud kannatanu ise. Isikuandmete edastamisel piisab kaudsest tahtlusest, kui isik möönab, et andmeid võidakse kasutada teise isikuna esinemiseks.[157]

KarS § 157² süüteokoosseisu kohaldumise kontekstis võib süvavõltsingute puhul tõusetuda küsimus, kas võltsing võimaldab ohvri tuvastamist viisil, mis koosseisu täidab. KarS § 157² osas on kirjanduses leitud, et ei ole üheselt selge, kas koosseisu täitmiseks piisab sellest, et isik suudab end ise kujutiselt ära tunda, või on vajalik, et isik oleks tuvastatav ka teiste jaoks. Kirjanduses esitatud seisukoha kohaselt peaks süüteokoosseis olema eelkõige täidetud juhul, kui kujutatud isik on äratuntav ka kolmandatele isikutele.[158] Arvestades aga süvavõltsingute realistlikkust ja nende loomise tüüpilist eesmärki – jätta mulje, et kujutis on ehtne – on

[150] *Ibidem*.
[151] Nõmper, A. KARSK § 157.2/3.1.
[152] *Ibidem*, § 157.2/3.1.
[153] *Ibidem*, § 157.1/3.4.
[154] *Ibidem*, § 157.2/3.4.
[155] *Ibidem*, § 157.2/3.5.
[156] *Ibidem*, § 157.2/3.7.
[157] *Ibidem*, § 157.2/4.
[158] Nimmo, M., lk 715.

tõenäoline, et sellised võltsingud võimaldavad ohvri tuvastamist ka kolmandatel isikutel. Samas ei saa välistada olukordi, kus süvavõltsing on madalama kvaliteediga ning kujutatud isik on tuvastatav vaid enda jaoks.

Süvavõltsingute abil toime pandud identiteedivargus võib tekitada kahju eelkõige isiku põhiõiguste ja -vabaduste rikkumise kaudu. Kirjanduses on KarS § 157[2] osas selgitatud, et hea nime ja maine kahjustamise oluliseks tunnuseks on pahatahtlikkus ning ründe häbistav ja alandav laad. Samuti on selgitatud, et identiteedivarguse puhul on isiku õigust aule ja heale nimele rikutud juhul, kui ettekujutus, mis inimesest luuakse, on isiku enda arvamuse kohaselt negatiivne ja tundub seda ka mõistlikule kõrvalseisjale.[159] Kui autentsena näiva süvavõltsingu abil kujutatakse kannatanut kompromiteerivas või alandavas olukorras, on tema õigust aule ja heale nimele rikutud: seda eelduslikult nii kannatanu enda hinnangul kui ka mõistliku kõrvalseisja seisukohast. Lisaks saavad kannatanu enesemääramisõigus ja eraelu puutumatus rikutud juba ainuüksi sellest, kui isiku kohta käivaid andmeid on ebaseaduslikult kasutatud ning selle tulemusena sekkutud isiku eraellu ja piiratud enesemääramisõigust mistahes ebaõige ettekujutuse loomisega.[160] Süvavõltsingute puhul on selline rikkumine sageli tahtlik, süsteemne ja suunatud isiku privaatsfääri tungimisele, kahjustades tema kontrolli oma identiteedi üle ning rikkudes õigust määrata, kuidas ja mil viisil ta teistele kujutatud on.

Süvavõltsingute kontekstis ei pruugi pelgalt negatiivse mõjuga võltsingute loomine ja levitamine täita identiteedivarguse koosseisu, kuna sellisel juhul võib puududa üks koosseisu keskseid tunnuseid: teise isikuna esinemine. Kirjanduses on selgitatud, et identiteedivarguse puhul on nõutav, et ebaõige ettekujutuse aluseks olev avaldus või tegevus peab isikuna esinemise tõttu väljapoole nähtuma selle konkreetse isiku enda käitumise või avaldisena.[161] Seega on identiteedivargusega tegu siis, kui negatiivse mõjuga süvavõltsingud näivad pärinevat ohvrilt endalt. KarS § 157² süüteokoosseis võib seega kohalduda juhtumitele, kus süvavõltsingute abil luuakse sotsiaalmeedias või veebifoorumis isikust võltsprofiil, mille kaudu toimub reaalne suhtlus kolmandate isikutega, kasutades kannatanu idenditeeti. Sellisel juhul on tegemist teise isikuna esinemisega, millele KarS § 157² koosseis kohalduks. Seisukohta kinnitab ka sätte seletuskiri[162], milles on rõhutatud, et interneti levikuga on

[159] *Ibidem*, lk 716.
[160] *Ibidem.*
[161] *Ibidem.*
[162] Karistusseadustiku muutmise seaduse eelnõu seletuskiri. 530 SE, § 157[2] – https://www.riigikogu.ee/tegevus/eelnoud/eelnou/2b386832-b657-ab0c-fb52-de02708302bc/Karistusseadustiku%20muutmise%20seadus/ (23.04.2025).

sagenenud teise isikuna esinemine erinevates suhtluskeskkondades – näiteks kommentaaride, blogide või võltskontode kaudu. Kui sellise tegevuse kaudu edastatakse ebaõiget, laimavat või solvavat teavet, võib see tõsiselt kahjustada isiku õigusi.

Identiteedivargusena saab käsitleda näiteks 2020. aasta Hongkongi juhtumit, kus süvavõltsitud häält kasutades esines kurjategija teise isikuna, et panna toime kelmus, mille tagajärjel tekitati 35 miljoni USA dollari väärtuses kahju.[163] Tasub märkida, et kirjanduse kohaselt on võimalik ideaalkogum kelmusega (KarS § 209).[164] Seejuures on avaldatud arvamust, et kui üks tegu täidab üheaegselt nii KarS §-s 209 kui ka §-s 157^2 sätestatud kuriteokoosseisu tunnused, on isiku tegevus suunatud kahe eri kuriteokoosseisus asuva eesmärgi täitmisele ning toob kaasa kahe eri isiku eri sisuga õiguste kahjustamise, mistõttu tuleks isikut süüdi mõista mõlemas kuriteos.[165]

Arvestades süvavõltsingute tehnoloogilist arengut, võib praktikas muutuda keerulisemaks eristada süvavõltsingute loomist ja levitamist esinemisest. Näiteks võib luua süvavõltsitud kujutise, mis videokõne vormis suhtleb kolmandate isikutega, jättes mulje, et tegemist on ehtsa isikuga. Kui selline tehisagent on loodud konkreetset isikut matkides ja teda tuvastataval viisil kujutades, on tuvastatavuse element täidetud. Kui agent tegutseb viisil, millega kaasneb negatiivne mõju matkitud isikule, on ka kahju tekkimise element täidetud. Samas puudub sellisel juhul füüsilisest isikust esineja. Sellisel juhul toimub identiteedivargus tehnoloogilise vahendaja kaudu, mille mõju kannatanu õigustele on siiski reaalne. Seetõttu võib KarS § 157^2 kehtiv sõnastus osutuda ebapiisavaks ning vajada ajakohastamist.

Kokkuvõtlikult võib öelda, et KarS § 157^2 lg 1 kontekstis võib süvavõltsingute loomist ja levitamist pidada karistatavaks siis, kui süvavõltsingu loomisel ja levitamisel kasutatakse ilma andmesubjekti nõusolekuta teda tuvastavaid või tuvastada võimaldavaid isikuandmeid ning seejuures toimub andmesubjektina esinemine, mille eesmärk on luua temast teadvalt ebaõige ettekujutus ning kahjustada tema seadusega kaitstud õigusi või huve, või varjata kuritegu.

[163] Brewster, T.
[164] Nõmper, A. KARSK § 157.2/5.
[165] Nimmo, M. Karistusseadustiku § 157.2 probleeme Internetiga seotud identiteedivarguste kontekstis. – Juridica 2014/6, lk 470.

3.3.2.2. Ahistav jälitamine KarS § 157[3] tähenduses

KarS § 157[3] lg 1 kohaselt teise isikuga korduva või järjepideva kontakti otsimise, tema jälgimise või muul viisil teise isiku tahte vastaselt tema eraellu sekkumise eest, kui selle eesmärk või tagajärg on teise isiku hirmutamine, alandamine või muul viisil oluliselt häirimine, kui puudub KarS §-s 137 sätestatud süüteokoosseis, karistatakse rahalise karistuse või kuni üheaastase vangistusega. Sätte objektiivne koosseis nõuab, et toimepanija teod oleksid järjepidevad või korduvad, eesmärgiga tekitada kannatanus hirmu või alandust või muul viisil olulist häiritust. Tahtluse sisustamisel on leitud, et süüteokoosseisu täitmiseks peab olema tuvastatud, et isikul oli teise isiku eraellu korduvalt sekkudes eesmärk ehk kavatsus ohvrit alandada või hirmutada või ta pidi vähemalt möönma, et tema tegevuse tagajärg on ohvrit alandav, hirmutav või muul moel oluliselt häiriv ehk tagajärje suhtes peab esinema vähemalt kaudne tahtlus.[166] Säte on mõeldud kaitsma isiku- ja eraelu puutumatust.[167] Kirjanduses väljendatu kohaselt on KarS § 157[3] lg 1 suunatud eelkõige just kaitseks naistevastase vägivalla vastu[168] ning hõlmab muu hulgas vaimse vägivalla ilminguid. Samuti on seletuskirjas[169] juhitud tähelepanu sellele, et sageli ei piirdu toimepanijad konkreetse ohvriga, vaid sihivad oma tegevuse ka ohvri lähedastele, süvendades ohvri hirmu ning tunnet, et ta on kaotanud kontrolli olukorra üle.

Tasub märkida, et süüteokoosseis ei hõlma üksnes jälitamist selle tavapärases tähenduses. Kirjanduse kohaselt võimaldab sätte sõnastus üsna laia grammatilist tõlgendust.[170] Grammatilise tõlgenduse kohaselt täidab KarS § 157[3] objektiivse koosseisu igasugune korduv või järjepidev teise inimese tahte vastane tema eraellu sekkumine, mille eesmärk või tagajärg on kannatanu jaoks oluliselt häiriv.[171] Süvavõltsingute kontekstis on oluline eelkõige teise isiku tahte vastase eraellu sekkumise tähenduse sisustamine. Eraellu sekkumine on mistahes tegu, millel on kannatanu privaatsfääri tungimise (eraelu puutumatuse rikkumise) iseloom.[172] Täiendavalt on kirjanduses juhitud tähelepanu, et KarS § 157[3] tõlgendamine peaks toimuma Euroopa Nõukogu naiste vastase vägivalla ja perevägivalla ennetamise ja tõkestamise

[166] Sommer, E. Kuidas tõlgendada karistusseadustiku §-i 157.3? – Juridica 2018/8, lk 540.
[167] *Ibidem*, lk 538.
[168] Tehver, J. KARSK § 157.3/2.
[169] Karistusseadustiku muutmise ja sellega seonduvalt teiste seaduste muutmise seaduse seletuskiri. 385 SE I. § 157.3. – https://www.riigikogu.ee/tegevus/eelnoud/eelnou/f9a7291c-8c46-4ad8-a740-4e1c55c83964/ (23.04.2025).
[170] Sommer, E., lk 537.
[171] *Ibidem*, lk 538.
[172] Tehver, J. KARSK § 157.3/4.3.

konventsiooni[173] (edaspidi: Istanbuli konventsioon) valguses.[174] Istanbuli konventsiooni seletuskirja kohaselt on ahistava jälitamisena vaadeldav tegevus, mis on konkreetsele isikule suunatud. Seejuures on selgitatud, et ähvardav käitumine võib sisaldada muu hulgas kannatanu kohta väära teabe levitamist internetis.[175]

Süvavõltsingute kontekstis omab koosseis seega olulist tähendust. Nimelt võivad süvavõltsingud, mis kujutavad isikut moonutatud, solvavas või muus ebameeldivas ja alandavas kontekstis (nt seksuaalses olukorras), täita KarS § 157³ lg 1 objektiivse koosseisu, kui sellise materjali loomine ja levitamine toimub korduva või järjepideva tegevusena ning on kantud tahtlusest ohvrit hirmutada, alandada või tema elu muul viisil olulisel määral häirida. Sellises olukorras ei pruugi toimepanija tegevus piirduda ainult üheainsa juhtumiga, vaid süvavõltsingute tehnoloogia lihtsus ja kättesaadavus võimaldab hõlpsasti korduvalt levitada või luua uut sisu, põhjustades ohvrile märkimisväärset vaimset kahju. Oluline on tähele panna, et säte nõuab toimepanijalt vähemalt teistkordset tegevust ehk korduvust, mida kinnitab ka kohtupraktika.[176] Sätte seletuskirja kohaselt loetakse korduvaks ka teist korda toime pandud tegu.[177] Seega võib säte kohalduda näiteks siis, kui teo toimepanija loob ohvrist mitmeid alandavaid süvavõltsinguid ning levitab neid erinevates ajahetkedes või erinevate platvormide kaudu.

Kohtupraktikas on alandamise mõistet sisustatud viisil, mis on kohaldatav ka süvavõltsingute juhtumitele. Alandamisega on tegemist siis, kui isik taandatakse tema inimväärikust oluliselt vähendava solvangu või häbistamise objektiks.[178] Süvavõltsingute tehnoloogia kaudu loodud materjalid, mis kujutavad isikut alandavas või häbistavas olukorras (näiteks pornograafilised süvavõltsingud), sellele määratlusele ka tõenäoliselt vastavad, kuna võivad panna ohvri tahtmatult avaliku häbistamise objektiks. Sellise materjali kiire ja pöördumatu levik tänapäeva digitaalruumis suurendab alanduse intensiivsust, sest ohver kaotab praktiliselt kontrolli enda kujutise ja isikliku väärikuse üle.

---

[173] Naistevastase vägivalla ja perevägivalla ennetamise ja tõkestamise Euroopa Nõukogu konventsioon. – RT II, 26.09.2017, 2.
[174] Sommer, E., lk 538.
[175] *Ibidem*.
[176] TlnRnKm 10.04.2024, 1-24-1954/4, p 27.
[177] Karistusseadustiku muutmise ja sellega seonduvalt teiste seaduste muutmise seaduse seletuskiri. 385 SE I. § 157.3. – https://www.riigikogu.ee/tegevus/eelnoud/eelnou/f9a7291c-8c46-4ad8-a740-4e1c55c83964/ (23.04.2025).
[178] TlnRnKm 10.04.2024, 1-24-1954/4, p 30.

Kohtupraktikas on selgitatud ka mõistet „muul viisil oluline häirimine“. Olulise häirimise all tuleb eeskätt silmas pidada olukorda, kus kannatanu käitumine ning seeläbi ka tema põhivabaduste teostamine on pikema perioodi vältel tingitud toimepanija tegudest. Sel juhul ei saa kannatanu nautida temale põhiseadusega tagatud põhivabadusi (eeskätt õigust vabale eneseteostusele), vaid peab tegelema toimepanija poolt loodud ebamugavustega, neid kannatama või püüdma neid aktiivselt vältida. Nii on muuhulgas siis, kui kannatanu ei saa end toimepanija tõttu turvaliselt tunda ja peab seetõttu pidevalt oma õigushüvede kaitseks valvel olema. Hinnangu andmisel tuleb ennekõike lähtuda objektiivse kõrvalseisja vaatenurgast. See tähendab, et oluline häirimine ei saa tuleneda üksnes kannatanu isikulisest eripärast või madalamast talumislävendist, vaid peaks asjaolusid arvestades olema sellisena tajutav ka objektiivsele kõrvalseisjale.[179] Süvavõltsingutega seotult võib selliseid tagajärgi täheldada: isik, kelle kujutist või häält on ilma tema nõusolekuta süvavõltsingu kaudu moonutatud ja levitatud, kogeb tihti turvatunde kadumist, pikaajalist ärevust ning kontrolli kaotust oma identiteedi ja avaliku kuvandi üle. Süvavõltsingute püsivus ja kiire levik internetis tähendab, et kannatanu võib olla pidevas teadmatuses selle osas, millal ja kuidas süvavõltsinguid taas levitatakse, ning peab aktiivselt tegelema sellega, et süvavõltsingud enam ei leviks. Samuti peab kannatanu olema pidevalt valmis selgitama teistele isikutele, et temast levivad süvavõltsingud ei ole ehtsad.

Kokkuvõtvalt tuleb KarS § 157³ lg 1 rakendamisel süvavõltsingute kontekstis lähtuda sellest, kas süvavõltsingute loomine ja levitamine toimub korduva või järjepideva tegevusena, mis on kantud selgest tahtlusest kannatanut hirmutada, alandada või muul viisil tema eraelu oluliselt häirida. Kui süvavõltsingute loomine ja levitamine on järjepidev või korduv ning selle tagajärjel muutub kannatanu alandamise või häbistamise objektiks või kahjustub oluliselt tema turvatunne ja võimalus põhivabadusi vabalt teostada, võib KarS § 157³ lg 1 kohaldamine olla põhjendatud, vajalik ja õigustatud. Üksiku süvavõltsingu loomine ja levitamine, isegi kui see kannatanu väärikust riivab, ei pruugi vastata ahistava jälitamise koosseisule. Seega tuleb selgelt eristada süvavõltsingute puhul olukordi, kus on tegemist tahtliku ja korduva ahistamisega, olukordadest, kus süvavõltsingute levitamine on pigem ühekordne tegu.

[179] TlnRnKm 10.04.2024, 1-24-1954/4, p 32.

3.3.2.3. Lapsporno valmistamine ja selle võimaldamine KarS § 178 tähenduses

KarS § 178 lg 1 sätestab, et nooremat kui kaheksateistaastast isikut pornograafilises või nooremat kui neljateistaastast isikut pornograafilises või erootilises situatsioonis kujutava pildi, kirjutise või muu teose või selle reproduktsiooni valmistamise, omandamise või hoidmise, teisele isikule üleandmise, näitamise või muul viisil kättesaadavaks tegemise eest, välja arvatud juhul, kui see toimub teoses või selle reproduktsioonis kujutatud noorema kui kaheksateistaastase isiku ja teo toimepanija vastastikusel nõusolekul põhinevas suhtes vabatahtlikult üksnes nende isiklikuks tarbeks, selle eest ei anta rahalist tasu või mis tahes muud hüve ning nende omavaheline suguühe või muu sugulise iseloomuga tegu ei ole kuriteona karistatav, karistatakse rahalise karistuse või kuni kolmeaastase vangistusega. Normi eesmärk on vähendada nõudlust ning sellega demotiveerida lapsporno tootmist, mille tulemusena peaks vähenema ka laste kasutamine pornograafiliste teoste valmistamisel.[180] Objektiivne koosseis seisneb lapsporno teose valmistamises, hoidmises, teisele üleandmises, näitamises või muul viisil kättesaadavaks tegemises.[181] Subjektiivne koosseis eeldab vähemalt kaudset tahtlust.[182]

KarS § 178 lg 1 kohaldamine süvavõltsingute kontekstis eeldab, et süvavõltsing kujutab konkreetset alla 18-aastast isikut pornograafilises või alla 14-aastast isikut pornograafilises või erootilises situatsioonis. Sellistel juhtudel on süvavõltsingu valmistamine, omandamine, hoidmine ja levitamine karistusõiguslikult selgelt keelatud ning hõlmatud lapsporno keelunormiga. Seda on selgitanud ka politseikapten M. Punak[183], mis näitab uurimisasutuste valmidust rakendada juba olemasolevat õiguslikku raamistikku, et reageerida süvavõltsingutest nähtuvatele ohtudele. Uurimisasutuste poolt avalikkusele avaldatud seisukohad võivad omada ka heidutavat mõju.

KarS § 178 kohaldamisel võib tõusetuda küsimus, kas karistusõiguslik vastutus laieneb ka sellise lapspornograafilise materjali valmistamisele, mis kujutab täielikult fiktiivset alaealist isikut: st süvavõltsingut, mille loomisel ei ole kasutatud ühegi reaalselt eksisteeriva isiku kujutist. Kohtupraktikas on leitud, et KarS § 178 sõnastusest on võimalik mõista seadusandja tahet kriminaliseerida selliste erootiliste või pornograafiliste teoste loomine ja käitlemine,

[180] Kurm, M. KARSK § 178/1.
[181] *Ibidem*, § 178/3.1.
[182] *Ibidem*, § 178/4.
[183] Jõerand, R.

millel kujutatavad inimesed on äratuntavalt lapsed. Kuna inimest on teoses võimalik kujutada ka ilma reaalset modelli kasutamata, siis ei ole reaalse modelli olemasolu koosseisu realiseerimiseks vajalik.[184] Sarnasele seisukohale on asutud ka varasemas praktikas, kus kohus on märkinud, et lapsporno teose valmistamine ei eelda modelli või näitlejana konkreetse alaealise kasutamist.[185] Ka kirjanduses on selgitatud, et koosseis ei eelda lapsporno teoses kujutatud isiku tuvastamist. Koosseisu kohaldamiseks piisab lapspornoks kvalifitseeruva teose olemasolust ja selle koosseisupärasest käitlemisest. Samuti ei ole vaja kindlaks teha lapsporno teoses kujutatu tegelikku vanust, vaid piisab sellest, kui pornograafilises situatsioonis kujutatu on mõistliku erapooletu vaatleja jaoks silmanähtavalt alaealine või erootilises asendis kujutatu silmanähtavalt lapseealine. Koosseisuteod on seega alaealisena näivat isikut kujutava pornograafilise teose ning lapseealisena näivat isikut kujutava pornograafilise või erootilise teose näitamine, hoidmine jne.[186]

Kokkuvõtlikult võib öelda, et KarS § 178 lg 1 kohaldub süvavõltsingutele siis, kui nende sisuks on alaealise või alaealisena näiva isiku kujutamine pornograafilises või erootilises situatsioonis. Oluline on rõhutada, et koosseis ei nõua täitmiseks reaalse isiku kujutamist. Sellest lähtuvalt saab süvavõltsingul põhinevate lapsporno juhtumite käsitlemisel kasutada juba kehtivaid kriminaalõiguslikke norme.

3.3.2.4. Väljapressimine KarS § 214 tähenduses

KarS § 214 sätestab, et varalise kasu üleandmise nõudmise eest, kui on ähvardatud piirata isiku vabadust, avaldada häbistavaid andmeid või hävitada või rikkuda vara, samuti kui on kasutatud vägivalda, karistatakse rahalise karistuse või kuni viieaastase vangistusega. Pildipõhise seksuaalse ahistamisega kaasneb sageli väljapressimine, kus ohvrit ähvardatakse intiimse sisuga materjali levitamisega. Sellist väljapressimise vormi on ingliskeelses diskursuses hakatud nimetama *sextortion*'iks.[187] Uuringud näitavad, et väljapressijate motiivid võivad olla mitmekesised: alates ohvri kontrollimisest ja kättemaksust kuni alandamise, naljatlemise või sotsiaalse kapitali suurendamiseni.[188] Politseikapten M. Punaku sõnul jõuab uurimisasutusteni

[184] TlnRnKo 11.10.2017, 1-15-11024/77, p 20.1.; RKKKo 18.12.2017, 1-17-689, 15.
[185] TlnRnKo 20.06.2017, 1-17-689/22, 8.2
[186] Kurm, M. KARSK § 178/3.2.2.
[187] Henry, N., Beard, G. Image-Based Sexual Abuse Perpetration: A Scoping Review. – TRAUMA, VIOLENCE, & ABUSE 2024/25 (5), lk 3989. https://journals-sagepub-com.ezproxy.utlib.ut.ee/doi/pdf/10.1177/15248380241266137 (24.04.2025).
[188] Henry, N., Beard, G., lk 3992.

mitu korda kuus juhtumeid, kus isikutelt nõutakse raha ähvardusega levitada nende kohta intiimseid fotosid.[189]

Väljapressimine on süvavõltsingute loomise ja levitamise kontekstis üha levinum kuriteoliik, kuna tehnoloogia võimaldab lihtsalt ja veenvalt luua kompromiteerivat ning häbistavat materjali, mida saab kasutada survestusvahendina.[190] Tüüpiliselt luuakse ohvrist intiimse sisuga süvavõltsing, mille järel võetakse temaga ühendust. Ohvrit ähvardatakse, et kui ta ei maksa nõutud summat, siis avaldatakse tema kohta häbistavat võltsmaterjali.[191] Kirjanduses on selgitatud, et ähvardus avaldada häbistavaid andmeid tähendab selliste teadete avaldamisega ähvardamist, mis peavad olema taunitavad nii objektiivselt kui subjektiivselt. Esimesel juhul oleksid need vastuolus moraali ja õigusteadvuses omaksvõetud väärtustega, teisel juhul on oluline, et teateid võtaks häbistavana ka isik, keda ähvardatakse. Ei ole oluline, kas andmed on välja mõeldud, moonutatud või tõesed.[192] Seega võib KarS § 214 olla kohaldatav ka süvavõltsingute kontekstis.

Ka kohtupraktikast ilmneb, et Eestis kasutatakse väljapressimise eesmärgil sihilikult fabritseeritud visuaalset sisu. Tartu Maakohtu 06.01.2023 otsuses[193] tunnistati isik O.P muu hulgas süüdi KarS § 214 lg 2 p 1 alusel. Süüdistuse kohaselt nõudis O.P kannatanult varalise kasu üleandmist, kasutades kannatanu suhtes psüühilist vägivalda, mis seisnes selles, et ähvardas sotsiaalmeedia sõnumite vahendusel kannatanu elu rikkuda, näo rikkuda ning kannatanust võltsitud alastipilte ehk häbistavaid andmeid avaldada. Kuigi otsuses ei täpsustatud, millisel viisil O.P kavatses alastipilte võltsida, näitab juhtum, et ka Eestis eksisteerib reaalne oht, et süvavõltsingute tehnoloogiat võidakse kasutada väljapressimise vahendina.

[189] Jõerand, R.
[190] Fletcher, R., *et al*. The dark side of Artificial Intelligence – Risks arising in dating applications. – Assessment & Development Matters 2024/16 (1), lk 19. https://research-ebsco-com.ezproxy.utlib.ut.ee/c/qlurcm/viewer/html/byrcq5bju5 (24.04.2025).
[191] Felipe, R. M., lk 299.
[192] Sootak, J. KARSK § 214/8.
[193] TMKo 06.01.2023, 1-22-7937/36

3.3.2.5. Kelmus KarS § 209 tähenduses

KarS § 209 lg 1 sätestab, et teisele isikule varalise kahju tekitamise eest tegelikest asjaoludest teadvalt ebaõige ettekujutuse loomise teel varalise kasu saamise eesmärgil – karistatakse rahalise karistuse või kuni neljaaastase vangistusega. Tegelikest asjaoludest ebaõige ettekujutuse loomine on pettuslik tegu ehk petmine, teise isiku kujutluse ehk intellektuaalse arusaama mõjutamine.[194] Kirjanduses on selgitatud, et petmine kui tegu võib seisneda eelkõige tegevuses – mitte ainult sõnaselgelt väljendatud väites, vaid ka konkludentses ehk tähenduslikus teos. Ka näiteks vormiriietuse kandmine, näitab konkludentselt, et väidetakse end olevat volitatud isik.[195]

Seega on ka kelmuse koosseisul oluline roll süvavõltsingute kontekstis. Süvavõltsingute abil on võimalik luua ebaõige ettekujutus, mille tulemusel saavad teo toimepanijad varalist kasu. Seda ilmestavad alapeatükis 2.3. esile toodud näidisjuhtumid. Võib nentida, et pettus jääb pettuseks, sõltumata vahendist, mida ebaõige ettekujutuse loomiseks kasutatakse. Õiguskaitseasutuste peamine ülesanne on pidada sammu tehnoloogilise arenguga, eriti tõendamise aspektist: tuleb osata kindlaks teha, kes oli süvavõltsitud materjali taga, milliseid vahendeid kasutati, kuidas leida kurjategijani viivaid digitaalseid jälgi. Väljakutseks võib osutuda juhtumite rahvusvaheline mõõde. Süvavõltsingute abil läbiviidavaid petuskeeme võidakse korraldada välisriikidest, mistõttu on oluline rahvusvaheline koostöö. Üheks tõhusaks koostööinstrumendiks küberkuritegude vallas on Euroopa Nõukogu arvutikuritegevuse vastase konventsioon (edaspidi: Budapesti konventsioon), mille osaline on ka Eesti, ja selle lisaprotokollid.[196] Budapesti konventsioon loob koostööraamistiku andmevahetuseks, süüdlaste väljaandmiseks ja tõendite kogumiseks ka piiriülestes juhtumites. Näiteks 2024. aasta prokuratuuri aastaraamatu kohaselt on keskkriminaalpolitsei edastanud Budapesti konventsiooni alusel tõendeid Soome Vabariigile seoses krüptoraha petuskeemiga.[197] Seega on ka rahvusvahelise mõõtmega süvavõltsingute juhtumite puhul võimalik koostöö hõlbustamiseks tugineda näiteks Budapesti konventsioonile.

[194] Sootak, J. KARSK § 209/5.
[195] *Ibidem*.
[196] The Convention on Cybercrime (Budapest Convention, ETS No. 185) and its Protocols. – Euroopa Nõukogu. https://www.coe.int/en/web/cybercrime/the-budapest-convention (24.04.2025).
[197] Prokuratuuri aastaraamat 2024. Küberkuritegevus. – Prokuratuur 2024. https://aastaraamat.prokuratuur.ee/prokuratuuri-aastaraamat-2024/kuberkuritegevus (24.04.2025).

3.3.3. Vahekokkuvõte

Kuigi Eesti õiguslik raamistik ei sisalda 2025. aasta seisuga süvavõltsingute jaoks spetsiaalset regulatsiooni, võimaldab kehtiv raamistik teatud tingimustel süvavõltsingutega seotud juhtumitele reageerida. Eraõiguslikud sätted võimaldavad ohvril nõuda kahju hüvitamist, kahju tekitava tegevuse lõpetamist ja sellest hoidumist ning ebaõigete andmete ümberlükkamist. Erinevad karistusseadustiku sätted – sealhulgas identiteedivargust (KarS § 157²), ahistavat jälitamist (KarS § 157³), lapsporno valmistamist ja võimaldamist (KarS § 178), väljapressimist (KarS § 214) ja kelmust (KarS § 209) reguleerivad normid – võivad olla kohaldatavad vastavalt süvavõltsingu sisu, eesmärgi ja tagajärgede iseloomule. Avalikkuse teadlikkus, et kehtivaid norme saab rakendada ka süvavõltsingute puhul, võib omada ka heidutavat mõju.

3.4. Euroopa Liidu õiguslik raamistik

Euroopa Komisjon on seadnud eesmärgiks ajakohastada Euroopa õigusraamistikku, et see vastaks digiajastu nõuetele.[198] Nõutele vastavus hõlmab eelkõige digiteenuseid puudutava regulatsiooni uuendamist, et tagada isikute põhiõiguste kaitset, tõhustada desinformatsiooni ja kuritegevuse vastast võitlust ning edendada innovatsiooni ja majanduskasvu. 2021. aasta märtsis kehtestati strateegiline raamistik „Digitaalne Kümnend“,[199] mille suuniseid määratleb „2030. aasta Digitaalne Kompass“. Eesmärgiks on EL-i digitaalse ülemineku edendamine neljas põhivaldkonnas: elanikkonna digipädevus, digitaalne taristu, ettevõtete digitaalne transformatsioon ja avalike teenuste digitaliseerimine. Eesmärk on seegi, et digimaailm peaks põhinema euroopalikel väärtustel, st et kedagi ei jäeta maha, kõik naudivad vabadust, kaitset ja õiglust. Strateegia hõlmab ka süvavõltsingute tehnoloogia reguleerimist, tagades, et selle väärkasutuse ennetamiseks ja tõkestamiseks rakendatakse asjakohaseid õiguslikke meetmeid.[200] Arvestades süvavõltsingute tehnoloogia arengut ja elutsüklit, on juba kehtivas õigusraamistikus mitmeid sätteid, mis süvavõltsingutele kohalduvad.

[198] EU Digital Strategy. – EU4Digital. https://eufordigital.eu/discover-eu/eu-digital-strategy/ (23.03.2025).
[199] Europe's Digital Decade. – Euroopa Komisjon 12.03.2025. https://digital-strategy.ec.europa.eu/en/policies/europes-digital-decade (23.03.2025).
[200] *Ibidem*.

3.4.1. Tehisintellekti käsitlev määrus

Euroopa Liidus 2024. aastal jõustunud tehisintellekti määrust[201] võib pidada üheks olulisemaks süvavõltsinguid käsitlevaks õigusaktiks, arvestades selle teedrajavat rolli esimese tervikliku TI regulatsioonina maailmas. Määruse keskseks eesmärgiks on parandada siseturu toimimist ühtse õigusraamistiku kehtestamisega eeskätt tehisintellektisüsteemide arendamiseks, turule laskmiseks, kasutusele võtmiseks ja kasutamiseks.[202] Seega toetab määrus strateegilist eesmärki luua õiguskindel ja usaldusväärne õigusraamistik digiajastu tehnoloogiliste väljakutsetega toimetulekuks.

Määruse kohaldamisala kontekstis on art 2 tähenduses eristatud kaks mõistet: TI-süsteemide pakkujad ja juurutajad. Määruse art 3 p 3 kohaselt on pakkuja füüsiline või juriidiline isik, ametiasutus, ametkond või muu organ, kes arendab TI-süsteemi või üldotstarbelist TI-mudelit või kellel on väljatöötatud TI-süsteem või üldotstarbeline TI-mudel ja kes laseb selle turule või võtab TI-süsteemi kasutusele oma nime või kaubamärgi all kas tasu eest või tasuta. Juurutajaks on vastavalt art 3 p-le 4 füüsiline või juriidiline isik, ametiasutus, ametkond või muu organ, kes kasutab TI-süsteemi oma volituste alusel, välja arvatud juhul, kui TI-süsteemi kasutatakse isikliku, mitte kutselise tegevuse jaoks. Oluline on art 2 lg-s 10 sätestatu, mille kohaselt ei kohaldata määrust isikliku, mitte kutsetegevuse käigus TI-süsteeme kasutavate füüsilistest isikutest juurutajate kohustuste suhtes.

Määruse oluliseks saavutuseks on ka süvavõltsingute esmakordne õiguslik definitsioon. Määruse art 3 p 60 järgi on süvavõltsing loodud või manipuleeritud kujutis või audio- või videosisu, mis sarnaneb tegelike isikute, esemete, kohtade, üksuste või sündmustega ning mis näib kasutajale petlikult ehtne või tõene. Mõistet on selgitatud ka määruse põhjenduspunktis 134, mille kohaselt on süvavõltsingud märgatavalt sarnased olemasolevate isikute, objektide, kohtade, üksuste või sündmustega ja võivad inimesele ekslikult ehtsad ja tõesed näida. Kuna nii artikkel kui ka põhjenduspunkt kasutavad fraasi „sarnaneb tegelikule/olemasolevale“ peaks süvavõltsing kujutama määruse tähenduses konkreetselt kedagi või midagi reaalselt eksisteerivat.[203] On aga leitud, et määruses tuleks mõistet laiendada, sest TI abil on võimalik

[201] 13. juuni 2024. aasta Euroopa Parlamendi ja nõukogu määrus (EL) 2024/1689, millega nähakse ette tehisintellekti käsitlevad ühtlustatud õigusnormid ning muudetakse määruseid (EÜ) nr 300/2008, (EL) nr 167/2013, (EL) nr 168/2013, (EL) 2018/858, (EL) 2018/1139 ja (EL) 2019/2144 ning direktiive 2014/90/EL, (EL) 2016/797 ja (EL) 2020/1828 (tehisintellekti käsitlev määrus). – ELT L 2024/2689, 12.7.2024.
[202] Tehisintellektimääruse põhjenduspunkt 1.
[203] Eitren, W. Deep fakes in the AI act. – Schjødt 07.11.2024. https://schjodt.com/news/deep-fakes-in-the-ai-act (23.03.2025).

luua ka täiesti fiktiivseid ehtsana näivad inimkujutusi ning esineb juhtumeid, kus selliseid täiesti fiktiivseid kujutisi on kasutatud poliitilistel või turunduslikel eesmärkidel.[204]

Samas on määruses kasutatav mõiste kooskõlas süvavõltsingute tavapärase tähendusega, kuna enamasti luuakse neid reaalselt eksisteerivatest isikutest. Lisaks laieneb mõiste ka muudele nähtustele, näiteks sündmustele või kohtadele. Süvavõltsing ei pea kujutama üksnes inimesi: võimalik on luua manipuleeritud kujutisi õnnetustest, looduskatastroofidest või sõjalistest rünnakutest. Näiteks 2023. aastal levis süvavõltsing, mis kujutas plahvatust Pentagoni lähistel ning põhjustas ajutise languse aktsiaturgudel. Sellised võltsingud võivad panustada desinformatsiooni levikusse ja sotsiaalsete rahutuste tekkesse.[205]

Määrus tugineb riskipõhisele lähenemisele, mille kohaselt kohaldatakse õigusnorme TI-süsteemide riskitaseme intensiivsuse ja ulatuse alusel. Selle tulemusel on määruses keelatud teatavad vastuvõetamatuks peetavad TI kasutusviisid, suure riskiga TI-süsteemidele on kehtestatud nõuded ja kohustused ning teatud TI-süsteemidele on sätestatud läbipaistvuskohustused.[206] Vastuvõetamatuks peetakse näiteks TI-süsteeme, mis võimaldavad kognitiivkäitumuslikku manipuleerimist (art 5 lg 1 p a). Suure riskiga on näiteks TI-süsteemid, mida kasutatakse kriitilises taristus, nagu transport, kuna see võib ohustada inimeste elu ja tervist, mistõttu allub see rangematele nõuetele.[207]

Süvavõltsingute kontekstis kohalduvad kehtiva määruse järgi eeskätt läbipaistvuskohustused. Samas on kirjanduses leitud, et TI-süsteemid, mida kasutatakse süvavõltsitud poliitilise desinformatsiooni levitamiseks, väljapressimiseks või seksuaalseks väärkohtlemiseks, tuleks liigendada suure riskiga TI-süsteemide hulka, arvestades nende võimet põhjustada märkimisväärset kahju.[208] Kirjanduses esitatud seisukohta toetab iseenesest ka määrus ise. Määruse art 6 sätestab suure riskiga TI-süsteemide liigitamise reeglid. Määruse art 6 lg 2 sätestab, et suure riskiga TI-süsteemideks peetakse ka III lisas osutatud TI-süsteeme. III lisa lg 8 p b kohaselt on suure riskiga ka TI-süsteemid, mis on ette nähtud kasutamiseks selleks, et mõjutada valimiste või rahvahääletuste tulemusi või füüsiliste isikute hääletamiskäitumist

[204] Łabuz, M. 2024, lk 7.
[205] Łabuz, M. Regulating Deep Fakes in the Artificial Intelligence Act. – Applied Cybersecurity & Internet Governance 2023/2 (1), lk 257–258. https://www.acigjournal.com/pdf-184302-105060?filename=Regulating%20Deep%20Fakes%20in.pdf (24.04.2025).
[206] Tehisintellekti määruse põhjenduspunkt 26.
[207] Fragale, M., Grilli, V. Deepfake, Deep Trouble: The European AI Act and the Fight Against AI-Generated Misinformation. – Columbia Journal of European Law 11.11.2024. https://cjel.law.columbia.edu/preliminary-reference/2024/deepfake-deep-trouble-the-european-ai-act-and-the-fight-against-ai-generated-misinformation/ (24.04.2025).
[208] Felipe, R. M., lk 298; 302; 304.

valimistel või rahvahääletustel.[209] Samas tuleb arvestada, et tavapäraselt on süvavõltsingute tehnoloogiad mitmeotstarbelised, mis tähendab, et tehnoloogia ei pruugi olla ette nähtud ainult demokraatlike protsesside mõjutamiseks.

Määruses põhjendustes on selgitatud, et teatavad TI-süsteemid, mis on mõeldud näiteks sisu looma, võivad põhjustada spetsiifilisi kellegi teisena esinemise või pettuse riske olenemata sellest, kas süsteemid on liigitatud suure riskiga süsteemideks või mitte. Seetõttu peaksid nende süsteemide kasutamise suhtes kehtima teatud olukordades spetsifiilised läbipaistvuskohustused.[210] Põhjendustes on toodud esile, et TI-süsteemid võivad luua suures koguses sünteesitud sisu, mida inimestel on üha raskem eristada inimeste loodud ja ehtsast sisust. Nende süsteemide laialdasel kättesaadavusel ja üha paranevatel võimetel on märkimisväärne mõju teabe ökosüsteemi terviklusele ja usaldusväärsusele, põhjustades uusi mastaapse väärinformatsiooni ja manipuleerimise, pettuse, kellegi teisena esinemise ja tarbijate eksitamise riske. Seetõttu on määrusega kehtestatud nõuded, et selliste TI-süsteemide pakkujad integreeriksid süsteemi tehnilised lahendused, mis võimaldavad masinloetavas vormingus märgistada ja tuvastada selle, et väljundi on loonud või seda on manipuleerinud tehisintellektisüsteem, mitte inimene.[211] Sarnased läbipaistvuskohustused on seatud ka teatud TI-süsteemide juurutajatele, kes kasutavad TI-süsteemi, et luua või manipuleerida pildi-, audio- või videosisu, mis sarnaneb märgatavalt olemasolevate isikute, objektide, kohtade, üksuste või sündmustega ja võib inimesele ekslikult ehtne ja tõene näida (süvavõltsingud). Juurutajad peavad selgel ja eristataval viisil avalikustama, et see sisu on kunstlikult loodud või seda on manipuleeritud, märgistades TI väljundi vastavalt ja avalikustades selle tehisliku päritolu.[212]

Süvavõltsingutele kohalduvad läbipaistvuskohustused on sätestatud määruse artiklis 50. Määruse art 50 lg 2 sätestab, et TI-süsteemide, sealhulgas üldotstarbeliste TI-süsteemide pakkujad, kes loovad sünteetilist audio-, pildi-, video- või tekstisisu, tagavad, et TI-süsteemi väljundid on märgitud masinloetavas vormingus ja tuvastatavad kui kunstlikult loodud või manipuleeritud. Seega on pakkujad kohustatud integreerima süsteemi tehnilised lahendused, mis võimaldavad masinloetavas vormingus märgistada ja tuvastada selle, et väljundi on loonud või seda on manipuleerinud TI-süsteem, mitte inimene. Sellisteks tehnilisteks lahenditeks on

[209] Vt ka tehisintellekti määruse põhjenduspunkt 62.
[210] *Ibidem*, põhjenduspunkt 132.
[211] *Ibidem*, põhjenduspunkt 133.
[212] *Ibidem*, põhjenduspunkt 134.

näiteks vesimärgistamine, metaandmete identifitseerimine ja krüptograafilised meetodid sisu päritolu ja autentsuse tõendamiseks.[213]

Määruse art 50 lg 4 sätestab, et sellise TI-süsteemi juurutajad, mis loob või manipuleerib pildi-, audio- või videosisu, mis kujutab endast süvavõltsingut, avalikustavad, et sisu on kunstlikult loodud või manipuleeritud. Seega on TI-süsteemi juurutajatele seatud kohustus, et ka inimesed, mitte ainult masinad, suudaksid tuvastada, et sisu on loodud TI abil. Selleks võib kasutada näiteks hoiatusteksti. Määruse artiklis 50 lg-s 4 on sätestatud ka teatud erandid, millal läbipaistvuskohustus puudub: näiteks õiguskaitselise kasutuse puhul või juhul kui sisu on ilmselgelt kunstiline, loominguline või satiiriline. Erandid võivad aga luua halli ala, kuna pahatahtlikud juurutajad võivad tugineda argumendile, et negatiivse sisuga süvavõltsingu puhul on tegemist näiteks satiiriga.[214] Ei ole ka välistatud, et mõiste „ilmselge“ tõlgendamine võib tekitada vastakaid arvamusi, mis jäävad kohtupraktika lahendada. Seega oleks tõenäoliselt vajalik läbipaistvuskohustuse erandite kitsam piiritlemine, et välistada süvavõltsingute pahatahtlik kasutamine näiteks satiirilise kattevarju all.

Määruse artiklis 50 lg-s 2 on kasutatud mõistet üldotstarbeline TI-süsteem, mis tähendab, et ka selliste süsteemide abil on võimalik luua süvavõltsinguid. Vastavalt määruse art 3 p-le 66 põhineb üldotstarbeline TI-süsteem üldotstarbelisel TI-mudelil ja suudab teenida mitmesuguseid eesmärke ja on mõeldud nii otseseks kasutamiseks kui ka integreerimiseks teistesse TI-süsteemidesse. Vastavalt määruse art 3 p-le 63 on üldotstarbelise TI-mudeliga tegemist sealhulgas siis, kui sellist TI-mudelit treenitakse suure hulga andmetega, kasutades mastaapset enesejärelevalvet, millele on omane märkimisväärne üldisus ja suudab pädevalt täita mitmesuguseid eri ülesandeid, olenemata mudeli turule laskmise viisist, ning mida saab integreerida mitmesugustesse järgmise etapi süsteemidesse või rakendustesse, välja arvatud TI-mudelid, mida kasutatakse teadus- ja arendustegevuses või prototüüpide loomiseks enne nende turule laskmist. Üldotstarbelisteks TI-süsteemideks on näiteks DALL-E ja ChatGPT.[215]

Määruse art-s 50 sätestatud läbipaistvuskohustuste rikkumistele järgneb rahaline karistus. Määruse art 99 lg 4 p g sätestab, et artiklile 50 mittevastavuse korral kohaldatakse haldustrahvi kuni 15 000 000 eurot, või kui rikkuja on ettevõtja, kuni 3% tema eelmise majandusaasta

[213] *Ibidem*, põhjenduspunkt 133.
[214] Felipe, R. M., lk 300.
[215] Browne, J., Moloney, M. What's a FLOP? How the AI Act Regulates General Purpose AI Systems. CEDPO AI and Data Working Group Micro-Insights Series March 2024. – Confederation of European Data Protection Agencies 03.2024, lk 4. https://cedpo.eu/wp-content/uploads/How-General-Purpose-AI-Models-are-regulated-under-the-AI.pdf (24.04.2025).

ülemaailmsest kogukäibest olenevalt sellest, kumb on suurem. Võib väita, et karistuse suurus peaks motiveerima eelkõige suuri tehnoloogiaettevõtteid pidama kinni määruse nõuetest. Küll aga esineb määruse jõustamisel tõenäoliselt praktilisi raskusi, kuna süvavõltsingute tehnoloogiate pakkujad ja juurutajad võivad tegutseda anonüümselt, misläbi võib nende reaalne sanktsioneerimine osutuda keeruliseks.

Tehisintellekti määrus loob läbi läbipaistvuskohustuste seega õigusliku raamistiku, mis tagab süvavõltsingute reguleerimise juba nende elütsükli varases etapis. Määrusega mitte ainult ei ennetata süvavõltsingutega seotud kahjusid, vaid luuakse ka selgem ja usaldusväärsem regulatiivne raamistik, mis maandab TI potentsiaalseid riske ühiskonnale. Samas ilmneb vajadus jätkata õiguslike sätete täpsustamist ja süvavõltsingute spetsiifiliste ohtude detailsemat reguleerimist. Oluline on edaspidi jälgida, kas läbipaistvuskohustused suudavad ennetada süvavõltsingutega kaasnevaid ühiskondlikke ja õiguslikke riske, või on vajalik täiendav, kitsamalt sihitud ja rangem regulatsioon.

3.4.2. Isikuandmete kaitse üldmäärus

Isikuandmetel on süvavõltsingute elütsüklis määrav roll. EL-is kaitseb andmesubjekte isikuandmete kaitse üldmäärus (IKÜM). Vastavalt IKÜM art 4 p-le 1 on isikuandmed igasugune teave tuvastatud või tuvastatava füüsilise isiku („andmesubjekti“) kohta. Tulenevalt IKÜM-i laiasõnalisest isikuandmete definitsioonist, kuuluvad ka andmed, mida kasutatakse TI-süsteemide treenimiseks või süvavõltsingute loomiseks, IKÜM-i kaitse alla.

IKÜM art 6 sätestab, et isikuandmete töötlemine on seaduslik ainult juhul, kui on täidetud vähemalt üks kuuest artiklis märgitud tingimusest. Süvavõltsinguid puudutavas saaksid töötlejad tugineda eelkõige sellele, et andmesubjekt on andnud nõusoleku töödelda oma isikuandmeid ühel või mitmel konkreetsel eesmärgil (art 6 lg 1 p a) või et isikuandmete töötlemine on vajalik vastutava töötleja või kolmanda isiku õigustatud huvi korral (art 6 lg 1 p f).[216] Kui süvavõltsingu loomine hõlmab protsessi, kus ühe isiku nägu monteeritakse näiteks teise isiku keha peale, on IKÜM-i nõuete täitmiseks vajalik mõlema poole nõusolek.[217] Tuginedes õigustatud huvile, peab süvavõltsingu looja kaaluma enda õigustatud huvi andmesubjekti huvide või põhiõiguste- ja vabadustega. Sellise huvi sisustamisel võivad

[216] Felipe, R. M., lk 307–308.
[217] *Ibidem*, lk 308.

pahatahtlikud isikud viidata näiteks sõnavabadusele või teadus- ja kunstitöö vabadusele (Euroopa Liidu põhiõiguste harta[218] artiklid 11 ja 13), väites, et süvavõltsingu loomine on osa loovast või uurimuslikust eneseväljendusest. Ka isikuandmete kaitse seadus[219] § 5 sätestab, et isikuandmeid võib andmesubjekti nõusolekuta töödelda akadeemilise, kunstilise ja kirjandusliku eneseväljenduse eesmärgil, eelkõige avalikustada, kui see ei kahjusta ülemäära andmesubjekti õigusi. Seega tuleb alati hinnata, kas andmesubjekti põhiõigused ja vabadused kaaluvad üle väidetava õigustatud huvi. Kui näiteks süvavõltsingu eesmärgiks on luua poliitilist satiiri, võiks sõnavabadust käsitleda õigustatud huvina, mis võib kaaluda üle andmesubjekti huvid. Kui aga eesmärgiks on luua kujutis, milles on isikut kujutatud häbistaval, näiteks seksuaalselt ahistaval viisil, peaks andmesubjekti huvid kaaluma üle töötleja väidetava õigustatud huvi.[220]

Kuigi IKÜM pakub andmesubjektidele õiguskaitsevahendeid töötlejate vastu, seejuures õigust nõuda isikuandmete parandamist (art 16) ja kustutamist (art 17), ei ole need vahendid sageli praktiliselt rakendatavad tulenevalt asjaolust, et süvavõltsinguid luuakse sageli anonüümselt, mis raskendab töötleja tuvastamist. Seejuures muudab õiguskaitsevahendite rakendamise keeruliseks asjaolu, et kui süvavõltsingud juba korra internetti üles laetakse, võivad need sinna ka ringlema jääda.[221]

3.4.3. Digiteenuste määrus

Digiteenuste määrust[222] (edaspidi: DSA) omab ka süvavõltsingutele regulatiivset mõju. Määruse eesmärgiks on panustada toimivasse vahendusteenuste siseturgu, ning luua harmoniseeritud reeglid turvalise, prognoositava ja usaldusväärse internetikeskkonna tarbeks.[223] Määrus tugineb turupiirkonna asukoha põhimõttele, rakendudes kõigile teenuseosutajatele, kelle teenuseid kasutavad ELis asuvad isikud, sõltumata teenuseosutaja enda asukohast.[224]

[218] Euroopa Liidu põhiõiguste harta. – ELT C 202, 7.6.2016, lk 389–405.
[219] Isikuandmete kaitse seadus. – RT I, 31.12.2024, 44.
[220] Felipe, R. M., lk 308.
[221] *Ibidem*, lk 309–310.
[222] 19. oktoobri 2022. aasta Euroopa Parlamendi ja nõukogu määrus (EL) 2022/2065, mis käsitleb digiteenuste ühtset turgu ja millega muudetakse direktiivi 2000/31/EÜ (digiteenuste määrus). – ELT L 277, 27.10.2022, lk 1–102.
[223] DSA põhjenduspunkt 9.
[224] *Ibidem*, põhjenduspunkt 7.

Süvavõltsingud levivad avalikkuseni peamiselt interneti kaudu, enamasti digiplatvormidel (art 3 p i), nagu sotsiaalmeediaplatvormid, mis osutavad teabe talletamise teenust (art 6). Art 6 lg 1 sätestab, et teenuseosutaja ei vastuta talletava teabe eest, kui teenuseosutajal pole tegelikku teavet tegevuse või ebaseadusliku sisu kohta (p a) ning kui teenuseosutaja tegeleb pärast sellise teabe saamist või teadlikkuse tekkimist kiiresti, et eemaldada ebaseaduslik sisu või tõkestada sellele juurdepääs (p b). Seega sõltub teenuseosutaja vastutus sellest, kas ta on teadlik platvormil levivast ebaseaduslikust sisust ning kui kiiresti ta selle eemaldamiseks tegutseb.

Süvavõltsingute reguleeritavus DSA alusel sõltub sellest, kas neid käsitletakse ebaseadusliku sisuna määruse art 3 p h tähenduses. Ebaseaduslik sisu on DSA tähenduses igasugune teave, mis iseenesest või seotuse tõttu teatava tegevusega, sh toodete müügi või teenuste osutamisega, ei ole kooskõlas liidu või mis tahes liikmesriigi õigusega, olenemata selle õiguse täpsest reguleerimisesemest või laadist. DSA annab ebaseadusliku sisu mõistele võrdlemisi laia tõlgendusruumi, mis on kooskõlas määruse põhjendustes esitatud eesmärgiga.[225] DSA põhjendustes on selgitatud, et mõistet tuleks mõista nii, et see osutab igasuguses vormis teabele, mis kohaldatava õiguse kohaselt on iseenesest ebaseaduslik – näiteks ebaseaduslik vaenukõne või terroristlik sisu ja ebaseaduslik diskrimineeriv sisu – või kui kohaldatavate normide kohaselt on teave ebaseaduslik, kuna see on seotud ebaseadusliku tegevusega. Sellise ebaseadusliku tegevuse näited on muu hulgas laste seksuaalset kuritarvitamist kujutavate piltide jagamine, ebaseaduslik privaatpiltide loata jagamine ja küberahistamine.[226] Seega haakub süvavõltsingute olemus teatud juhtudel DSA ebaseadusliku sisu mõistega.

DSA art 16 lg 1 kohustab teabe talletamise teenuste osutajaid kehtestama lihtsad ja elektroonilised mehhanismid, mille kaudu igaüks saab teavitada keskkonnas levivast ebaseaduslikust sisust. Saadud teateid tuleb töödelda aegsasti, hoolsalt, erapooletult ja objektiivselt, otsustades sisu eemaldamise või leviku piiramise üle (art 16 lg 6). Seega, kui kasutaja märkab platvormil ebaseadusliku sisuga süvavõltsingut, peab tal olema võimalus sellest teavitada ja platvorm peab kiiresti reageerima. Lisaks nõuab DSA artikkel 12 lõige 1, et teenuseosutajad määraksid ühtse kontaktpunkti elektrooniliseks ja kasutajasõbralikuks suhtluseks, mis on süvavõltsingute kontekstis eriti oluline, kuna seksuaalse väärkohtlemise ohvritel on tihti raskusi sisutõrje saavutamisega.[227] Tasub märkida, et viiteid DSA-le nähtub ka

[225] DSA põhjenduspunkt 12.
[226] DSA põhjenduspunkt 12.
[227] Rigotti, C., *et al*. Image-Based Sexual Abuse and EU Law: A Critical Analysis. German Law Journal 2024/25 (9), lk 1489. https://www-cambridge-org.ezproxy.utlib.ut.ee/core/journals/german-law-

tehisintellekti määrusest. Tehisintellekti määruse põhjendustes rõhutatakse, et TI abil loodud sisu märgistamise kohustus ei piira DSA artikli 16 lõike 6 alusel teabe talletamise teenuse pakkujatele pandud kohustust töödelda teateid ebaseadusliku sisu kohta ega mõjuta konkreetse sisu ebaseaduslikkuse hindamist.[228]

Väga suurtele digiplatvormidele ja internetipõhistele otsingumootoritele kehtestab DSA täiendavad kohustused. DSA art 33 lg 1 kohaselt loetakse nendeks platvormideks ja otsingumootoriteks sellised, mida kasutavad liidus keskmisel vähemalt 45 miljonit aktiivset teenusesaajat kuus. Väga suur digiplatvorm on näiteks Facebook ja väga suur otsingumootor näiteks Google.[229] Sellistele teenuseosutajatele rakenduvad muu hulgas täiendavad kohustused, nagu riskihindamine (art 34), riskide maandamine (art 35) ning sõltumatu audit (art 37).

DSA abil on loodud õiguslik raamistik, kus teatud süvavõltsingud – näiteks pornograafilise sisuga teosed, mida on loodud ja levitatud ilma kujutatud isiku nõusolekuta, valimispettusi levitavad või terroristliku sisuga visuaalid – võivad kvalifitseeruda ebaseaduslikuks sisuks ja seeläbi kuuluda eemaldamiskohustuse alla. Samas ei ole süvavõltsingud oma olemuselt automaatselt ebaseaduslikud. Ebaseaduslikkus sõltub DSA tähenduses nende sisust, kontekstist ja mõjust kolmandate isikute õigustele.

3.3.4 Naistevastase vägivalla ja perevägivalla tõkestamise direktiiv

2024. aastal vastu võetud Euroopa Parlamendi ja nõukogu direktiiv (EL) 2024/1385 rõhutab vajadust ühtlustada kuritegude ja karistuste määratlusi kübervägivalla puhul, kus vägivald on seotud info- ja kommunikatsioonitehnoloogia (edaspidi: IKT) kasutamisega. Põhjendustes tuuakse esile, et kübervägivald tabab eelkõige naisi – eriti poliitikuid, ajakirjanikke ja inimõiguslasi – ning võib viia sotsiaalse tõrjutuse, ärevuse ja äärmuslikel juhtudel enesetapuni.[230] Direktiiv haakub otseselt eelnevates peatükkides kirjeldatud süvavõltsingutest põhjustatud ohtudega, mis mõjutavad ohvrite vaimset tervist ja ühiskondlikku osalust. Täiendavalt on selgitatud, et IKT kasutamisega kaasneb oht, et teatavat liiki kübervägivald

journal/article/imagebased-sexual-abuse-and-eu-law-a-critical-analysis/B0CF334A0037DE3CA2067B79F506EB87 (25.04.2025).

[228] Tehisintellekti määruse põhjendus 136.

[229] Supervision of the designated very large online platforms and search engines under DSA. – Euroopa Komisjon 06.02.2025. https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses (25.04.2025).

[230] Naistevastase vägivalla ja perevägivalla tõkestamise direktiivi põhjenduspunkt 17.

võimendub kergesti, kiiresti ja ulatuslikult, mis tähendab selget ohtu tekitada ohvrile sügavat ja pikaajalist kahju või süvendada seda.[231] Ka see haakub eelnevalt töös kirjeldatuga.

Lisaks on selgitatud, et ilma isiku nõusolekuta tema intiimpiirkonda või seksuaaltegevust kujutava materjali levitamine IKT vahendite abil võib ohvrile põhjustada tõsist kahju, arvestades sellise sisu leviku kiirust ja intiimsust. Direktiiviga hõlmatakse kõik materjaliliigid – pildid, videod, audioklipid jms –, olenemata sellest, kas ohver oli loomisega nõus või edastas selle ise. Samuti käsitletakse keelatud tegevusena materjali nõusolekuta tootmist, muutmist või manipuleerimist, sealhulgas TI abil loodud süvavõltsinguid, mis jätavad eksitava mulje ohvri seksuaaltegevusest.[232] Direktiivi kohaselt on tõsist kahju tekitav käitumine selline, mis tõenäoliselt põhjustab ohvrile rasket psühholoogilist kahju või hirmu enda ja lähedaste turvalisuse pärast. Raske kahju tõenäosust hinnatakse iga juhtumi konkreetseid asjaolusid arvestades, tuginedes objektiivsetele faktidele.[233] Ka seetõttu on oluline, et avalikkus ja õiguskaitseorganid mõistaksid süvavõltsingute potentsiaalset kahju. Eelnevalt on järeldatud, et intiimse sisuga süvavõltsingute loomine ja levitamine põhjustab tavaliselt tõsist kahju ning ei saa olla käsitatav väikese rikkumisena.

Direktiivi art 5 lg 1 kohustab seega liikmesriike kriminaliseerima sellised teod, kus ilma isiku nõusolekuta tehakse IKT vahenditega avalikkusele kättesaadavaks tema intiimseid kehaosi või seksuaaltegevust kujutav materjal (art 5 lg 1 p a), samuti seksuaaltegevusest mulje jätva materjali tootmine, manipuleerimine, muutmine ja sellejärgne levitamine (art 5 lg 1 p b), kui sellega põhjustatakse ohvrile tõsist kahju. Seega kuuluvad kriminaliseerimisele nii nn tavapärase kättemaksuporno levitamine kui ka nõusolekuta pornograafiliste süvavõltsingute loomine ja levitamine. Täiendavalt sätestab art 5 lg 1 p c, et kriminaalkorras kuulub karistamisele ka eeltoodud tegudega ähvardamine, et sundida isikut midagi tegema, millegagi nõustuma või millegi tegemisest hoiduma. Art 5 lg 1 p c haakub seega Eestis kehtiva KarS §-ga 214, kuid on mõnevõrra laiem, kuna KarS § 214 süüteokoosseisu tunnuseks on varalise kasu üleandmise nõudmine. Direktiivi art 10 lg 4 sätestab, et art-s 5 osutatud kuritegude eest mõistetava vangistuse ülemmäär on üks aasta, kusjuures art 11 näeb ette ka erinevad raskendavad asjaolud (nt kui süütegu pandi toime endise elukaaslase vastu või korduvate rikkumiste puhul). Arvestades, et kord loodud pornograafilise sisuga süvavõltsingud võivad jääda ohvrit aastateks painama, tulenevalt ka sellest, et materjal võibki jääda internetti levima,

[231] *Ibidem*, põhjenduspunkt 18.
[232] *Ibidem*, põhjenduspunkt 19.
[233] *Ibidem*, põhjenduspunkt 18.

saab vangistust pidada mõjusaks, proportsionaalseks ja hoiatavaks.[234] Direktiivi art 49 lg 1 sätestab, et liikmesriigid jõustavad käesoleva direktiivi järgimiseks vajalikud õigus- ja haldusnormid hiljemalt 14. juuniks 2027.

Kirjanduses on märgitud, et direktiivi sõnastus võib põhjustada rakendusprobleeme. Art 5 lg 1 p a hõlmab vaid intiimsete kehaosade või seksuaaltegevuse kujutamist, jättes välja muu intiimse käitumise, nagu riiete vahetamine või tualeti kasutamine.[235] Selle kriitikaga võib nõustuda, kuna ka sellise materjali levitamine võib ohvrit kahjustada. Probleeme tekitab ka art 5 lg 1 p b, mis kriminaliseerib vaid seksuaaltegevust kujutavad süvavõltsingud, jättes välja näiteks alasti kujutised.[236] Kirjanduses esitatud kriitikaga võib nõustuda, kuna isikutest luuakse ka sellist materjali, mis kujutab isikuid alasti, kuid mitte konkreetselt seksuaaltegevuses. Selliselt loodi süvavõltsinguid näiteks eespool kirjeldatud Almendralejo kaasuses. Ka art 5 lg 1 p c on leidnud mõistetavat kritiikat, kuna see ei pruugi hõlmata juhtumeid, kus näiteks endine elukaaslane ähvardab intiimse sisuga materjali levitamisega ainuüksi eesmärgiga põhjustada ohvrile psühholoogilist kahju, ilma et ta midagi konkreetset nõuaks.[237] See tähendab, et tõenäoliselt vajaks säte ümbersõnastamist ja täpsustamist viisil, mis keelaks ka teod, kus isikutest luuakse ja levitatakse materjali, mis kujutab neid ka intiimsetes olukordades, mitte ainult seksuaalses tegevuses. Samas saab pidada kiiduväärseks, et EL on otsustanud rakendada konkreetseid süvavõltsingute kriminaliseerimisele suunatud meetmeid.

3.3.5. Vahekokkuvõte

EL on seadnud eesmärgiks TI ja süvavõltsingute reguleerimise. 2024. aastal vastu võetud tehisintellekti määrus sätestab esmakordselt süvavõltsingute mõiste ning kehtestab läbipaistvuskohustused TI-süsteemide pakkujatele ja juurutajatele. DSA kohustab platvorme eemaldama ebaseaduslikku sisu, sealhulgas teatud süvavõltsinguid, ning IKÜM annab ohvritele meetmed andmete väärkasutuse korral. Naistevastase vägivalla ja perevägivalla direktiiv kohustab liikmesriike 2027. aastaks kriminaliseerima süvavõltsingute nõusolekuta loomise ja levitamise ning sellise tegevusega ähvardamise. Kuigi EL õiguslik raamistik vajab veel kindlasti täiendamist, on esimesed olulised sammud ohtude maandamise suunas astutud.

[234] Vt ka naistevastase vägivalla ja perevägivalla tõkestamise direktiivi põhjenduspunkt 28.
[235] Rigotti, C., *et al*., 2024, lk 1483.
[236] *Ibidem*, lk 1484.
[237] *Ibidem*.

KOKKUVÕTE

Käesolevas magistritöös uuriti süvavõltsingute fenomeni, käsitledes nende arengut, kaardistades peamisi ohte ning analüüsides, kuidas Eestis ja Euroopa Liidus kehtiv õiguslik raamistik suudab neile ohtudele reageerida ja neid maandada. Analüüsi tulemusena leiti, et süvavõltsingud kujutavad tõsist ohtu eelkõige kolmes valdkonnas: naiste- ja lastevastases seksuaalses väärkohtlemises, poliitilises manipulatsioonis ja desinformatsiooni levitamises ning finantskuritegevuses.

Töö üheks keskseks järelduseks on see, et süvavõltsingute kõige akuutsem ja vahetum oht avaldub just soopõhise ja seksuaalse vägivalla kontekstis. Magistritöös leiti, et süvavõltsingud kujutavad endast uut digitaalse vägivalla vormi, kandes soopõhise ja seksuaalse väärkohtlemise ohud tehnoloogilisse keskkonda ning võimendades seniseid probleeme raskemini tuvastataval viisil. Süvavõltsingute tehnoloogia võimaldab luua realistlikke pornograafilisi videoid peaaegu igaühest. Erinevalt varasematest tehnoloogiatest võimaldab süvavõltsingute tehnoloogia kiiresti ja vähese vaevaga luua väga realistlikku kahjustavat materjali, mida saab massiliselt levitada. Materjali levik internetis süvendab hirmu ja umbusaldust, pärssides naiste osalust avalikus elus ja suurendades laste taasohvristamise riski. Samas on näha, et avalikkuse teadlikkus süvavõltsingute tegelikust mõjust on endiselt madal, mistõttu alahinnatakse ohvrite kannatusi. Madal teadlikkus koos tehnoloogia kättesaadavuse ja visuaalse veenvusega võib aidata kaasa virtuaalse väärkohtlemise normaliseerumisele.

Süvavõltsingud kujutavad demokraatiale ohtu kolmel tasandil. Esiteks võimaldavad need levitada valeinfot, nagu näitasid 2023. aasta juhtumid Ühendkuningriigis ja Slovakkias. Teiseks soodustab süvavõltsingute olemasolu valetaja dividendi nähtust, kus ka autentset materjali võidakse pidada võltsituks, võimaldades poliitikutel vastutusest kõrvale hiilida, nagu ilmnes Malaisia skandaalis. Tasub aga märkida, et valetaja dividendi efekt ei pruugi olla nii tõhus kui varasemalt arvati. Kolmandaks võib süvavõltsingute kasutamine süvendada kriisi- ja julgeolekusituatsioonides ohtu, et otsuseid tehakse eksitava info põhjal. Lisaks võivad süvavõltsingud võimendada ühiskondlikku polariseerumist ja moonutada ajaloolist mälu, süvendades usalduskriisi demokraatlike institutsioonide ja meedia suhtes.

Süvavõltsingute tehnoloogia kujutab tõsist ohtu finantskuritegevuses. Realistlikkus, madalad loomekulud ja tehnoloogiline kättesaadavus soodustavad pettusi, kus juba üks edukas skeem võib tuua kuritegelikele võrgustikele märkimisväärset kasumit. Mida veenvamaks muutub

võltsitud sisu, seda suurem on petuskeemide õnnestumise tõenäosus ja motivatsioon investeerida veelgi keerukamatesse lahendustesse. Finantssektor on eriti haavatav, sest süvavõltsingud õõnestavad lisaks varalisele kahjule ka usaldust autentimissüsteemide vastu. Süvavõltsingutel põhinevad kuriteod kasutavad veenvalt manipuleeritud heli- ja videomaterjali, millega eksitatakse juhte ja töötajaid. Seetõttu peavad õiguskaitseorganid ja finantsasutused uuendama oma turvameetmeid ja ennetusstrateegiaid, sealhulgas tõstma ohtudest teadlikkust. Arvestada tuleb ka rahvusvahelist mõõdet, mis muudab menetlemise keerukaks ja kulukaks. Üks tõhusamaid viise nende ohtude vähendamiseks on süsteemne ja järjepidev avalikkuse teavitustöö, mis tugevdab ühiskonna vastupanuvõimet digiajastu keerukamatele kuritegevuse vormidele.

Kuigi 2025. aasta seisuga ei ole Eesti õiguslikus raamistikus otseselt süvavõltsingutele suunatud regulatsiooni, võimaldab kehtiv raamistik teatud tingimustel süvavõltsingutega seotud juhtumitele reageerida. Eraõiguslikest meetmetest on võimalik rakendada kahju hüvitamise ja kahju tekitava tegevuse lõpetamise ja sellest hoidumise nõudeid. Lisaks on võimalik nõuda ebaõigete andmete ümberlükkamist. Karistusõiguslike meetmete rakendamisel võivad kohalduda näiteks identiteedivargust (KarS § 157²), ahistavat jälitamist (KarS § 157³), lapsporno valmistamist ja võimaldamist (KarS § 178), väljapressimist (KarS § 214) või kelmust (KarS § 209) käsitlevad sätted. Avalikkuse teadlikkus, et olemasolevaid norme saab süvavõltsingute puhul rakendada, võib omada ka heidutavat mõju.

Euroopa Liidu tasandil on viimastel aastatel käivitatud mitmeid algatusi, mille eesmärk on reguleerida TI-d, sealhulgas süvavõltsinguid. Eriti oluline on 2024. aasta lõpus vastu võetud tehisintellekti käsitlev määrus, mis sätestab esmakordselt süvavõltsingute mõiste ning kehtestab läbipaistvuskohustused TI-süsteemide pakkujatele ja juurutajatele. Lisaks kohustab digiteenuste määrus platvorme eemaldama ebaseaduslikku sisu, sealhulgas teatud liiki süvavõltsinguid. Samuti võimaldab isikuandmete kaitse üldmäärus ohvritel nõuda õiguskaitsevahendite rakendamist isikuandmete töötlemise rikkumise korral. Naistevastase vägivalla ja perevägivalla tõkestamise direktiiv kohustab liikmesriike võtma 2027. aastaks vastu karistusõiguslikud normid, mis keelaksid süvavõltsingute nõusolekuta loomise ja levitamise, sealhulgas sellise tegevusega ähvardamise. Kuigi Euroopa Liidu õigusraamistik vajab veel kindlasti täiendamist, väärivad juba astutud sammud tunnustust.

Magistritöös jõuti järeldusele, et süvavõltsingute ohtude tõhus maandamine eeldab mitmetasandilist lähenemist. Kõige tulemuslikumaks on kombineeritud lähenemine, mis

ühendab kaks põhisuunda. Esiteks tuleb arendada õiguslikku raamistikku, kehtestades selged vastutusmehhanismid süvavõltsingute väärkasutamise eest. Samuti on oluline reageerida paindlikult tehnoloogia arengust tulenevatele uutele riskidele. Teiseks tuleb panustada ühiskondliku teadlikkuse tõstmisesse: suurendada meediakirjaoskust, arendada kriitilist mõtlemist valeinfo suhtes ja parandada teadlikkust digitaalsetest ohtudest.

Kokkuvõttes võib tõdeda, et süvavõltsingud on ühtaegu tehnoloogiline innovatsioon, mis peegeldab TI kasulikke võimalusi, kuid samal ajal paneb tõsiselt proovile ühiskondliku vastupidavuse. Magistritöö näitas, et kuigi süvavõltsingutest tulenevad ohud on tõsised, ei ole need ületamatud ning sihipärased õiguslikud ja ühiskondlikud meetmed võivad pakkuda toimivaid lahendusi. Esimesed sammud on tehtud, ent ees seisab pikk tee süsteemsete ja terviklikumate lahendusteni. Lõppjäreldus rõhutab vajadust tasakaalu leidmise järele: ühelt poolt on oluline kaitsta tõde, usaldusväärsust ja turvalisust, teisalt tuleb avatuna hoida innovatsiooni ja loovuse arenguvõimalused. Süvavõltsingute esitatud väljakutse sunnib meid ümber mõtestama, mis on tänapäeval tõde, kuidas infot kontrollida ja mille alusel seda usaldada. Edu mõõdupuuks saab olema suutlikkus kujundada õiguslik raamistik, mis kaitseb faktide ja tõe tähendust ka üha veenvamate manipulatsioonide ajastul. Tehnoloogia arenedes peavad arenema ka meie kaitsemehhanismid: sihipärase ja koordineeritud tegutsemisega on võimalik kasutada TI positiivset potentsiaali, kaitstes samal ajal põhiväärtusi, millest sõltuvad vabad ja avatud ühiskonnad.

RISKS ASSOCIATED WITH THE CREATION AND DISTRIBUTION OF DEEPFAKES AND THEIR MITIGATION THROUGH THE EXISTING LEGAL FRAMEWORK. Abstract

This master's thesis undertakes a comprehensive study of the phenomenon of deepfakes, a rapidly advancing form of synthetic media produced through artificial intelligence technologies. The thesis examines the evolution of deepfake technology, maps the various risks associated with its misuse, and analyzes the extent to which the current Estonian and European Union legal frameworks are equipped to respond to and mitigate these emerging threats. Through detailed analysis, the study identifies three primary domains where deepfakes present considerable and growing risks: gender-based sexual abuse, political manipulation and disinformation, and financial crime.

One of the central findings of this study is that the most acute and immediate threat posed by deepfakes arises within the sphere of gender-based violence and sexual exploitation. Deepfake technology enables the creation of hyper-realistic pornographic videos and other intimate content without the consent of the individuals depicted, fundamentally transforming and exacerbating the landscape of digital sexual abuse. This evolution marks a significant departure from earlier forms of image or video manipulation, which often required specialized skills and remained relatively detectable. In contrast, contemporary deepfake tools allow for the rapid, effortless, and large-scale production and dissemination of harmful material, frequently accessible to even unskilled users. The viral nature of digital platforms compounds the damage: once deepfake content is released, it spreads uncontrollably across social media, forums, and encrypted networks, making removal virtually impossible and amplifying the trauma experienced by victims. This persistent circulation fosters pervasive fear and distrust, particularly among women, leading many to self-censor, withdraw from public, social, and professional spheres, and experience profound violations of their autonomy and dignity. Children, as particularly vulnerable targets, face heightened risks of secondary victimization, with long-lasting psychological harm that can extend into adulthood.

Moreover, the research reveals that societal awareness of the deep emotional, psychological, and reputational consequences of deepfake victimization remains alarmingly limited. The public frequently underestimates the severity of these abuses, often trivializing them as harmless pranks or fictional entertainment, rather than recognizing them as serious and enduring violations of human rights. This gap in understanding, combined with the growing

accessibility and realism of deepfake technologies, contributes to the normalization of virtual forms of sexual violence. In turn, this normalization risks reinforcing harmful gender stereotypes, perpetuating a culture of objectification, and undermining broader efforts to combat gender-based violence both online and offline.

The findings suggest that without concerted legal and societal interventions, deepfakes could further entrench patterns of discrimination and abuse in the digital age, creating a chilling effect on women's and marginalized groups' participation in public discourse and professional life. Addressing the challenges posed by deepfake-enabled sexual exploitation thus demands not only stronger legal protections and enforcement mechanisms but also sustained public awareness campaigns, targeted support for victims, and a broader societal commitment to safeguarding dignity, consent, and equality in the digital environment.

Beyond the profound personal harms inflicted on individuals, deepfakes also present systemic threats to democratic institutions and the overall functioning of open societies. This thesis identifies three principal mechanisms through which deepfakes erode democratic resilience and institutional trust. Firstly, deepfakes serve as powerful tools for the dissemination of disinformation and the fabrication of alternative narratives, with the potential to mislead voters, destabilize electoral processes, and manipulate public opinion on a large scale. Real-world examples from the United Kingdom and Slovakia in 2023 illustrate how strategically released deepfake content could influence political dynamics, shift electoral outcomes, and fuel public confusion, particularly when disseminated during critical periods such as election campaigns or political crises. The speed, reach, and emotional impact of deepfake-driven disinformation campaigns dramatically complicate efforts to safeguard democratic deliberation and informed citizen participation.

Secondly, the mere existence and public awareness of deepfakes have given rise to the phenomenon known as the „liar's dividend." This dynamic allows individuals, particularly public figures such as politicians and corporate leaders, to cast doubt on the authenticity of genuine evidence, dismissing legitimate allegations as fabrications. The Malaysian political scandal highlighted in the thesis serves as a vivid case study, demonstrating how the invocation of deepfakes, even without substantive evidence, can effectively shield wrongdoers from accountability. However, the research also nuances this understanding by acknowledging that regarding video deepfakes, the liar's dividend is not uniformly effective.

Thirdly, in high-stakes crisis and security contexts – such as armed conflicts or terrorist threats – deepfakes pose an even graver danger. They can inject false or misleading information into fast-moving situations, forcing military, political, or humanitarian actors to make rapid decisions based on manipulated evidence. The incidents involving Ukraine's leadership underscore how deepfake technology could be weaponized to sow confusion, demoralize populations, and manipulate the course of conflicts. In such volatile environments, the ability to trust the authenticity of information becomes not merely a matter of political preference but a question of national and human security.

The cumulative effects of deepfake dissemination reach far beyond individual events. Over time, the repeated exposure to fake or contested content might contribute to deep societal polarization, erode collective memory, and foster cynicism toward institutions traditionally entrusted with upholding truth. As deepfakes increasingly blur the line between reality and fabrication, the very foundations of democratic governance – transparency, accountability, and public trust – are placed at risk. Strengthening democratic resilience against deepfake-driven manipulation thus demands comprehensive strategies encompassing legal, technological, educational, and societal measures aimed at reinforcing the critical infrastructures of truth and trust that open societies depend upon.

The thesis further demonstrates that deepfake technology poses profound and rapidly evolving challenges to the financial sector, threatening not only individual institutions but also the broader integrity of financial markets and economic stability. The increased realism of synthetic audio and video content, combined with the relatively low production costs and widespread availability of deepfake-generating tools, has significantly lowered the barriers to entry for sophisticated fraud schemes. Criminal enterprises can now exploit deepfakes to convincingly impersonate corporate executives, forge internal communications, fabricate client interactions, and circumvent traditional authentication mechanisms such as voice or video-based identity verification systems.

This technological advancement elevates the complexity and success rate of social engineering attacks, such as CEO fraud, by adding a potent audiovisual dimension that significantly boosts credibility in the eyes of unsuspecting victims. As the technical quality of synthetic media forgeries continues to improve, the probability of successful scams rises correspondingly, providing strong incentives for organized crime networks to invest heavily in the development and deployment of advanced synthetic media capabilities. What once required elaborate

planning and insider knowledge can now be achieved remotely and at scale, amplifying both the reach and impact of financial crimes.

The financial sector's inherent dependence on trust, rapid decision-making, and reliable verification systems renders it uniquely vulnerable to such threats. A single deepfake-enabled breach can not only cause substantial direct financial losses but also erode confidence in digital communication channels, client verification procedures, and the security of transactions. Consequently, financial institutions are under increasing pressure to continuously upgrade their cybersecurity infrastructure, integrate advanced detection technologies capable of identifying manipulated media, and train employees to recognize the warning signs of deepfake-enabled fraud attempts.

Moreover, the transnational and decentralized nature of cybercrime involving deepfakes significantly complicates law enforcement and judicial efforts. Criminal actors often operate across multiple jurisdictions, exploiting regulatory gaps and differences in legal frameworks to evade detection and prosecution. This reality underscores the urgent need for enhanced international cooperation.

Recognizing and addressing the human factor remains equally critical. Public education campaigns aimed at raising awareness about the risks and indicators of deepfake fraud must become a central pillar of financial crime prevention strategies. Empowering both financial sector employees and the general public with the knowledge and tools to critically assess audiovisual information can significantly reduce societal vulnerability. Ultimately, building financial sector resilience against deepfake-enabled threats requires a holistic approach that combines technological innovation, robust regulatory frameworks, institutional vigilance, and widespread societal engagement.

Although, as of 2025, Estonian law does not yet contain specific regulations directly addressing deepfakes, the existing legal framework provides mechanisms to respond to related harms. Civil remedies, including claims for damages and injunctions to prevent ongoing harm, offer victims a path to seek redress. In parallel, criminal law provisions targeting offenses such as identity theft (Penal Code § 157[2]), harassing pursuit (Penal Code § 157[3]), child pornography (Penal Code § 178), extortion (Penal Code § 214), and fraud (Penal Code § 209) can be applied depending on the nature of the deepfake incident. Raising public awareness about the applicability of these legal provisions to deepfake-related offenses can enhance deterrence and reinforce the legitimacy of the legal system's response.

At the European Union level, significant regulatory initiatives have been launched to address artificial intelligence broadly, with specific attention to the challenges posed by deepfakes. The AI Act, adopted in late 2024, marks a critical milestone by providing the first explicit legal definition of deepfakes and imposing transparency obligations on developers and users of AI systems. Complementing this, the Digital Services Act mandates platform operators to remove illegal content, including deepfakes where applicable, thus tightening the responsibility of intermediaries. The General Data Protection Regulation (GDPR) offers additional recourse for victims whose personal data is misused in the creation of deepfakes. Moreover, the recently adopted Directive on combating violence against women and domestic violence requires all EU member states, including Estonia, to criminalize the creation and distribution of non-consensual deepfake content by 2027. These developments collectively signal a growing recognition within the EU of the urgent need to address the unique challenges deepfakes pose across multiple dimensions of societal life.

Deepfakes epitomize the dual-edged nature of technological progress: on one side, they showcase the extraordinary creative potential and innovation of generative artificial intelligence; on the other, they expose profound vulnerabilities within our social, legal, economic, and political systems. They challenge our ability to verify truth and authenticity and strain the resilience of institutions that rely on a shared factual foundation. While the risks introduced by deepfakes are serious – undermining individual rights, destabilizing democratic discourse, facilitating financial crimes, and eroding public trust – they are not insurmountable.

The thesis ultimately concludes that effectively managing the risks associated with deepfakes requires a multi-layered and integrative strategy. Confronting these challenges demands a comprehensive and proactive response. Legal reforms must provide clear definitions, establish accountability mechanisms, and ensure enforceable sanctions for the malicious use of synthetic media. Equally important is the societal dimension: widespread public awareness initiatives are crucial for promoting media literacy, critical thinking, and an informed skepticism toward digital content. Empowering citizens to recognize and challenge manipulated information will help reduce societal vulnerability. Only through such a dual approach – combining robust legal action with proactive societal engagement – can the growing threats posed by deepfakes be meaningfully addressed.

Ultimately, the true measure of success will lie in our collective ability to uphold the integrity of information in an era where synthetic realities are increasingly indistinguishable from

authentic ones. Preserving the boundary between fact and fabrication is essential not only for protecting individual dignity but also for ensuring the continued functioning of democratic institutions founded on truth, accountability, and public trust. As technology evolves, so must our defenses: and with deliberate, coordinated efforts, it is possible to harness the positive potential of AI while safeguarding the fundamental values on which free and open societies depend.

KASUTATUD LÜHENDID

3D – kolmemõõtmeline

AI – Artificial Intelligence, eesti keeles: tehisintellekt

art – artikkel

CSAM – Child Sexual Abuse Material, eesti keeles: laste seksuaalse väärkohtlemise materjal

DSA – digiteenuste määrus

EL – Euroopa Liit

FTC – Föderaalne kaubanduskomisjon

GAN – generative adversarial network

IKT – info- ja kommunikatsioonitehnoloogia

IKÜM – isikuandmete kaitse üldmäärus

IWF – Internet Watch Foundation

KarS – karistusseadustik

komm – kommentaar

lg – lõige

lk – lehekülg

m – määrus

MIT – Massachusetts Institute of Technology

o – otsus

p – punkt

PS – Eesti Vabariigi põhiseadus

RKKK – Riigikohtu kriminaalkolleegium

SKP – sisemajanduse kogutoodang

TI – tehisintellekt

TlnRnK – Tallinna Ringkonnakohus

TMK – Tartu Maakohus

USA – Ameerika Ühendriigid

VAE – variational autoencoder

vlj – väljaanne

VÕS – võlaõigusseadus

ÜRO – Ühinenud Rahvaste Organisatsioon

KASUTATUD MATERJALID

Kasutatud kirjandus

1. Acemoglu, D. The simple macroeconomics of AI. – Economic Policy 2025/40 (121), lk 13–58. https://doi.org/10.1093/epolic/eiae042 (23.03.2025).
2. Amerini, I., Barni, M., Battiato, S., Bestagini, P., Boato, G., Bruni, V., Caldelli, R., De Natale, F., De Nicola, R., Guarnera, L., Mandelli, S., Majid, T., Marcialis, G. L., Micheletto, M., Montibeller, A., Orrù, G., Ortis, A., Perazzo, P., Puglisi, G., ... Vitulano, D. Deepfake Media Forensics: Status and Future Challenges. – Journal of Imaging 2025/11 (3), lk 1–42. https://www.researchgate.net/publication/389456404 (23.03.2025).
3. Chesney, B., Citron, D. Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security. California Law Review 2019/107 (6), lk 1753–1820. https://heinonline-org.ezproxy.utlib.ut.ee/HOL/Page?collection=journals&handle=hein.journals/calr107&id=1806&men_tab=srchresults (24.04.2025).
4. Das, M. K., Kumar, M., Kapil, I. K., & Yadav, R. K. Deepfake Creation Using Gans and Autoencoder and Deepfake detection. – 2nd International Conference on Vision Towards Emerging Trends in Communication and Networking Technologies (ViTECoN), Vision Towards Emerging Trends in Communication and Networking Technologies (ViTECoN), 2023 2nd International Conference On 05.2023, lk 1–6. https://ieeexplore-ieee-org.ezproxy.utlib.ut.ee/stamp/stamp.jsp?tp=&arnumber=10157962 (25.04.2025).
5. Dunn, S. Legal Definitions of Intimate Images in the Age of Sexual Deepfakes and Generative AI. – McGill Law Journal 2024/69, lk 1–15. https://ssrn.com/abstract=4813941 (23.04.2025).
6. Felipe, R. M. Generative AI and deepfakes: a human rights approach to tackling harmful content. – International Review of Law, Computers & Technology 2024/38 (3), lk 297–326. https://www-tandfonline-com.ezproxy.utlib.ut.ee/doi/pdf/10.1080/13600869.2024.2324540 (24.04.2025).
7. Fletcher, R., Tzani, C., Ioannou, M. The dark side of Artificial Intelligence – Risks arising in dating applications. – Assessment & Development Matters 2024/16 (1),

lk 17–23. https://research-ebsco-com.ezproxy.utlib.ut.ee/c/qlurcm/viewer/html/byrcq5bju5 (24.04.2025).

8. Fragale, M., Grilli, V. Deepfake, Deep Trouble: The European AI Act and the Fight Against AI-Generated Misinformation. – Columbia Journal of European Law 11.11.2024. https://cjel.law.columbia.edu/preliminary-reference/2024/deepfake-deep-trouble-the-european-ai-act-and-the-fight-against-ai-generated-misinformation/ (24.04.2025).
9. Goldstein, J. A., Lohn, A. Deepfakes, Elections, and Shrinking the Liar's Dividend. – Brennan Center for Justice 23.01.2024. – https://www.brennancenter.org/our-work/research-reports/deepfakes-elections-and-shrinking-liars-dividend (23.03.2025).
10. Hancock, J. T., Bailenson, J. N. The Social Impact of Deepfakes. – Cyberpsychology, Behaviour, and Social Networking 2021/24 (3), lk 149–152. https://par.nsf.gov/servlets/purl/10233906 (23.03.2025).
11. Henry, N., Beard, G. Image-Based Sexual Abuse Perpetration: A Scoping Review. – TRAUMA, VIOLENCE, & ABUSE 2024/25 (5), lk 3981–3998. https://journals-sagepub-com.ezproxy.utlib.ut.ee/doi/pdf/10.1177/15248380241266137 (24.04.2025).
12. Kelleher, K. Revenge Porn and Deep Fake Technology: The Latest Iteration of Online Abuse. – Boston University School of Law 10.08.2023. https://sites.bu.edu/dome/2023/08/10/revenge-porn-and-deep-fake-technology-the-latest-iteration-of-online-abuse/ (15.04.2025).
13. Kinks, L. Loova tehisintellekti kasutamise võimalik mõju kujutava kunsti valdkonnale Eesti näitel. Magistritöö. Juhendaja Kadri Asmer. Tartu: Tartu Ülikool 2024. https://dspace.ut.ee/server/api/core/bitstreams/38937763-6937-4d75-a9b2-f43f67bc60aa/content (23.04.2025).
14. Łabuz, M. A Teleological Interpretation of the Definition of Deep Fakes in the EU Artificial Intelligence Act–A Purpose-Based Approach to Potential Problems With the Word "Existing". – Policy & Internet 2024/17 (1), lk 1–14. https://doi-org.ezproxy.utlib.ut.ee/10.1002/poi3.435 (24.04.2025).
15. Łabuz, M. Regulating Deep Fakes in the Artificial Intelligence Act. – Applied Cybersecurity & Internet Governance 2023/2 (1), lk 252–291. https://www.acigjournal.com/pdf-184302-105060?filename=Regulating%20Deep%20Fakes%20in.pdf (24.04.2025).

16. Le, Binh M., Kim, J., Woo, S. S., Moore, K., Abuadbba, A., Tariq, S. SoK: Systematization and Benchmarking of Deepfake Detectors in a Unified Framework. – arXiv 02.03.2025. https://arxiv.org/pdf/2401.04364 (16.04.2025).
17. Lovato, J., St-Onge, J., Harp, R., Lopez, G. S., Rogers, S. P., Haq, I. U., Hébert-Dufresne, L., Onaolapo, J. Diverse misinformation: impacts of human biases on detection of deepfakes on networks. – npj Complexity 2024/5, lk 1–13. https://www.nature.com/articles/s44260-024-00006-y (25.04.2025).
18. Masood, M., Nawaz, M., Malik, K. M., Javed, A., Irtaza, A. Deepfakes Generation and Detection: State-of-the-art, open challenges, countermeasures, and way forward. – arXiv 23.11.2021. https://arxiv.org/pdf/2103.00484 (25.04.2025).
19. McGlynn, C., et al. 'It's Torture for the Soul': The Harms of Image-Based Sexual Abuse. – Social & Legal Studies 2023/30 (4), lk 541–562. https://journals.sagepub.com/doi/pdf/10.1177/0964663920947791 (23.04.2025).
20. Nadal, D., Jančárik, P. Beyond the deepfake hype: AI, democracy, and "the Slovak case". – Harvard Kennedy School Misinformation Review 2024/5 (4), lk 1–9. https://misinforeview.hks.harvard.edu/article/beyond-the-deepfake-hype-ai-democracy-and-the-slovak-case/ (25.04.2025).
21. Nair. A. Real porn and pseudo porn: The regulatory road. – International Review of Law, Computers & Technology 2010/24 (3), lk 223–232. https://www-tandfonline-com.ezproxy.utlib.ut.ee/doi/epdf/10.1080/13600869.2010.523611 (21.04.2025).
22. Nimmo, M. Identiteedivarguse piiritlemine solvamisest ja laimamisest Eesti õigussüsteemis. – Juridica 2017/10, lk 710–717.
23. Nimmo, M. Karistusseadustiku § 157^2 probleeme Internetiga seotud identiteedivarguste kontekstis. – Juridica 2014/6, lk 464–473.
24. Phipps, B., Hadoux, X., Sheng, N., Campbell, J. P., Liu, T. Y. A., Keane, P. A., Cheung, C. Y., Chung, T. Y., Wijngaarden, P. AI image generation technology in ophthalmology: Use, misuse and future applications. – Progress in Retinal and Eye Research 2025/106, lk 1–24. https://www-sciencedirect-com.ezproxy.utlib.ut.ee/science/article/pii/S1350946225000266 (25.04.2025).
25. Rigotti, C., McGlynn, C. Towards an EU criminal law on violence against women: The ambitions and limitations of the Commission's proposal to criminalise image-based sexual abuse. – New Journal of European Criminal Law 2022/13 (4), lk 452–477. https://journals.sagepub.com/doi/epub/10.1177/20322844221140713 (23.03.2025).

26. Rigotti, C., McGlynn, C., Benning, F. Image-Based Sexual Abuse and EU Law: A Critical Analysis. German Law Journal 2024/25 (9), lk 1472–1493. https://www-cambridge-org.ezproxy.utlib.ut.ee/core/journals/german-law-journal/article/imagebased-sexual-abuse-and-eu-law-a-critical-analysis/B0CF334A0037DE3CA2067B79F506EB87 (25.04.2025).
27. Schiff, K. J., Schiff, D., Bueno, N. S. The Liar's Dividend: Can Politicians Claim Misinformation to Evade Accountability? – American Political Science Review 2025/119 (1), lk 71–90. https://isps.yale.edu/research/publications/isps24-07 (23.03.2025).
28. Smith, H., Mansted, K. Weaponised Deep Fakes. Weaponised Deep Fakes: National Security and Democracy. – Australian Strategic Policy Institute 2020, lk 11–14. https://www.jstor.org/stable/resrep25129.7?seq=1 (21.04.2025).
29. Sommer, E. Kuidas tõlgendada karistusseadustiku §-i 157.3? – Juridica 2018/8, lk 537–541.
30. Sootak, J., Pikamäe, P. Karistusseadustik. Komm vlj. 5. vlj. Tallinn: Juura 2021.
31. Vahkal, H. Infotehnoloogia ja digivormi kasutamise perspektiivid tõendamisel kriminaalmenetluses. Magistritöö. Juhendaja Mario Rosentau. Tartu: Tartu Ülikool 2022. https://dspace.ut.ee/server/api/core/bitstreams/c5b8ec07-46de-4bc8-847a-61a432a1bfd6/content (23.04.2025).
32. Varul, P., Kull, I., Kõve, V., Käerdi M., Sein, K. Võlaõigusseadus IV. Komm vlj. Tallinn: Juura 2020.
33. Westerlund, M. The Emergence of Deepfake Technology: A Review. – Technology Innovation Management Review 2019/9 (11), lk 39–52. https://timreview.ca/sites/default/files/article_PDF/TIMReview_November2019%20-%20D%20-%20Final.pdf (21.04.2025).

Kasutatud õigusaktid

34. 13. juuni 2024. aasta Euroopa Parlamendi ja nõukogu määrus (EL) 2024/1689, millega nähakse ette tehisintellekti käsitlevad ühtlustatud õigusnormid ning muudetakse määruseid (EÜ) nr 300/2008, (EL) nr 167/2013, (EL) nr 168/2013, (EL) 2018/858, (EL) 2018/1139 ja (EL) 2019/2144 ning direktiive 2014/90/EL, (EL) 2016/797 ja (EL) 2020/1828 (tehisintellekti käsitlev määrus). – ELT L, 2024/1689, 12.7.2024.

35. 14. mai 2024. aasta Euroopa Parlamendi ja nõukogu direktiiv (EL) 2024/1385, mis käsitleb naistevastase vägivalla ja perevägivalla tõkestamist. – ELT L, 2024/1385, 24.5.2024.
36. 19. oktoobri 2022. aasta Euroopa Parlamendi ja nõukogu määrus (EL) 2022/2065, mis käsitleb digiteenuste ühtset turgu ja millega muudetakse direktiivi 2000/31/EÜ (digiteenuste määrus). – ELT L 277, 27.10.2022, lk 1–102.
37. 27. aprilli 2016. aasta Euroopa Parlamendi ja nõukogu määrus (EL) 2016/679, millega kehtestatakse füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus). – ELT L 119, 4.5.2016, lk 1–88.
38. Eesti Vabariigi põhiseadus. – RT I, 15.05.2015, 2.
39. Euroopa Liidu põhiõiguste harta. – ELT C 202, 7.6.2016, lk 389–405.
40. Isikuandmete kaitse seadus. – RT I, 31.12.2024, 44.
41. Karistusseadustik. – RT I, 12.12.2024, 6.
42. Naistevastase vägivalla ja perevägivalla ennetamise ja tõkestamise Euroopa Nõukogu konventsioon. – RT II, 26.09.2017, 2.
43. Võlaõigusseadus. – RT I, 04.07.2024, 18.

Kasutatud kohtupraktika

44. RKKKo 18.12.2017, 1-17-689.
45. TlnRnKm 30.11.2021, 2-21-16615/19.
46. TlnRnKm 10.04.2024, 1-24-1954/4.
47. TlnRnKo 20.06.2017, 1-17-689/22.
48. TlnRnKo 11.10.2017, 1-15-11024/77.
49. TMKo 06.01.2023, 1-22-7937/36.

Muud allikad

50. 2023 State of Deepfakes. Realities, Threats, and Impact. – Security Hero 2023. https://www.securityhero.io/state-of-deepfakes/ (23.03.2025).

51. Aastaraamat 2024-2025. – Kaitsepolitseiamet 14.04.2025, lk 1–74. https://kapo.ee/sites/default/files/content_page_attachments/aastaraamat-2024-2025_0.pdf (21.04.2025).
52. Accelerated Capability Environment. Case Study. Innovating to detect deepfakes and protect the public. – GOV.UK 05.02.2025. https://www.gov.uk/government/case-studies/innovating-to-detect-deepfakes-and-protect-the-public (15.04.2025).
53. Ahmed, N., Haigh, A., Thomson, A., Harmsworth, E. Money scams: Deepfakes, AI will drive $10 trn in financial fraud, crime. – Business Standard 22.08.2023. https://www.business-standard.com/world-news/money-scams-deepfakes-ai-will-drive-10-trn-in-financial-fraud-crime-123082200083_1.html (23.03.2025).
54. AI CSAM REPORT UPDATE in conjunction with our Oct 23 report. What has changed in the AI CSAM landscape? Prompt: from fantasy to photo-realistic reality. – Internet Watch Foundation 07.2024, lk 1–28. https://www.iwf.org.uk/media/nadlcb1z/iwf-ai-csam-report_update-public-jul24v13.pdf (21.04.2025).
55. Ajder, H., Glick, J. Deepfakes, Satire, and the Politics of Synthetic Media. – Just Joking! The collaboration between Co-Creation Studio at MIT Open Documentary Lab and the human rights, video and technology network WITNESS 12.2021. https://cocreationstudio.mit.edu/just-joking/ (23.03.2025).
56. Ajder, H., Patrini, G., Cavalli, F., Cullen, C. The State of Deepfakes: Landscape, Threats, and Impact. – Deeptrace 09.2019, lk 1–21. https://regmedia.co.uk/2019/10/08/deepfake_report.pdf (23.03.2025).
57. Balarabe, T. Stable Diffusion Deepfakes: Creation and Detection. – Medium 10.12.2024. https://medium.com/@tahirbalarabe2/stable-diffusion-deepfakes-creation-and-detection-15103f99f55d (13.04.2025).
58. Berthier, V. As the investigation into a Slovak journalist Monika Tódová's "deepfake" is reopened, RSF is calling for this type of attack to be criminalised. – Reporters Without Borders 06.03.2024. https://rsf.org/en/investigation-slovak-journalist-monika-t%C3%B3dov%C3%A1-s-deepfake-reopened-rsf-calling-type-attack-be (25.04.2025).
59. Bjola, C. Algorithmic invasions: How information warfare threatens NATO's eastern flank. – Nato Review 07.02.2025. https://www.nato.int/docu/review/articles/2025/02/07/algorithmic-invasions-how-information-warfare-threatens-nato-s-eastern-flank/index.html (23.03.2025).
60. Bogdanov, D., Etti, P., Kamm, L., Ostrak, A., Stomakhin, F., Toomsalu, M., Valdma, S. H., Veldre, A. Tehisintellekti ja masinõppe tehnoloogia riskide ja nende leevendamise

võimaluste uuring. Aruanne. – Riigi Infosüsteemi Amet ja Cybernetica AS 27.02.2024, lk 1–111. https://www.ria.ee/sites/default/files/documents/2024-03/Tehisintellekti-masinoppe-tehnoloogia-riskide-uuring-2024.pdf (23.03.2025).

61. Brewster, T. Fraudsters Cloned Company Director's Voice In $35 Million Heist, Police Find. – Forbes 02.05.2023. https://www.forbes.com/sites/thomasbrewster/2021/10/14/huge-bank-fraud-uses-deep-fake-voice-tech-to-steal-millions/ (22.04.2025).
62. Briefing Paper: Deepfake Image-Based Sexual Abuse, Tech-Facilitated Sexual Exploitation and the Law. – Equality Now 17.01.2024, lk 1–9. https://audri.org/wp-content/uploads/2024/01/EN-AUDRi-Briefing-paper-deepfake-06.pdf (23.03.2025).
63. Bristow, T. Keir Starmer suffers UK politics' first deepfake moment. It won't be the last. – Politico 09.10.2023. https://www.politico.eu/article/uk-keir-starmer-labour-party-deepfake-ai-politics-elections/ (23.03.2025).
64. Browne, J., Moloney, M. What's a FLOP? How the AI Act Regulates General Purpose AI Systems. CEDPO AI and Data Working Group Micro-Insights Series March 2024. – Confederation of European Data Protection Agencies 03.2024, lk 1–7. https://cedpo.eu/wp-content/uploads/How-General-Purpose-AI-Models-are-regulated-under-the-AI.pdf (24.04.2025).
65. Bueermann. G., Perucica, N. How can we combat the worrying rise in the use of deepfakes in cybercrime? – World Economic Forum 19.05.2023. https://www.weforum.org/stories/2023/05/how-can-we-combat-the-worrying-rise-in-deepfake-content/ (23.03.2025).
66. Byman, D. L., Gao, C., Meserole, C., Subrahmanian, V. S. Deepfakes and International Conflict. – Foreign Policy at BROOKINGS 02.2023, lk 1–21. https://www.brookings.edu/wp-content/uploads/2023/01/FP_20230105_deepfakes_international_conflict.pdf (23.03.2025).
67. Cole, S. Reddit Just Shut Down the Deepfakes Subreddit. – Vice 07.02.2018. https://www.vice.com/en/article/reddit-shuts-down-deepfakes/ (14.04.2025).
68. Conrad, L. Can deepfake technology be used for good? – Launched Tech News 31.05.2019. https://tbtech.co/news/can-deepfake-technology-be-used-for-good/ (25.04.2025).
69. Contreras, B. Tougher AI Policies Could Protect Taylor Swift–And Everyone Else–From Deepfakes. – Scientific American 26.01.2024.

https://www.scientificamerican.com/article/tougher-ai-policies-could-protect-taylor-swift-and-everyone-else-from-deepfakes/ (23.03.2025).

70. Crawford, A., Smith, T. Illegal trade in AI child sex abuse images exposed. – BBC News 28.06.2023. https://www.bbc.com/news/uk-65932372 (23.03.2025).
71. Cybersecurity Information Sheet. Contextualising Deepfake Threats to Organizations. – National Security Agency, Federal Bureau of Investigation, Cybersecurity and Infrastructure Security Agency 12.09.2023, lk 1–18. https://media.defense.gov/2023/Sep/12/2003298925/-1/-1/0/CSI-DEEPFAKE-THREATS.PDF (21.04.2025).
72. Deep-Fake Audio and Video Links Make Robocalls and Scam Texts Harder to Spot. – Federal Communications Commission 08.06.2024. https://www.fcc.gov/consumers/guides/deep-fake-audio-and-video-links-make-robocalls-and-scam-texts-harder-spot (25.04.2025).
73. Deepfake Technology: A Brief History Worth Knowing. – European Identity Theft Observatory System 15.05.2024. https://eithos.eu/deepfake-technology-1-history-useful-to-know/ (23.03.2025).
74. Deepfake Trends 2024. – Regula 2024, lk 1–44. https://static-content.regulaforensics.com/PDF-files/0831-Regula-Deepfake-Research-Report-Final-version.pdf? (22.04.2025).
75. Deepfakes in the Financial Sector: Understanding the Threats, Managing the Risks. A Report by the FS-ISAC Artificial Intelligence Risk Working Group. – Financial Services Information Sharing and Analysis Center 10.2024, lk 1–16. https://www.fsisac.com/hubfs/Knowledge/AI/DeepfakesInTheFinancialSector-UnderstandingTheThreatsManagingTheRisks.pdf? (22.04.2025).
76. Devine, C., O'Sullivan, D., Lyngaas, S. A fake recording of a candidate saying he'd rigged the election went viral. Experts say it's only the beginning. – CNN Politics 01.02.2024. https://edition.cnn.com/2024/02/01/politics/election-deepfake-threats-invs/index.html (25.04.2025).
77. Dunn, S. Women, Not Politicians, Are Targeted Most Often by Deepfake Videos. – Centre for International Governance Innovation 03.03.2021. https://www.cigionline.org/articles/women-not-politicians-are-targeted-most-often-deepfake-videos/ (23.03.2025).
78. Eitren, W. Deep fakes in the AI act. – Schjødt 07.11.2024. https://schjodt.com/news/deep-fakes-in-the-ai-act (23.03.2025).

79. EU Digital Strategy. – EU4Digital. https://eufordigital.eu/discover-eu/eu-digital-strategy/ (23.03.2025).
80. Europe's Digital Decade. – Euroopa Komisjon 12.03.2025. https://digital-strategy.ec.europa.eu/en/policies/europes-digital-decade (23.03.2025).
81. Graham, M. M. Deepfakes: Federal and state regulation aims to curb a growing threat. – Thomson Reuters 26.06.2024. https://www.thomsonreuters.com/en-us/posts/government/deepfakes-federal-state-regulation/ (23.03.2025).
82. Holroyd, M., Olorunselu, F. Deepfake Zelenskyy surrender video is the 'first intentionally used' in Ukraine war. – Euro News 16.03.2022. https://www.euronews.com/my-europe/2022/03/16/deepfake-zelenskyy-surrender-video-is-the-first-intentionally-used-in-ukraine-war (23.03.2025).
83. How AI is being abused to create child sexual abuse imagery. Prompt: from fantasy to photo-realistic reality. – Internet Watch Foundation 10.2023, lk 27. https://www.iwf.org.uk/media/q4zll2ya/iwf-ai-csam-report_public-oct23v1.pdf (21.04.2025).
84. How Stalin's propaganda machine erased people from photographs, 1922-1953. – Rare Historical Photos 07.12.2021. https://rarehistoricalphotos.com/stalin-photo-manipulation-1922-1953/ (21.04.2025).
85. Jõerand, R. DIGITAALNE ÕUDUS LEVIB! Süvavõltsitud alastifotod tekitavad ohvrites paanikahooge. – Õhtuleht 10.03.2025. https://www.ohtuleht.ee/1126142/digitaalne-oudus-levib-suvavoltsitud-alastifotod-tekitavad-ohvrites-paanikahooge? (23.03.2025).
86. Karistusseadustiku muutmise ja sellega seonduvalt teiste seaduste muutmise seaduse seletuskiri. 385 SE I. § 157.3. – https://www.riigikogu.ee/tegevus/eelnoud/eelnou/f9a7291c-8c46-4ad8-a740-4e1c55c83964/ (23.04.2025).
87. Karistusseadustiku muutmise ja sellega seonduvalt teiste seaduste muutmise seaduse seletuskiri. 385 SE I. § 157.3. – https://www.riigikogu.ee/tegevus/eelnoud/eelnou/f9a7291c-8c46-4ad8-a740-4e1c55c83964/ (23.04.2025).
88. Karistusseadustiku muutmise seaduse eelnõu seletuskiri. 530 SE, § 157.2. – https://www.riigikogu.ee/tegevus/eelnoud/eelnou/2b386832-b657-ab0c-fb52-de02708302bc/Karistusseadustiku%20muutmise%20seadus/ (23.04.2025).

89. Kõiv, O., Ilves, M. Juristid hoiatavad: tehisaru avab küberkiusajatele uued horisondid. Üha enam asetatakse tüdrukute nägusid pornovideosse. – Eesti Päevaleht 04.11.2023. https://epl.delfi.ee/artikkel/120244858/juristid-hoiatavad-tehisaru-avab-kuberkiusajatele-uued-horisondid-uha-enam-asetatakse-tudrukute-nagusid-pornovideosse (23.03.2025).
90. Leffer, L. AI Audio Deepfakes Are Quickly Outpacing Detection. – Scientific American 26.01.2024. https://www.scientificamerican.com/article/ai-audio-deepfakes-are-quickly-outpacing-detection/ (23.03.2025).
91. Llach, L. Naked deepfake images of teenage girls shock Spanish town: But is it an AI crime? – Euro News 24.09.2023. https://www.euronews.com/next/2023/09/24/spanish-teens-received-deepfake-ai-nudes-of-themselves-but-is-it-a-crime (23.03.2025).
92. Mengesha, S., Diaz, A., Dunn, K. Protecting Against Sexual Violence Linked to Deepfake Technology. – The Regulatory Review 13.04.2024. https://www.theregreview.org/2024/04/13/protecting-against-sexual-violence-linked-to-deepfake-technology/ (23.03.2025).
93. Metz, R. How a deepfake Tom Cruise on TikTok turned into a very real AI company. – CNN Business 06.08.2021. https://edition.cnn.com/2021/08/06/tech/tom-cruise-deepfake-tiktok-company (23.03.2025).
94. Milmo, D. UK engineering firm Arup falls victim to £20m deepfake scam. – The Guardian. https://www.theguardian.com/technology/article/2024/may/17/uk-engineering-arup-deepfake-scam-hong-kong-ai-video (22.04.2025).
95. Morgan, S. Cybercrime Facts and Statistics. 2021 REPORT: CYBERWARFARE IN THE C-SUITE. CYBERSECURITY VENTURES 21.01.2021, lk 1–19. https://cybersecurityventures.com/wp-content/uploads/2021/01/Cyberwarfare-2021-Report.pdf (22.04.2025).
96. Nearly two-thirds of women worry about being a victim of deepfake pornography, ESET UK Research reveals. – ESET 20.03.2024. https://www.eset.com/uk/about/newsroom/press-releases/nearly-two-thirds-of-women-worry-about-being-a-victim-of-deepfake-pornography-eset-uk-research-reveals/ (23.03.2025).
97. Prokuratuuri aastaraamat 2024. Küberkuritegevus. – Prokuratuur 2024. https://aastaraamat.prokuratuur.ee/prokuratuuri-aastaraamat-2024/kuberkuritegevus (24.04.2025).

98. Sancho, D., Ciancaglini V. Surging Hype An Update on the Rising Abuse of GenAI. – Trend Micro 30.07.2024. https://www.trendmicro.com/vinfo/es/security/news/cybercrime-and-digital-threats/surging-hype-an-update-on-the-rising-abuse-of-genai (22.04.2025).
99. Silva de Alwis, R., Vialle, E. Is AI-Facilitated Gender-Based Violence the Next Pandemic? – The Regulatory Review 06.05.2024. https://www.theregreview.org/2024/05/06/de-silva-de-alwis-vialle-is-ai-facilitated-gender-based-violence-the-next-pandemic/ (23.03.2025).
100. Silverman, C. How To Spot A Deepfake Like The Barack Obama–Jordan Peele Video. – BuzzFeed 17.04.2018. https://www.buzzfeed.com/craigsilverman/obama-jordan-peele-deepfake-video-debunk-buzzfeed (23.03.2025).
101. Solberg, M. Q1 2025 Deepfake Incident Report: Mapping Deepfake Incidents. – Resemble.AI 04.2025, lk 1–20. https://www.resemble.ai/wp-content/uploads/2025/04/ResembleAI-Q1-Deepfake-Threats.pdf (22.04.2025).
102. Somers, M. Deepfakes, explained. – MIT Management 21.07.2020. https://mitsloan.mit.edu/ideas-made-to-matter/deepfakes-explained (23.03.2025).
103. Spain: Court punishes schoolboys for spreading AI deepfakes of girls. Scottish Legal News 10.07.2024. https://www.scottishlegal.com/articles/spain-court-punishes-schoolboys-for-spreading-ai-deepfakes-of-girls (21.04.2025).
104. Supervision of the designated very large online platforms and search engines under DSA. – Euroopa Komisjon 06.02.2025. https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses (25.04.2025).
105. Swatton, P., Leblanc, M. What are deepfakes and how can we detect them? The science behind the tech that's transforming the online world. – The Alan Turing Institute 07.06.2024. https://www.turing.ac.uk/blog/what-are-deepfakes-and-how-can-we-detect-them (23.03.2025).
106. Zainul, E. No prosecution – Ag. – The Edge Malaysia 10.01.2020. https://theedgemalaysia.com/article/no-prosecution-%E2%80%94-ag (21.04.2025).
107. Tampuu, A. Piltide genereerimine. Tehisintellekti Algkursus 2019/20. – Tartu Ülikool. Arvutiteaduse instituut. https://courses.cs.ut.ee/2020/Tehisintellekti_algkursus/Main/PARTIIIGen (23.03.2025).

108. The Convention on Cybercrime (Budapest Convention, ETS No. 185) and its Protocols. – Euroopa Nõukogu. https://www.coe.int/en/web/cybercrime/the-budapest-convention (24.04.2025).

109. Vilenkin, R. How De-aging Technology is Changing Hollywood & the Future of Film-making. – Respeecher 27.01.2021. https://www.respeecher.com/blog/de-aging-technology-changing-hollywood-future-film-making (23.03.2025).

110. Williamson, E. Q&A: With Zelenskyy Surrender Hoax, the Feared Future of Deepfakes Is Here. – UVA Today 17.03.2022. https://news.virginia.edu/content/qa-zelenskyy-surrender-hoax-feared-future-deepfakes-here (23.03.2025).