



RIIGIKOGU KANTSELEI ÕIGUS- JA ANALÜÜSIOSAKOND

Süvavõltsingud ja demokraatlik infokeskkond

Nr 6

06.04.2026

Teemaleht annab ülevaate süvavõltsingutest, keskendudes nende tähendusele, peamistele riskidele ning mõjule avalikule arutelule, poliitikale ja demokraatlikule infokeskkonnale. Samuti vaadeldakse riikide kogemusi, Eesti ja Euroopa Liidu regulatiivset raamistikku ning võimalusi, kuidas süvavõltsingutega seotud riske vähendada teadlikkuse, tehniliste lahenduste ja institutsionaalse valmisoleku abil.

Mida tähendab süvavõltsing ja miks see teema on oluline?

Süvavõltsing ehk *deepfake* on tehisintellekti abil loodud või manipuleeritud audiovisuaalne sisu, mis võib näida vaatajale ehtsa ja usutavana. Sisuliselt on tegemist pildi, heli või videoga, milles inimesele omistatakse sõnu või tegusid, mida ta tegelikult ei öelnud ega teinud (Kindsiko, 2023). Süvavõltsingud on olulised seetõttu, et need ei ähmasta üksnes piiri tõese ja vale vahel, vaid võivad kahjustada inimeste mainet, suurendada pettuste hulka, mõjutada kohtumenetlusi ning õonestada usaldust avaliku teabe, meedia ja demokraatlike institutsioonide vastu (Past, 2025; Rosin, 2019).

Süvavõltsingud ei piirdu enam ammu üksnes meelelahutusliku sisuga. Varasemad tuntud näited sotsiaalmeedias tõid hästi esile, kui veenvalt saab avaliku elu tegelase nägu ja häält järele teha. Süvavõltsinguid on kasutatud ka pornograafilise sisu loomisel, identiteedipettustes ja küberkiusamises. Risk ei puuduta enam üksnes kuulsusi. Inimesed jätavad endast sotsiaalmeediasse suure digijälje ja nii saab võltsinguid üha lihtsamini luua ka tavakasutajate kohta. Eriti haavatavad võivad olla noored, kelle identiteet kujuneb suurel määral sotsiaalmeedia keskkonnas ning kelle jaoks võrgu- ja pärismaailm on tihedalt põimunud (Kindsiko, 2023).

Lisaks üksikisiku kahjustamisele on süvavõltsingud muutunud laiemaks ühiskondlikuks ja julgeolekuliseks probleemiks. Past (2025) on Riigikogu Toimetistes märkinud, et tehisintellekti abil loodud süvavõltsingud ja nn odavvõltsingud¹ muudavad ehtsa ja manipuleeritud sisu eristamise järjest raskemaks ning loovad koos ühiskondlike vastasseisude, suunatud mõjutamise ja väheneva usaldusega soodsa pinnase valeinfo levikuks. Seetõttu ei ole süvavõltsingud ainult tehnoloogiline, vaid ka demokraatia, avaliku arutelu ja ühiskondliku vastupanuvõime küsimus.

Süvavõltsingud poliitikas ja parlamentides

Austria parlamendi 2026. aastal ECPRD² koostöövõrgustiku kaudu parlamendiliikmeid kujutavate süvavõltsingute kohta läbiviidud küsitlusest selgus, et see teema ei ole enam pelgalt teoreetiline risk. Enamik 34-st vastanud parlamendist märkis, et nad on sellistest juhtumitest teadlikud ning neid on viimastel aastatel ette tulnud rohkem. Riikide reaktsioonid on olnud erinevad. Mõnes

¹ Odavvõltsing (ingl *cheapfake* või *shallowfake*) on eksitav või manipuleeritud meediasisu, mis põhineb pigem olemasoleva materjali osalisel moonutamisel, valikulisel esitamisel või „osalistest tõdedest väikeste valedeni” loogikal kui keerukal tehisintellektil (University of Maryland, 2024). <https://cmns.umd.edu/news-events/news/Nirupam-Roy-fighting-deepfakes-shallowfakes-and-media-manipulation>

² ECPRD – European Centre for Parliamentary Research and Documentation on 1977. aastal loodud Euroopa parlamentide koostöövõrgustik.

parlamendis on teemat arutatud juhatuses või komisjonides, mõnes on piiratud üldiste juhiste ja nõuannetega, mõnes on aga kaalutud õiguslikke või tehnilisi lisameetmeid. Näiteks on Taanis pornograafiliste süvavõltsingute osas muudetud kriminaalõigust ning Lätis arutatud muudatusi, mille eesmärk on kaitsta valimiste ausust ja avalikku teenistusse nimetamise usaldusväärsust. Ühendkuningriigis on tehtud ettepanek tugevdada kandidaatide kohta levitatavate valeväidete regulatsiooni. Iirimaal vaadatakse C2PA-l³ põhinevate lahenduste rakendamist osana laiemast algatusest, mille eesmärk on tugevdada autentsust ja vastupanu manipuleeritud sisule. See hõlmab päritoluteabe lisamist näiteks pildi- ja videosisule. Šveitsis on parlamendiliikmetele pakutud välise nõustaja abi ning õigusabikulude kindlustust.

Eestis on see probleem seni olnud vähem nähtav. Avalikult ei ole dokumenteeritud juhtumeid, kus sotsiaalmeedias või internetis oleks laiemalt levinud otseselt Riigikogu liikmete vastu suunatud süvavõltsitud videod. Küll aga on Eesti meedias kajastatud vähemalt üht väidetavat *deepfake*'i juhtumit, mis puudutas Riigikogu väliskomisjoni (Kärmas, 2021). Samas on Eestis esinenud juhtumeid, kus avaliku elu tegelaste, sealhulgas poliitikute nimesid ja pilte on kasutatud petuskeemides, eeskätt investeerimis- ja reklaamipettustes. Eraldi süvavõltsingute tõkestamiseks mõeldud meetmeid ei ole seni kasutusele võetud. Selle asemel on piiratud pigem toetavate sammudega, nagu koostöö Riigi Infosüsteemi Ametiga (RIA) küberturvalisuse ja väärinfo küsimustes, infoturbejuhiste jagamine ning ametlike videote avaldamine kontrollitud kanalites.

Regulatiivne raamistik Eestis ja Euroopas

Eestis puudub eraldi süvavõltsingute loomise ja kasutamise õiguslik regulatsioon, kuid teatud juhtudel võivad sellele rakenduda teiste õigusaktidega kehtestatud normid (näiteks karistusseadustiku § 157², mis käsitleb teise isiku identiteedi ebaseaduslikku kasutamist). Teistes riikides on pilt üldjoontes sarnane. Norra parlamendi 2024. aastal koostatud ECPRD süvavõltsingute reguleerimise kohta läbiviidud küsitluse järgi puudus enamikus vastanud riikides⁴ vastav eriseadus, kuid seda reguleerisid muud õigusnormid, näiteks karistusõigus, andmekaitse ja isikuõiguste kaitse.

Oluline muutus on toimunud Euroopa Liidu tasandil. Süvavõltsingute käsitlemisel on keskne roll vähemalt kolmel ELi õigusaktil. Esiteks näeb tehisintellekti käsitlev määrus ehk *AI Act* ette läbipaistvuskohustused manipuleeritud heli-, pildi- ja videosisu puhul, st kasutajale tuleb teatavaks teha, kui tegemist ei ole autentse sisuga (määrus (EL) 2024/1689, 2024)⁵. Teiseks paneb digiteenuste määrus ehk DSA väga suurtele veebiplatvormidele ja otsingumootoritele kohustuse hinnata süsteemseid riske, võtta kasutusele maandamismeetmeid ja suurendada läbipaistvust, sealhulgas olukorras, kus manipuleeritud sisu võib mõjutada avalikku arutelu või demokraatlikke protsesse (määrus (EL) 2022/2065, 2022)⁶. Kolmandaks on valimiste usaldusväärsuse seisukohalt oluline poliitilise reklaami läbipaistvuse määrus, mille eesmärk on vähendada info manipuleerimist ja välismõju riske valimiste ajal (määrus (EL) 2024/900, 2024)⁷. Valimiste usaldusväärsuse seisukohalt väärib märkimist ka komisjoni soovitus, kus juhitakse tähelepanu vajadusele tugevdada valimisprotsesside vastupanuvõimet ka digitaalses informumis (komisjoni

³ C2PA – Coalition for Content Provenance and Authenticity on avatud tehniliste spetsifikatsioonide raamistik, mille eesmärk on võimaldada digitaalsele sisule lisada päritolu- ja muutmisandmeid, et oleks paremini näha, kust sisu pärineb ja kuidas seda on muudetud. <https://c2pa.org/about/>

⁴ Küsitlusele vastasid Eesti, Kanada, Rootsi, Saksamaa, Soome ja Taani.

⁵ 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, 12.7.2024. https://eur-lex.europa.eu/legal-content/ET/TXT/PDF/?uri=OJ:L_202401689

⁶ Euroopa Parlamendi ja nõukogu määrus (EL) 2022/2065, 19. oktoober 2022, mis käsitleb digiteenuste ühtset turgu ja millega muudetakse direktiivi 2000/31/EÜ (digiteenuste määrus), ELT L 277, 27.10.2022. <https://eur-lex.europa.eu/legal-content/ET/TXT/PDF/?uri=CELEX:32022R2065>

⁷ Euroopa Parlamendi ja nõukogu määrus (EL) 2024/900, 13. märts 2024, poliitreklaami läbipaistvuse ja suunamise kohta, ELT L, 20.3.2024. https://eur-lex.europa.eu/legal-content/ET/TXT/PDF/?uri=OJ:L_202400900

soovitus (EL) 2023/2829, 2023)⁸. Eestis on nende regulatsioonide rakendamise ja järelevalvega seotud eeskätt Tarbijakaitse ja Tehnilise Järelevalve Amet ning isikuandmete küsimustes Andmekaitse Inspektsioon.

Kuidas end süvavõltsingute eest kaitsta?

Süvavõltsingute vastu ei ole ühtainsat universaalset kaitsemeedet. Esimene ja kõige olulisem kaitseliin on allikakriitika. Kaju (2025) rõhutab Riigikogu Toimetistes, et allikakriitika peab muutuma igapäevaseks oskuseks. Hinnata tuleb autorit, avaldamiskonteksti, levitamiskanalit, eesmärki ja emotsionaalset tooni. Sama kehtib ka audiovisuaalse sisu puhul. Kui video või helisalvestis tekitab tugeva emotsiooni või näib poliitiliselt plahvatuslik, ei tohiks seda pidada automaatselt tõendiks. Eesti õigusosalases käsitluses on juba osutatud, et süvavõltsingute teke mõjutab ka kohtute ja avalikkuse suhtumist heli- ja videosalvestiste usaldusväärsusse ning et teadlikkus võimaldab võltsimise riskiga arvestada (Rosin, 2019).

Teine kaitseliin on tehniline ja institutsionaalne. Ametlikke videoid ja avalikke pöördumisi tuleks avaldada ainult kontrollitud kanalites ning võimalusel lisada neile päritolu või autentsust kinnitavad tehnilised markerid. Rahvusvahelisest võrdlusest selgus, et mõnes riigis kaalutakse või vaadatakse üle ka tehnilisi lahendusi, mis aitaksid tugevdada sisu autentsuse tõendamist ja vähendada manipuleeritud sisu mõju, sealhulgas C2PA-l põhinevaid lahendusi. Eestis on seni tuginetud ametlike videote avaldamisele kontrollitud kanalites, infoturbejuhiste jagamisele ning koostööle RIA-ga. See pakub küll teatud esmase kaitse, kuid eraldi süvavõltsingute tõkestamise süsteemi ei ole kasutusele võetud.

Kindsiko (2023) rõhutab, et ainuüksi süvavõltsingute teema teadvustamine on juba oluline samm. Sama kehtib ka avaliku sektori, poliitikute ja ajakirjanike puhul. Mida rohkem on ühiskonnas teadmisi sellest, kuidas süvavõltsinguid luuakse, milliseid mustreid need kasutavad ja millistes kanalites need levivad, seda väiksem on nende vahetu mõju. Seetõttu on meediapädevus, digihügieen ja kriitiline mõtlemine mitte üksnes hariduslikud eesmärgid, vaid ka osa riigi infosõltumatusest ja julgeolekust (Kaju, 2025; Past, 2025).

Kokkuvõte

Süvavõltsingud on kiiresti arenev nähtus, mis ühendab endas tehnoloogilise innovatsiooni, identiteediriskid, pettused, mainekahju, desinformatsiooni ja demokraatliku usalduse nõrgenemise ohu. Eesti praktikas on avalikult kajastatud vähemalt üks väidetav juhtum, kus süvavõltsingu või sarnase videomanipulatsiooni abil püüti mõjutada avaliku võimu kandjaid või institutsioone. Samuti näitab poliitikute nimede ja piltide kasutamine pettustes, et see risk on olemas. Euroopa tasandil on õiguslik raamistik viimastel aastatel tugevnenud, kuid paljud riigid alles otsivad sobivat tasakaalu õiguslike meetmete, platvormivastutuse ja teadlikkuse tõstmise vahel.

Eestis võiks edasiseks kaaluda vähemalt nelja sammu: esiteks ametliku audiovisuaalse sisu autentsuskinnituse tugevdamist; teiseks kiire reageerimise korra loomist avaliku elu tegelasi puudutavate süvavõltsingute puhuks; kolmandaks süvavõltsingute ja odavvõltsingute teema sidumist süsteemsemalt meediapädevuse, valimiste usaldusväärsuse ja infosõltumatuse poliitikatega; ning neljandaks selgemat õiguslikku analüüsi selle kohta, kas ja millal on olemasolevad Eesti normid piisavad ning millal oleks vaja täiendavaid meetmeid. Mitmes riigis liigutakse tehnilise autentsuse, teadlikkuse tõstmise ja kitsamalt sihitud õigusmuudatuste kombinatsiooni suunas.

Kaur Kõtsi
nõunik
kaur.kotsi@riigikogu.ee

⁸ Komisjoni soovitus (EL) 2023/2829, 12. detsember 2023, kaasavate ja probleemikindlate valimisprotsesside kohta liidus ning Euroopa Parlamendi valimiste Euroopa mõõtme ja tõhusa läbiviimise kohta, ELT L, 20.12.2023. https://eur-lex.europa.eu/legal-content/ET/TXT/PDF/?uri=OJ:L_202302829

Kasutatud allikad

- Euroopa Parlamendi ja nõukogu määrus (EL) 2022/2065, 19. oktoober 2022, mis käsitleb digiteenuste ühtset turgu ja millega muudetakse direktiivi 2000/31/EÜ (digiteenuste määrus), ELT L 277, 27.10.2022.
<https://eur-lex.europa.eu/legal-content/ET/TXT/PDF/?uri=CELEX:32022R2065>
- Euroopa Parlamendi ja nõukogu määrus (EL) 2024/900, 13. märts 2024, poliitreklaami läbipaistvuse ja suunamise kohta, ELT L, 20.3.2024.
https://eur-lex.europa.eu/legal-content/ET/TXT/PDF/?uri=OJ:L_202400900
- 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, 12.7.2024.
https://eur-lex.europa.eu/legal-content/ET/TXT/PDF/?uri=OJ:L_202401689
- Kaju, K. (2025). Allikakriitilisuse põhimõtted meie igapäevasteks oskusteks. Riigikogu Toimetised, 51, 67-70.
<https://rito.riigikogu.ee/wordpress/wp-content/uploads/2025/06/RiTo-51.pdf>
- Kindsiko, E. (2023, 28. veebruar). Deepfake ehk süvavõltsingud. Mihus.
<https://mihus.mitteformaalne.ee/deepfake-ehk-suvavoltsingud/>
- Komisjoni soovitus (EL) 2023/2829, 12. detsember 2023, kaasavate ja probleemikindlate valimisprotsesside kohta liidus ning Euroopa Parlamendi valimiste Euroopa mõõtme ja tõhusa läbiviimise kohta, ELT L, 20.12.2023.
https://eur-lex.europa.eu/legal-content/ET/TXT/PDF/?uri=OJ:L_202302829
- Kärmas, M. (2021, 8. september). Deepfake'id panevad julgeolekuspetsialiste aina rohkem muretsema. ERR. <https://www.err.ee/1608332183/deepfake-id-panevad-julgeolekuspetsialiste-aina-rohkem-muretsema>
- Past, L. (2025). Kas EL suudab ohjeldada infokaost ja manipuleerimist ühismeedias? Riigikogu Toimetised, 51, 51-58.
<https://rito.riigikogu.ee/wordpress/wp-content/uploads/2025/06/RiTo-51.pdf>
- Rosin, J. (2019, 29. november). „Huvitaja”: Deepfake näitab inimesi tegemas asju, mida nad tegelikult teinud pole. ERR. <https://www.err.ee/1008786/huvitaja-deepfake-naitab-inimesi-tegemas-asju-mida-nad-tegelikult-teinud-pole>
- University of Maryland. (2024, January 29). Fighting deepfakes, shallowfakes and media manipulation. College of Computer, Mathematical, and Natural Sciences.
<https://cmns.umd.edu/news-events/news/Nirupam-Roy-fighting-deepfakes-shallowfakes-and-media-manipulation>