

TARTU ÜLIKOOL
ÕIGUSTEADUSKOND
Avaliku õiguse osakond

Saara Arianne Avestik

TEHISINTELLEKTIGA SEOTUD TUMEDATE MUSTRITE
REGULEERIMINE VÕIMETEPÕHISE MUDELI ABIL

Magistritöö

Juhendaja
Dr iuris Mario Rosentau

Tartu
2026

SISUKORD

SISSEJUHATUS	4
1. TUMEDATE MUSTRITE ARENG JA ALUSED	9
1.1. Areng	9
1.2. Kasutatavad terminid	15
1.2.1. Tehisintellekt	15
1.2.2. Käitumisökonomika	16
1.2.3. Digitaalne asümmeetria	16
1.2.4. Tehnilised terminid	16
1.3. Tumede mustrite mõiste defineerimise keerukus	17
1.5. Levinud tumedad mustrid	20
1.5.1. Võrdluse ärahoidmine	20
1.5.2. Kinnitushäbistamine	20
1.5.3. Peidetud reklaam	20
1.5.4. Võlts nappus	21
1.5.5. Võlts sotsiaaltunnustus	21
1.5.6. Võlts pakilisus	22
1.5.7. Sunnitud tegevus	22
1.5.8. Keerukas tühistamine	23
1.5.9. Peidetud kulud	23
1.5.10. Peidetud tellimus	23
1.5.11. Näägutamine	24
1.5.12. Takistus	24
1.5.13. Eelvalimine	24
1.5.14. Hiilimine	24
1.5.15. Eksitav sõnastus	25
1.5.16. Visuaalne takistus	25
1.6. Tumede mustrite liigitamine	25
2. ÜLEVAADE TUMEDATE MUSTRITE KÄSITLUSEST EUROOPA LIIDU ÕIGUSES	28
2.1. E-privatsuse direktiiv	29
2.2. Ebaausate kaubandustavade direktiiv	31
2.3. Tarbija õiguste direktiiv	34
2.4. Isikuandmete kaitse üldmäärus	37
2.5. Digiteenuste määrus	38
2.6. Digiturgude määrus	41
2.7. Andmemäärus	42
2.8. Tehisintellekti käsitlev määrus	43
2.8.1. Tumede mustrite käsitus tehisintellekti määruses	44
2.8.2. Riskipõhine lähenemine tehisintellekti käsitlevas määruses	47

3. TEHISINTELLEKTI VÕIMETE PÕHINE TUMEDATE MUSTRITE KÄSITLUS	50
3.1. Kitsa tehisintellekti võimed, mis võimaldavad või võimendavad tumedate mustrite kasutust.	52
3.1.1. Profileerimine.	52
3.1.2. Personaliseerimine.	52
3.1.3. Pidev arenemise-ja kohanemisvõime.	52
3.1.5. Paralleelsete kasutajakogemuste testimisvõime.	53
3.2. Väljapakutav mudel	53
3.3. Võrdlus olemasoleva seadusandluse kitsaskohtadega.	56
KOKKUVÕTE	58
CAPABILITY BASED REGULATORY MODEL OF DARK DESIGN PATTERNS RELATED TO ARTIFICIAL INTELLIGENCE	61
Kasutatud kirjandus	66

SISSEJUHATUS

Digitaalses keskkonnas pole midagi looduslikku või juhuslikku. Kõik, mis veebilehe külastaja arvutiekraanile kuvatakse, on tema jaoks disainitud. Ripikmenüüde paigutus, nuppude või teksti värviskeemid, kasutaja eest ära märgitud ruudukesed – see kõik võib alateadvuslikult või ka tajutavalt mõjutada kasutaja käitumist ja valikuid veebilehel. Kui selliseid kallutavaid disainivõtteid kasutatakse, et õõnestada veebilehe külastaja autonoomiat või manipuleerida teda tegema valikuid, mis pole tema parimates huvides, kutsutakse neid võtteid tumedateks mustriteks.

Tumedaid mustreid kui selliseid digitaalses kontekstis kirjeldas esimesena kasutajakogemuse disainer Harry Brignull, kes 2010. aasta augustis lõi veebilehe¹, kus arhiveeris, loetles ja liigitas neid manipuleerivaid võtteid ja nendega seotud kohtuasju, artikleid ja seadusakte, et probleemile tähelepanu juhtida. Nüüdseks on möödunud peaaegu viisteist aastat tumedate mustrite esmakordsest kirjeldamisest. Selle perioodi jooksul on leidnud aset kolm “lainet” tumedate mustrite alases teadustöös. Esimese lainena üritati tumedaid mustreid kui uusi digiplatvormidega kaasnevaid nähtusi liigitada. Seejärel uuriti nende levikut ja esinemissagedust erinevatel veebilehtedel ning viimaks asuti empiriiliselt hindama, kuidas mõjuvad need mustrid tarbijatele.² Selle aja jooksul on tumedatest mustritest saanud märkimisväärne ja kinnistunud oht digikeskkonnas, mida on uuritud ja arutatud nii käitumisökonomilises kui ka õiguslikus võtmes.

Probleemi levik süvenes ülemaailmse COVID-19 pandeemia ajal, mil paljud inimesed olid kodus viibimise tõttu sunnitud töötama, oste sooritama ja meelelahutust leidma digikeskkonna erinevate võimaluste kaudu. Euroopa Komisjon avaldas 2020. aastal uue tarbijakaitse tegevuskava, mille eesmärgiks oli tarbijate toimetulekuvõime parandamine ja seeläbi majanduse kestliku taastumise edendamine peale pandeemiat.³ Tegevuskava raames kajastati ka tumedate mustrite probleemi ning kirjeldati neid kui kaubandustavasid, “millega eiratakse tarbijate õigust teha teadlikke valikuid, kuritarvitatakse nende käitumislake eelarvamusi või

¹Brignull, H., Leiser, M., Santos, C., & Doshi, K. (2023, April 25). *Deceptive patterns – user interfaces designed to trick you*. deceptive.design. Retrieved 27.03.2025, from <https://www.deceptive.design/>

² OECD. Dark commercial patterns. 2022. Lk 21.

³ Komisjoni teatis Euroopa Parlamendile ja Nõukogule. Uus tarbijakaitse tegevuskava. 13.11.2020. <https://eur-lex.europa.eu/legal-content/ET/TXT/HTML/?uri=CELEX:52020DC0696>

kallutatakse otsustusprotsesse.”⁴ Tegevuskava kehtimise perioodil on tumedaid mustreid otseselt või kaudselt juba käsitletud jõustunud digiteenuste, digiturgude ja tehisintellekti määrukses ning suure tõenäosusega on neil ka oluline roll veel alles planeeritud digitaalse õigluse määrukses.⁵

Majanduskoostöö ja Arengu Organisatsioon on 2022. aastal välja andnud tumedate ärimustrite tegevuskava, milles kirjeldab tumedaid mustreid kui praktikaid, mis “juhivad, petavad, sunnivad või manipuleerivad tarbijaid tegema valikuid, mis tihti pole nende parimais huvides.”⁶ Inimeste manipuleerimine, eksitamine või petmine kui selline pole muidugi õiguslikult enneolematu või uudne väljakutse. Euroopa Liit on tumedate mustritega seotud või neile sarnanevaid probleeme käsitlenud ka varem, osaliselt läbi andmekaitse või tarbijakaitse prisma. Näiteks sätestab isikuandmete kaitse üldmäärus, milliste parameetritega nõusolek on antud kehtivalt, ning paljud tarbijale suunatud tumedad mustrid kvalifitseeruvad agressiivseks või eksitavaks ebaausate kaubandustavade direktiivi järgi.

Tegemist on laia ja aktuaalse probleemiga, mille efektiivsest reguleerimisest oleneb otseselt ka teiste kehtivate õigusaktide kaitse efektiivsus digikeskkonnas. Näiteks on tumedaid mustreid laialdaselt kasutatud, et eksitada tarbijat andma isikuandmete kaitse määrukses tulenevat küpsiste nõusolekut.⁷ Milline näeks välja õigusmaastik füüsilises maailmas, kui lepingud sisaldaksid tingimusi, mis on kirjutatud nähtamatu tindiga või eraldi paberilehele, mille peab teenusepakkuja kontori sahtlitest ise üles leidma? Kui olemasolevate seaduste sätetest kõrvale hiilimine pole piisavalt efektiivselt keelatud, pole tegu mitte eraldiseisva kõrvalehiilimise probleemiga, vaid süstemaatilise probleemiga, millel on oluline mõju kõigile digikeskkonda kujundavatele õigusaktidele.

Tumedate mustrite mõjuvust on suurendanud asjaolu, et veebilehtede külastatelt korjatakse rohkem andmeid, kui kunagi varem. Tihti käib tumedate mustrite kasutamine käsikäes

⁴ Komisjoni teatis Euroopa Parlamendile ja Nõukogule. Uus tarbijakaitse tegevuskava. 13.11.2020. <https://eur-lex.europa.eu/legal-content/ET/TXT/HTML/?uri=CELEX:52020DC0696>

⁵ Mission letter to Michael McGrath. Ursula von der Leyen. https://commission.europa.eu/document/download/907fd6b6-0474-47d7-99da-47007ca30d02_en?filename=Mission%20letter%20-%20McGRATH.pdf

⁶ OECD (2022), “Dark commercial patterns”, *OECD Digital Economy Papers*, No. 336, OECD Publishing, Paris, <https://doi.org/10.1787/44f5e846-en>. Lk 2.

⁷ Behavioral study on unfair commercial practices in the digital environment: dark patterns and manipulative personalisation. European Commission. 2022. Lk 45.

isikustamisega või personaliseerimisega,⁸ mille käigus kasutatakse veebilehe külastaja andmeid ning käitumist veebilehel, et talle sobivamaid pakkumisi või sisu esitada. Isikustamine võib olla neutraalne või positiivne kogemus kasutaja jaoks, kuid võib sisaldada ka haavatavuste tuvastamist või profileerimist, mis on eriti kahjulik koosmõjus teiste tumedate mustritega.⁹ Tavapäraselt kasutavadki veebilehed mitmeid erinevaid tumedaid mustreid korraga ning üksikult neid reeglina ei esine.¹⁰ See tähendab ühtlasi, et kasutaja võib tumedate mustrite tõttu korraga kannatada mitmesugust kahju – näiteks majanduslikku ja ajalist kahju, mis võivad omakorda põhjustada psühholoogilist kahju.¹¹

Probleemi süvenemist on mõjutanud ka tehisintellekti kiire areng ja kasutuselevõtu tõus viimaste aastate jooksul, mis on mitmeid digiplatvormidel varasemalt kasutuses olnud tumedaid mustreid võimendanud ning võimaldanud ka täiesti uusi meetodeid tarbija valikute ja harjumuste tahtevastaseks manipuleerimiseks. Tehisintellekti abil on muuhulgas võimalik: enneolematu koguses andmeid koguda ja töödelda; reaalselt kasutaja käitumist ette aimata ja sellega kohaneda; tuvastada kõige tuluteenivamad tähelepanulõksud konkreetse isiku jaoks; ning ajastada ja paigutada nõusoleku küsimised täpselt sellesse hetkesse ja kohta, kus veebilehe külastaja suurima tõenäosusega oma õiguste riivega nõustub. Rääkimata unikaalsete artiklite, fotode, arvustuste ja muu sarnase sisu genereerimisest, mida ei ole võimalik tuvastada ja eemaldada varasemalt efektiivsete spämmifiltritega. See kõik muudab juba väljakujunenud kahjulikud tumedad mustrid veelgi dünaamilisemaks, personaliseeritumaks ning kasutaja jaoks raskemini ära tabatavaks.

Varem mainitud Euroopa Komisjoni uues tarbijakaitse tegevuskavas on toonitatud vajadust selliste tsiviilvastutuslike meetmete järgi, mis tagaks tehisintellekti põhjustatud kahju ohvritele võrdväärse kaitse muudete toodete ja teenuste põhjustatud kahju kaitsega.¹² 2024. aastal välja antud tehisintellekti käsitlev määrus on nüüdseks jõustunud ning käesolevas töös

⁸ Behavioral study on unfair commercial practices in the digital environment: dark patterns and manipulative personalisation. European Commission. 2022. Lk 6.

⁹ Helberger, Micklitz H.-W. et al. (2021) "Structural asymmetries in digital consumer markets", study for BEUC, Lk. 110.
https://www.beuc.eu/sites/default/files/publications/beuc-x-2021-018_eu_consumer_protection_2.0.pdf

¹⁰ Behavioral study on unfair commercial practices in the digital environment: dark patterns and manipulative personalisation. European Commission. 2022. Lk 6.

¹¹ OECD (2022), "Dark commercial patterns", *OECD Digital Economy Papers*, No. 336, OECD Publishing, Paris, <https://doi.org/10.1787/44f5e846-en>. Lk. 24.

¹² Komisjoni teatis Euroopa Parlamendile ja Nõukogule. Uus tarbijakaitse tegevuskava. 13.11.2020. <https://eur-lex.europa.eu/legal-content/ET/TXT/HTML/?uri=CELEX:52020DC0696>

hindan, kuivõrd sellise võrdväärse kaitse tagamine õnnestunud on, keskendudes täpsemalt just tumedate mustritega seonduvale tehisintellekti põhjustatud kahjule.

Tehisintellekti käsitlev määrus kasutab riskipõhist lähenemist ning kategoriseerib tehisintellektide kasutusviisid nende potentsiaalselt põhjustatava kahju järgi neljaks kasvavaks riskikategooriaks:

- a) minimaalse riskiga kasutusviisid, mida ei reguleerita;
- b) piiratud riskiga kasutusviisid, millele kehtivad läbipaistvuskohustused kasutaja suhtes;
- c) suure riskiga kasutusviisid, millele kohalduvad laiaulatuslikumad läbipaistvus- ja testimisstandardid ja järelvalve;
- d) vastuvõetamatu riskiga kasutusviisid, mis on keelatud.

Tumedaid mustreid piirab eelkõige tehisintellekti määruse 5. artikkel, mis käsitleb kõige kõrgema riskitasemega, s.t. vastuvõetamatu riskiga tehisintellektisüsteeme. Nimelt keelustab viienda artikli esimene lõige tehisintellektisüsteemid, “milles on kasutatud inimese teadvusest kaugemale ulatuva alalävisele tajule suunatud võtteid või sihilikult manipuleerivaid või petlikke võtteid, mille eesmärk või tagajärg on isiku või isikute rühma käitumise oluline moonutamine, kahjustades oluliselt nende võimet teha teadlik otsus ja pannes nad seeläbi tegema otsuse, mida nad ei oleks muul juhul teinud, viisil, mis põhjustab või mõistliku tõenäosusega põhjustab sellele isikule, teisele isikule või isikute rühmale olulist kahju”.

Sellisel käsitlusel on olulised puudused, mis jätavad paljude tumedate mustrite põhjustatud kahju kaitsealast välja. Üheks näiteks on olulise kahju põhjustamise kõrge standard ning sellise kahju põhjuslikult tehisintellekti tegevusega seostamise keerukus. Tehisintellekti põhjustatud kahju on tihti süsteemne, laiaulatuslik ning võib ilmnedas alles hiljem,¹³ mistõttu ei piisa kahju hindamisest üksikisikule või isikute grupile tehisintellektisüsteemi turule laskmise hetkel. Neid ja teisi tehisintellekti käsitleva määruse puuduseid analüüsin lähemalt käesoleva töö teises peatükis.

¹³ Kaminski, Margot E., The Developing Law of AI: A Turn to Risk Regulation (April 12, 2023). The Digital Social Contract: A Lawfare Paper Series (April 2023), U of Colorado Law Legal Studies Research Paper No. 24-5, Lk 3. Available at SSRN: <https://ssrn.com/abstract=4692562> or <http://dx.doi.org/10.2139/ssrn.4692562>

Puuduste kõrvaldamiseks ja tehisintellekti võimendatud ja võimaldatud tumedate mustrite probleemi efektiivsemaks tõkestamiseks pakun kolmandas peatükis välja mudeli, mis põhineb tehisintellektile omaste võimete piiramisel juhul, kui nende võimete kasutusviis vastab tumedate mustrite tunnustele. Pakutud mudel on tehnoloogianeutraalne, tulevikukindlam ning võimaldab lihtsamat *ex ante* hindamist.

Käesoleva magistritöö eesmärgiks ongi hinnata, kas tehisintellektipõhiste tumedate mustrite kasutus on olemasoleva Euroopa Liidu seadusandlusega efektiivselt reguleeritud ning pakkuda kitsaskohtade katmiseks välja alternatiivne tehisintellektile omaste võimete põhine mudel nimetatud tehisintellektipõhiste tumedate mustrite reguleerimiseks.

Töö ülesehitus koosneb kirjeldavast osast esimeses peatükis, mis annab ülevaated tumedate mustrite probleemi arenemisest ja süvenemisest digikeskkonnas ja tüüpiliste tumedate mustrite olemusest ning kirjeldab tumedate mustrite mõiste defineerimise ja põhjaliku taksonoomia loomise keerukust. Teine peatükk koosneb analüüsivast osast, mis hindab olemasolevate Euroopa Liidu määruste kaitse efektiivsust antud probleemi kontekstis ja kolmas peatükk sisaldab normatiivset osa, mis annab soovitusi tuvastatud kitsaskohtade korrigeerimiseks.

Tööd iseloomustavad järgmised EMS märksõnad: tehisintellekt, tarbijakaitse, digitaalarhitektuur, digiplatvormid, Euroopa Liidu õigus.

1. TUMEDATE MUSTRITE ARENG JA ALUSED

1.1. Areng

Muidugi on tumedad mustrid – petlik või tarbijat mõjutav disain – eksisteerinud ka varem, nii füüsilises maailmas kui ka virtuaalmaailmas selle sünnist saati. Näiteks võib öelda, et on tegemist tumeda mustriga, kui toidupoes on odavaimad kaubad kõige alumisele riiulile pandud, kus tarbija neid märgata ei pruugi ning kätte saamiseks kükitama peaks. Vastupidine olukord on kommiletis, kus kõige silmatorkama kujundusega snäkid on alumisel riiulil, kus need lapsele silma paistavad ning kust laps neid ise krabada ulatab. Peale selle, et tuttava multikategelasega pakend lapse vanusest tulenevat haavatavust¹⁴ ära kasutab, on vanema jaoks emotsionaalne lisapingutus last kommipakki tagasi panema veenda. Tulemuseks võib olla ost, mida vanem ilma tumeda mustri mõjuta sooritanud poleks ning milles ta võib pealekauba süüdistada jonnivat last või ennast, kaupluse riiulipaigutust küsitlemata. Digitaalsed tumedad mustrid mõjutavad ja suunavad sarnaselt kasutajate tehtavaid valikuid ja käitumist nagu tumedad mustrid päriselus. Kuid digitaalkeskkonnas navigeerimine on tarbija jaoks keerukam ja vähem intuitiivne, iga veebileht on erinev ning kasutajat mõjutada üritavaid kõrvalekaldeid tavadisainist on raskem tuvastada, ning samuti raskem seostatada kasutajale kahjuliku lõpptulemusega.

Füüsilises maailmas esinevad tumedad mustrid on praktiliselt kõik ammu kodifitseeritud mõne teise mõiste ja liigituse kaudu. Näiteks on üheks esimestest tumedaid mustreid kammitsevatest seadustest Vana-Roomas 50 aastat e.m.a jõustunud Lex Julia de Annona, mis nägi ette karistused tehnikult vilja hinna tõstmise ning ostjatele erineva hinna esitamise eest.¹⁵ Kaks aastatuhandet on möödunud ning digimaailmas on levinud praktikaks tume muster, mille kohaselt toote või teenuse esmajärjekorras näidatavat hinda muudetakse olenevalt näiteks sellest, kas ostu sooritaja vaatab pakkumist nutitelefoni või arvutist,¹⁶ või isegi

¹⁴Emma Calvert. Food marketing needs rules with teeth. 2021. Lk 19. The European Consumer Organisation. https://www.beuc.eu/sites/default/files/publications/beuc-x-2021-084_food_marketing_to_children_needs_rules_with_teeth.pdf

¹⁵Consumer empowerment in the digital economy: A critical analysis of the Cameroonian law on consumer protection in the digital age. Akama Samuel Penda. International Journal of Law. 2022. Lk 75. <https://www.lawjournals.org/assets/archives/2022/vol8issue4/8-4-14-240.pdf>

¹⁶Consumer market study on online market segmentation through personalised pricing/offers in the European Union. Final report. 2018. Lk 206.

olenevalt sellest, kas veebilehe kuvamiseks kasutatakse Apple'i või Windowsi operatsioonisüsteemi.¹⁷

Võib tunduda, et toodete ja teenuste digikeskkonda ümberasumisega on kahe silma vahele jäänud mõned põhimõtted, mis füüsilises keskkonnas pikaajaliselt juurdunud on. Erinevatel praktilistel kaalutlustel võib sellist arengut loomulikuks pidada: enneolematu keskkond vajab uusi norme, mis enneolematu keskkonna pidevalt arenevaid nüansse arvestada oskaks, kuid õigusnormistiku ümber sõnastamine võtab aega. Ootamise käigus on tänapäevane internetikasutaja jõudnud harjuda ebaausatele võtetele allumisega ning näeb neid paratamatu osana oma digikogemusest – oma õigustest loobumist nähakse digitaalteenuste kasutamise hinnana.¹⁸

Siiski pole tarbija suhtumine oma õigustesse alati nii jõuetu olnud. Näitena võib võtta segavad ja petlikud reklaamivõtted, mis Interneti esmalt tavatarbijateni jõudmise ajal plahvatuslikult arenesid ning erinevate tegurite koosmõjul tavapärasest kasutajakogemusest taandusid. Interneti laialdasema kasutuselevõtu algusaastatel koosnes see laias laastus väikestest veebilehtedest ja spetsiifilistest ühemeheprojektidest, mille looja tahtis midagi enda tarbeks üles laadida, jäädvustada või teistegagi jagada. Veebilehe disaini ja kujunduse keerukus olenes sellest, kuivõrd loojal kunsti- ja programmeerimisvaistuga tuttavaid jagus. Internetti ei nähtud veel ennast tõestanud usaldusväärse ja turvalise müügiplatvormina ning lihtsaimaks vahendiks, millega üks väikese veebilehe pidaja võis oma domeenile ja serverile tehtud kulutused tasa teenida, oli lehe kasutajatele reklaamide näitamine.

Vähereguleeritud elektroonilises keskkonnas kerkisid kasutajavaenulikud reklaamivormid nagu hüdra pead: välkuvad neonbännerid; võltsid lingid; väited, et oled tuhandes külastaja ja midagi võitnud; automaatselt mängima hakkavad hääle- ja videoklipid; masintõlgitud laim-uudised mõne kuulsuse eraelu või surma kohta ning muidugi – vaadeldava veebilehe ette uues aknas avanevad *pop-up* reklaamid ning nende noorem, salakavalam variant – *pop-under*

https://commission.europa.eu/publications/consumer-market-study-online-market-segmentation-through-personalised-pricingoffers-european-union_en

¹⁷ Personaliseeritud hinna või personaliseeritud tootejärjestuse kujundamine on kõige rohkem levinud lennupiletite müügi ja hotellindusega tegelevatel veebilehtedel. Consumer market study on online market segmentation through personalised pricing/offers in the European Union. Final report. 2018. Lk 46. https://commission.europa.eu/publications/consumer-market-study-online-market-segmentation-through-personalised-pricingoffers-european-union_en

¹⁸ Behavioral study on unfair commercial practices in the digital environment: dark patterns and manipulative personalisation. European Commission. 2022. Lk 86

reklaamid, mille aken avanes veebilehe taga, mistõttu kasutaja ei märganud seda kuni brauseri sulgemiseni ning ei pruukinud teada, milline veebileht reklaamilt teenis. Petlikke või peidetud reklaamivõtteid, mis suunasid kasutajat klikkima ja veebilehele tasu tooma, võib pidada üheks esimestest laialt levinud tumedateks mustriteks digikeskkonnas.

Pop-up reklaamide väljamõtteleja on küll hiljem vabandanud¹⁹, kuid Pandora laegas oli avatud ning sellised reklaamipraktikad said lahutamatuks osaks 2000-date internetikogemusest. Seadusandlusel läks aega, et hakata piirama erinevaid segavate reklaamide aspekte – näiteks Euroopa Liidu e-privatsuse direktiivi²⁰ kujul, mis nõudis veebikülastaja nõusolekut küpsiste kasutamiseks ning mõjutas seeläbi kaudselt reklaame, mis olid küpsiste abil kasutajaid erinevatel veebilehtedel jälginud.

Otsesem ja kiirem surve selliste reklaamipraktikate kadumiseks avaldus aga kasutajatelt. Tihti oli võimalik hinnata veebilehe usaldusväärsust ja kvaliteeti selle järgi, kui segavad, petlikud ja rohkearvulised olid selle reklaamid. Kui veebilehe avamisel avanes ka kolm *pop-up* reklaami ning välvivate neonbännerite tõttu oli keeruline sisule keskenduda, võis kasutaja ühe pilguga hinnata, et lehe prioriteediks on reklaamitulu maksimeerimine, ning valida teise samasisulise veebilehe, mis kasutajakogemust rohkem hindas. Kuna ebameeldiva reklaamikogemuse saanud kasutajad naasid lehele vähese tõenäosusega, olid jätkusuutlikumad need veebisaidid, mille reklaamid olid tagasihoidlikumad ning mida kasutajad regulaarselt külastama jäid.

Selline “loomulik valik” tingis veebilehe omanikelt vähem segavate reklaamide eelistamise ja reklaame pakkuvatelt firmadelt enesereguleerimise. Näiteks E-maili teenuste pakkujad lisasid filtrid spämmkirjade eristamiseks ja kustutamiseks.²¹ Lisaks võistlesid veebibrauserid kasutajale mugavaima kogemuse pakkumises, lisades brauseritesse näiteks automaatse *pop-up*

¹⁹Ethan Zuckerman, kes *pop-up* reklaamide idee tuli, tahtis luua viisi eraldada kontroversiaalse sisuga reklaam veebilehest, mis reklaamiga tulu teenis. Rohkem artiklis: The Internet's Original Sin. Ethan Zuckerman. 2014. The Atlantic. <https://www.theatlantic.com/technology/archive/2014/08/advertising-is-the-internets-original-sin/376041/>

²⁰EUROOPA PARLAMENDI JA NÕUKOGU DIREKTIIV 2002/58/EÜ, 12. juuli 2002,

milles käsitletakse isikuandmete töötlemist ja eraelu puutumatuse kaitset elektroonilise side sektoris (eraelu puutumatust ja elektroonilist sidet käsitlev direktiiv) <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02002L0058-20091219>

²¹ Stigler, Lk 308.

akende blokeerimise, mis tõi kaasa ka selle reklaamiviisi vähenemise, kuna vähesed neid aknaid nägid. Seega kasutajakogemus paranes oluliselt vabaturumajandusele sarnaneva konkurentsi, pakkumise ja nõudluse kaudu, vajamata põhjalikku sekkumist seadusandjalt. Aastatuhande vahetuse aegsed digitaalturgude uurijad arvasid, et Interneti eripärased omadused võivad kaasa tuua täiusliku turu, kus ostjad on tänu otsingu kergusele täielikult hindadest ja toodete valikust informeeritud ning edasimüüjad teenivad nullkasumit turu kõrge võistlevuse tõttu.²²

Kakskümmend aastat hiljem on tarbija ja digiplatvormide jõuvahekord muutunud ning ei meenuta enam konkurentsirohket vabaturumajandust. Kasutajasõbralikumate disainivõtetega uustulijad ei saa tarbijatele efektiivselt pakkuda populaarsete veebilehtedega võrdväärseid alternatiive ning digiturg ei suuda ennast vabalt korrigeerida turgu valitsevate tehnosiidude tõttu, kes saavad konkurentsilt tarbijatele ühepoolseid hindu, nõudmisi ja tingimusi esitada.

23

Peale reklaamide on arenenud lõpmatu arv viise, kuidas elektrooniliselt tulu teenida igast inimkogemusest, -vajadusest, -loomingust ja -tundest. Internetist on saanud asendamatu kogukonnakeskus, mis on tarbijaga alati kaasas telefoni või sülearvuti kujul, ootamaks sisustamata hetke, mida täita uudiste, suhtluse, ostlemise, meelelahutuse või muu meelepärasega. Poliitilisi debatte saab pidada säutsude kaudu, kaaslase võib leida sotsiaalmeediast või äppidest ning ostuideid saab suunamudijatelt. Sotsiaalmeedia platvormid suudavad e-maili või telefonikontaktide kaudu leida üles vanad tuttavad ja klassikaaslased, õnnelikul juhul selleks kasutajalt luba küsides.²⁴ On väheseid, kes poleks tehnouhiskonna mugavustest osa võtnud. Tänapäevane tarbija ei istu süvenenult lauaarvuti taga, vaid kannab digikeskkonda kaasas, mis omakorda teeb teda haavatavamaks erinevatele uudsetele tumedatele mustritele hajameelsuse ja tähelepanu jaotumise tõttu.

²² Brynjolfsson, Erik, and Michael D. Smith. "Frictionless Commerce? A Comparison of Internet and Conventional Retailers." *Management Science*, vol. 46, no. 4, 2000, pp. 563–85. *JSTOR*, <http://www.jstor.org/stable/2661602>. Accessed 5 Apr. 2025. Lk 1.

²³ Stigler Lk 81

²⁴ LinkedIn kasutas 2013. aastal kasutajaliidese disaini, mis importis kasutaja loaga tema kontaktid ning esitas neid sarnaselt juba kontot omavate isikute kontaktidega. Kui kasutaja esitatud kontaktile klikkis, saatis LinkedIn tema poolt kontaktile kutse veebilehega liitumiseks. LinkedIn maksis klassihagi rahuldamiseks 13 miljonit dollarit. Täpsemalt California kohtu otsuses: Perkins et al v. LinkedIn Corp. 13-CV-04303-LHK.

Koos tuluteenimisvõimalustega on laienenud ka tumedate mustrite arv, mis tõukavad kasutajaid erinevaid veebilehele kasulikke ja tarbijatele kahjulikke otsuseid tegema, olgu selleks siis oma andmete ülemäärane jagamine, väärtusliku aja raiskamine või ebavajaliku ostu sooritamine. Manipuleerivate võtete kasutamisel ei pea suured digiplatvormid kartma, et kasutajad halvema kogemuse tõttu konkurendi juurde lahkuksid, kuna samaväärilisi tumedate mustrite vabu alternatiive pole. Samuti ei tunne kasutajad ilma tumedate mustrite alase teadmispagasita neid manipulatiivseid võtteid ära ega tea, millised neist on seadusevastased ning millised lubatud.²⁵ Kasutajad on ka nii harjunud tumedate mustritega, et ka ilmselgeid manipuleerivaid võtteid ignoreeritakse, kui neid pakutakse koos muidu kvaliteetse teenusega.

26

Kasutajate vähese teadlikkuse probleemi süvendab digitaalne asümmeetria, mis digiplatvormidel valitseb.²⁷ Veebilehe külastaja ei tea, kuidas veebilehe erinevad funktsioonid töötavad; millist infot kuvatakse teistele külastajatele; ega milliseid tema andmetest konkreetse funktsiooni täitmiseks kasutatakse. Näiteks hinda võrdlevate veebilehtede kasutajatele – kes seeläbi näitavad, et on tundlikumad toote hinna osas – võidakse otse hinda võrdlevalt veebilehelt müügiportaali sisenedes odavama hinnaga tooteid või teenuseid pakkuda, kuid see-eest rakendada ostuprotsessi käigus kõrgemaid lisatasusid, mis viivad kasutajale märkamatuult toote koguhinna tagasi tavatasemele.²⁸

Euroopa Liit on sellele jõuvahekorrale reageerinud olemasolevate tarbijakaitsega seotud õigusaktide ajakohastamisega²⁹, erinevate tumedate mustrite alaste uuringute ja parimate praktikate ülevaadete koostamisega ning ka uute digiteenuste ja digiturgude määruste kokkupanekuga. Digiteenuste ja digiturgude määrused tõstavad muude platvormide taustal esile väga suure Euroopa Liidu sisese kasutajaskonnaga digiplatvormid, otsingumootorid ja

²⁵ Behavioral study on unfair commercial practices in the digital environment: dark patterns and manipulative personalisation. European Commission. 2022. Lk 86

²⁶ EC study Lk. 120, 87

²⁷ Helberger, Micklitz H.-W. et al. (2021) “Structural asymmetries in digital consumer markets”, study for BEUC, Lk. 108.
https://www.beuc.eu/sites/default/files/publications/beuc-x-2021-018_eu_consumer_protection_2.0.pdf

²⁸ Personaliseeritud hinna või personaliseeritud tootejärjestuse kujundamine on kõige rohkem levinud lennupiletite müügi ja hotellindusega tegelevatel veebilehtedel. Consumer market study on online market segmentation through personalised pricing/offers in the European Union. Final report. 2018. Lk 46.
https://commission.europa.eu/publications/consumer-market-study-online-market-segmentation-through-personalised-pricing-offers-european-union_en

²⁹ Omnibussi direktiiv haldas x y z +++

nn. pääsuvalitsejad, millele nende turul valitseva jõupositsiooni tõttu kohaldatakse ka rangemaid piiranguid.

Lisaks neile olemasolevatele määrustele on Ursula von der Leyeni teise komisjoni päevakavas ka uue digitaalse õigluse määruse loomine, mis keskenduks tarbijate kaitsele praeguses digiühiskonnas levinud ebaeetiliste võtete, tumedate mustrite ja muude haavatavuste ära kasutamise eest.³⁰ Sellesisulise määruse koostamise päevakavva võtmine toonitab digimaastikul valitseva olukorra tõsidust ning asjaolu, et juba eksisteeriv õigusraamistik vajab täiendust tumedate mustrite efektiivseks piiramiseks. Avalik tagasiside- ja konsulteerimisperiood digitaalse õigluse määruse osas kestis vahemikus 19. mai kuni 31. august 2025. a. Töö kirjutamise hetkel on algatus ettevalmistamisel.

Esialgne ettepanek eraldiseisva digitaalse õigluse määruse loomiseks kerkis digitaalse õiglusega seostuvate tarbija õigusi käsitlevate õigusaktide sobivuskontrolli käigus.³¹ Sobivuskontroll tuvastas mitmeid kitsaskohti Euroopa Liidu asjakohases seadusandluses ning süvenevaid probleeme modernses digikeskkonnas, nimelt:

- a) tumedate mustrite lai levik populaarsetel veebilehtedel;³²
- b) sõltuvusttekitava ja tähelepanu hõivava disaini levik;³³
- c) ebaausa personalisatsiooni tõus näiteks tarbijale soovimatute isikustatud reklaamide, soovitude ja hinnapakkumiste näol;³⁴
- d) sotsiaalmeedia ja suunamudijate kaudu turustamine;³⁵
- e) probleemid digitaalsete lepingute ja tellimustega;³⁶
- f) tarbija vastu ebaõiglased lepingutingimused digikeskkonnas;³⁷
- g) automaatsete või tehisintellekti põhiste tarkade lepingute levik;³⁸
- h) *dropshipping*, ehk füüsilise laojäägita toote müügi vahendamine tootjalt ostjale;³⁹

³⁰https://commission.europa.eu/document/download/907fd6b6-0474-47d7-99da-47007ca30d02_en?filename=Mission%20letter%20-%20McGRATH.pdf

³¹Digitaalse õigluse sobivuskontroll. Euroopa Komisjon. 2024. Lk 144. https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13413-Digital-fairness-fitness-check-on-EU-consumer-law_en

³² Samas. Sobivuskontroll Lk 146.

³³ Samas. Sobivuskontroll Lk 153.

³⁴ Samas. Sobivuskontroll Lk 162.

³⁵ Samas. Sobivuskontroll Lk 169.

³⁶ Samas. Sobivuskontroll Lk 176.

³⁷ Samas. Sobivuskontroll Lk 182.

³⁸ Samas. Sobivuskontroll Lk 195.

³⁹ Samas. Sobivuskontroll Lk 200.

- i) tehisintellektil põhinevate tekstirobotite kasutamine klienditeeninduses inimteenindaja asemel;⁴⁰
- j) kõrgema hinnaga edasimüügi eesmärgil automaatseid oste sooritavad robotid;⁴¹
- k) ürituste piletite müügihinna dünaamiline muutmine.⁴²

Digitaalse õigluse määrus peaks esialgse info põhjal käsitlema eelnevas loetelus sisalduvaid probleeme alates punktist a kuni punktini d.⁴³ Ehk on võimalik, et digitaalse õigluse määrus täidab tulevikus tumedate mustrite alases regulatsioonis lüngad, kaasa arvatud tehisintellektiga seotud tumedate mustrite osas, mida käesolev töö välja toob. Kuivõrd see õigusakt on aga alles planeeritud,⁴⁴ saab töö kirjutamise hetkel analüüsida vaid olemasolevates määrustes ja direktiivides sisalduvaid põhimõtteid.

1.2. Kasutatavad terminid

1.2.1. Tehisintellekt

Iga tehisintellektialase teadustöö jaoks on oluliseks võtmeküsimuseks see, kuidas defineerida tehisintellekti, kuna selle terminiga sildistatakse tihti erineva mahu, võimete ja ülesannetega süsteeme. Näiteks liigitatakse tehisintellekti kitsaks või üldiseks olenevalt sellest, kas see saab hakkama üht tüüpi ülesannete täitmisega või on võimeline kohalduma mitmete erinevate rollidega.⁴⁵ Kui tehisintellekt on võimeline kohalduma, on tegemist üldtehisintellektiga; kui tehisintellekt on loodud ühetaoliste probleemide lahendamiseks, on tegemist kitsa tehisintellektiga. Antud töö kontekstis räägib kaks argumenti kitsa tehisintellekti termini kaasamise kasuks.

Esiteks ei ole võrdelist seost tehisaru kompleksuse ja sellega kasutajale avaldatud negatiivse mõju vahel, mistõttu üldise TI-ga piirdumine jätaaks töö uurimisalast välja paljud lihtsama

⁴⁰ Samas. Sobivuskontroll Lk 200.

⁴¹ Samas. Sobivuskontroll Lk 202.

⁴² Samas. Sobivuskontroll Lk 202.

⁴³ https://commission.europa.eu/document/download/907fd6b6-0474-47d7-99da-47007ca30d02_en?filename=Mission%20letter%20-%20McGRATH.pdf

⁴⁴ Digitaalse õigluse määrase esialgset ettepanekut võib oodata 2026. aasta lõpuks.

⁴⁵ Kaimar Karu. Tehisintellekti keerukad küsimused. Juridica 2021/1. Lk 43.

toimimismehhanismiga tehisintellektil baseeruvad tumedad mustrid, millel võib sellegipoolest olla oluline mõju teenuse kasutaja valikuvabadusele.

Teiseks kitsa tehisintellekti kasutuse poolt rääkivaks argumendiks on asjaolu, et värskes tehisintellekti käsitlevas määruses endas on võetud aluseks üsna üldsõnaline OECD tehisintellekti definitsioon, millele vastab ka kitsas tehisintellekt. Täpsemalt ütleb TI määruse artikkel 3 lõige 1: “”Tehisintellektisüsteem” on masinpõhine süsteem, mis on projekteeritud töötama erineval autonoomsuse tasemel ning mis võib pärast juurutamist olla kohanemisvõimeline ja mis saadud sisendist otseste või kaudsete eesmärkide saavutamiseks järeltab, kuidas genereerida väljundeid, näiteks prognoose, sisu, soovitusi või otsuseid, mis võivad mõjutada füüsilist või virtuaalset keskkonda”. Kuna see mõiste ei sisalda minimaalset autonoomsuse taset, eesmärgid võivad olla kaudsed, kohanemisvõimelisuse nõuet ega füüsilise või virtuaalse keskkonna mõjutamise nõuet, jääb mõistest alles “masinpõhine süsteem, mis sisendist järeltab, kuidas väljundeid genereerida”. Seda tehisintellekti definitsiooni on kritiseeritud kui kohalduvat peaaegu kõigile programmidele.⁴⁶ Ka antud töö lähtub kitsa tehisintellekti definitsioonist, et hõlmata ka lihtsamate tehisintellektide abil kasutatavaid tumedaid mustreid.

1.2.2. Käitumisökonomika

Käitumisökonomika on majanduslik teooria, mis lähtub põhimõttest, et inimeste võime teha mõistlikke valikuid on piiratud nende kognitiivsetest võimetest.⁴⁷ Kognitiivsed nihked mõjutavad kõigi inimeste käitumist. Õiguslikus kontekstis oodatakse tihti mõistlikku käitumist, mida inimesed realistlikult teha ei pruugi.

1.2.3. Digitaalne asümmeetria

Digitaalne asümmeetria võib olla informatsiooniline, käitumuslik, tehniline või majanduslik jõuvahekord digiplatvormi kasutaja ja teenuse pakkuja vahel.

⁴⁶ Ebers, Martin. “Truly Risk-Based Regulation of Artificial Intelligence How to Implement the EU’s AI Act.” *European Journal of Risk Regulation*, 2024, 1–20. <https://doi.org/10.1017/err.2024.78>. Lk 12.

⁴⁷ Cass R. Sunstein, Christine Jolls & Richard H. Thaler, “A Behavioral Approach to Law and Economics,” 50 *Stanford Law Review* 1471 (1998). Lk. 1545. <https://www.jstor.org/stable/1229304>

1.2.4. Tehnilised terminid

Digiplatvormide näol on tegemist teabe talletamise teenusega, mille käigus talletatakse teenusesaajate taotlusel teenusesaajate esitatud teavet ning levitatakse seda teavet teenusesaajate taotlusel üldsusele.⁴⁸ Teisitiõeldes on tegemist veebilehtedega, mis säilitavad ja jagavad kasutajate loodud sisu ja teavet, nagu näiteks erinevad sotsiaalmeediaplatvormid.

Internetipõhine kasutajaliides⁴⁹ tähendab tarkvara, sealhulgas veebisaiti või selle osa ning rakendusi, kaasaarvatud mobiilirakendusi.⁵⁰ Lihtsustatult öeldes on tegemist veebilehe osadega, mis on kasutajale nähtavad, kogetavad või kasutatavad ning on loodud veebilehe, mitte teiste kasutajate poolt.

1.3. Tumede mustrite mõiste defineerimise keerukus

Harry Brignull oli esimene, kes tumede mustrite mõistet kasutas, defineerides neid kui “trikid, mida veebilehtedel ja äppides kasutatakse, et panna sind tegema midagi, mida sa ei tahtnud, nagu näiteks millegi ostmine või end millekski kirja panemine.”⁵¹ Hiljem on Majanduskoostöö ja Arengu Organisatsioon kasutanud “tumede äriliste mustrite”⁵² mõistet, mida on defineerinud kui võtteid, mis “juhivad, petavad, sunnivad või manipuleerivad tarbijaid tegema valikuid, mis tihti pole nende parimais huvides.”⁵³ Tihti kasutatakse tumedatest mustritest rääkides mõnda muud terminit, näiteks “petlik disain” või “petlikud mustrid”.⁵⁴ Ka õiguslikus kontekstis on mõnevõrra välditud “tumede mustrite” nimetamist sellisena, kui mõni muu termin on täpsem või konteksti sobilikum.

Näiteks kasutas terminit “tumedad mustrid” Euroopa Liidu õigusaktidest esimesena digiteenuste määrus, küll mitte regulatiivosas, vaid preambulis. Nimelt defineerib preambuli

⁴⁸ DSA art 3 lg i.

⁴⁹ User Interface või UI ing. k.

⁵⁰ DSA art 3 lg m.

⁵¹ Brignull, H., Leiser, M., Santos, C., & Doshi, K. (2023, April 25). *Deceptive patterns – user interfaces designed to trick you*. deceptive.design. Retrieved 27.03.2025, from <https://www.deceptive.design/>

⁵² “Dark commercial patterns” ing. k.

⁵³ OECD (2022), “Dark commercial patterns”, *OECD Digital Economy Papers*, No. 336, OECD Publishing, Paris, <https://doi.org/10.1787/44f5e846-en>. Lk 2.

⁵⁴ “Petliku disaini” ja “petlike mustrite” mõistet “tumede mustrite” mõiste asemel on muuhulgas kasutanud ka Harry Brignull ise.

67. punkt saksa ja inglise keeles eksplitsiitselt tumedaid mustreid kui tavasid, mis “[...] kas tahtlikult või tegelikult moonutavad või kahjustavad oluliselt teenusesaajate suutlikkust teha sõltumatuid ja teadlikke valikuid või otsuseid.” Määruse eesti ja prantsuse keelses versioonis on piiratud “tumedate mustrite” ümbersõnastamisega tehnoloogiliseks terminiks, “digiplatvormide internetipõhised eksitavad kasutajaliidesed”. Võib väita, et nii see definitsioon kui ka “petlik disain” on terminina täpsemad ning annavad probleemi sisu paremini edasi, kui “tumedad mustrid”, mis vajab mõistmiseks selgitust.

Autor eelistab siiski “tumedaid mustreid” kui kõlavamat üldterminit, mis hõlmab erinevaid digikeskkonnas levinud praktikaid. Tumedad mustrid ei ole ainult petlikud või eksitavad, vaid võivad seisneda ka näiteks kasutajale valiku andmata jätmises või valiku üles leidmise keerukaks tegemises. Tumedad mustrid ei koosne vaid kujunduslikest elementidest nagu nuppude värv, menüüde alajaotus jms, vaid ka näiteks emotsionaalselt laetud või segasest sõnastusest.⁵⁵ Element, mis kasutajat talle ebasoodsat otsust tegema mõjutab, ei pruugi olla mitte küsimuse kujundus või sõnastus, vaid näiteks aeg ja koht, millal küsimust talle esitatakse. Näiteks võib laupäeva varahommikul klubitänaval viibiv isik olla oma ebaadekvaatse seisundi tõttu vastuvõtlikum impulsiivsete ostude sooritamisele.

Tumedad mustrid ei pruugi sisaldada ka pahatahtlikku elementi või eesmärki isikut manipuleerida, eksitada või petta. Tume muster võib ilmuda ka heatahtliku kasutajaliidese disaineri käe läbi, kes ei pruugi mõista, miks konkreetne tehniline lahendus eriti efektiivselt tööle on hakanud,⁵⁶ eriti juhul, kui disainielement on ilma selle tööpõhimõttesse pikemalt süvenemata kopeeritud mõnelt populaarsemalt digiplatvormilt. Veel halvem on olukord juhul, kui disaineriks on inimese asemel tehisintellekt, kuna tehisintellekti välja töötatud mudel, mis täidab näiteks äriliste huvide maksimeerimise eesmärki, võib välja töötada väga problemaatilise mudeli lihtsalt seetõttu, et see on efektiivseim ja täidab ärilist eesmärki kõige paremini.⁵⁷ Tehisintellekt üldjuhul ei kaalu taotletavaid ärilisi huve teenuse kasutajate põhiõiguste riive vastu ega arvesta võimalikku negatiivset mõju inimesele või ühiskonnale. Näiteks on Youtube'i platvormi videote algoritmiline soovitusüsteem soodustanud

⁵⁵ OECD Dark commercial patterns Lk 9.

⁵⁶ Willis, Lauren E., Deception by Design (August 12, 2020). Loyola Law School, Los Angeles Legal Studies Research Paper No. 2020-25, 34 Harvard Journal of Law & Technology 115 (2020), Lk. 150. Available at SSRN: <https://ssrn.com/abstract=3694575>

⁵⁷ Willis, Lauren E., Deception by Design (August 12, 2020). Loyola Law School, Los Angeles Legal Studies Research Paper No. 2020-25, 34 Harvard Journal of Law & Technology 115 (2020), Lk. 148. Available at SSRN: <https://ssrn.com/abstract=3694575>

kontroversiaalsete videote levikut, soovitades dieedi teemalisi videosid vaadanud haavatavatele teismelistele tüdrukutele ka videosid juhtnööridega, kuidas anoreksiat saada.⁵⁸ Soovitussüsteemi ülesanne leida videod, millele kasutaja suure tõenäosusega klikib ning platvormil veel aega veedab ning rohkem reklaame näeb, on täidetud, kuid kasutaja tervise ja heaolu silmas pidamine vajab selliste soovituste märkamist ning ennetamist.

Tume muster ei pruugi olla ka ebaseaduslik või tingimata vajada õiguslikku reguleerimist. Näiteks võivad tarbijad eelistada nende huvidele vastavaid reklaame,⁵⁹ hoolimata sellest, et nii reklaamifirmad kui ka digiplatvorm selle arvelt teenib ning tarbija otsuseid teeb, mida ta muul juhul vahest teinud poleks.

Ülalkirjutatu põhjal oleneb tumedate mustrite defineerimine suuresti eesmärgist, mille nimel neid mõisteid kirjeldatakse. Käesoleva töö eesmärgiks on võimalikult põhjalikult tuvastada tehisintellekti abil võimaldatud või võimendatud tumedad mustrid, mistõttu võtan aluseks eriti laia tumedate mustrite tõlgenduse, millest olen eemaldanud kujundusliku elemendi ja pahatahtliku eesmärgiga seotud tunnused, mis esinevad Brignulli ja digiteenuste määrase toodud mõistetes.

Tumedad mustrid on selle töö kontekstis võtted, mis suurendavad oluliselt tõenäosust, et digiplatvormi kasutaja teeb platvormile kasuliku ning endale kahjuliku otsuse, mida ta ilma tumeda mustri kasutamiseta ei teeks.

⁵⁸ Stigler Committee on Digital Platforms: Final Report. 2019. Lk. 66.

⁵⁹ EC Study Lk. 278.

1.5. Levinud tumedad mustrid

Nagu ka eelnevas alapeatükis kirjeldatud, pole kasutusele võetud ühtset tumedate mustrite definitsiooni.⁶⁰ Siiski valitseb erialakirjanduses laias laastus üksmeel selle osas, millised digiplatvormidel levinud võtted on näideteks tumedatest mustritest.⁶¹ See alapeatükk annab ülevaate tüüpilistest digiplatvormidel kasutavatest tumedatest mustritest, võttes aluseks Harry Brignulli tumedate mustrite veebilehel toodud 16-tüübilise loetelu.⁶²

1.5.1. Võrdluse ärahoidmine

Võrdluse ärahoidmine tähistab tumedat mustrit, mille käigus erinevate toodete või veebilehtede pakutavate teenuste võrdlus tehakse kasutaja jaoks nii keeruliseks, et tal pole enne otsustamist võimalik tuvastada, milline toode või teenus vastab kõige paremini tema vajadustele.⁶³ Näiteks ostuplatvormil toodete odavama hinna järgi sorteerimisel siiski kallimate toodete odavamatega läbisegi esitamine, mis ei lase tarbijal tuvastada, milline on odavaim toode, mis tema vajadustele vastab.

1.5.2. Kinnitushäbistamine

Kinnitushäbistamine kujutab kasutaja emotsioonide või haavatavustega mängimist, et kasutajale kasuliku otsuse tegemist keerulisemaks teha teda häbistades või alavääristades.⁶⁴

Näiteks kinnitushäbistamisest võib olla disainivõtte, mille käigus kasutaja peab keelduva otsuse kinnituseks vajutama nuppu sisuga “kinnitan, et ei soovi uudiskirja ega oma tervise eest hoolitseda.”

1.5.3. Peidetud reklaam

⁶⁰ OECD. Dark commercial patterns. 2022. Lk 13.

⁶¹ OECD. Dark commercial patterns. 2022. Lk 13.

⁶² Brignull, H., Leiser, M., Santos, C., & Doshi, K. (2023, April 25). *Deceptive patterns – user interfaces designed to trick you*. deceptive.design. Retrieved 27.03.2025, from <https://www.deceptive.design/types>

⁶³ Brignull, H., Leiser, M., Santos, C., & Doshi, K. (2023, April 25). *Deceptive patterns – user interfaces designed to trick you*. deceptive.design. Retrieved 27.03.2025, from <https://www.deceptive.design/types>

⁶⁴ Brignull, H., Leiser, M., Santos, C., & Doshi, K. (2023, April 25). *Deceptive patterns – user interfaces designed to trick you*. deceptive.design. Retrieved 27.03.2025, from <https://www.deceptive.design/types>

Peidetud reklaam tähistab mustrit, mille käigus reklaamsõnum sulandatakse muu veebilehel esitatava sisuga selliselt, et kasutaja võib sellele ekslikult klikkida või mitte tuvastada, et tegemist on reklaamiga. Digiplatvorm teenib sellisest ekslikult tehtud otsusest ning kasutaja kulutab oma aega ja tähelepanu reklaamile.⁶⁵

Näiteks on Euroopa Kohus sellist mustrit käsitlenud C-102/20 eelotsuses, mis puudutas reklaamsõnumite kuvamist päris e-kirjadele sarnaneval kujul ja nende hulgas kasutaja elektronpostkastis.⁶⁶ Otsus käsitles peidetud reklaami mustrit läbi ebaausate kaubandustavade direktiivi sätete.

1.5.4. Võlts nappus

Võltsi nappusega on tegu juhul, kui kasutaja tunneb survet tehingu kiireks sooritamiseks, kuna talle näidatakse kasutajaliideses indikaatorit, et toodet on alles limiteeritud koguses või et selle ostmisest on huvitatud väga palju inimesi. Võltsi nappuse tume muster kasutab kasutaja vastu ära tema kognitiivset nihet, mille järgi inimesed ihaldavad vähe saada olevaid asju rohkem.⁶⁷

Võltsi nappuse tume muster kujutab endast üht e-poodides levinumatest tumedatest mustritest.⁶⁸ Selle näiteid võib leida erinevatest veebipoodidest, näiteks Amazoni või Aliexpressi platvormilt, mis tihti toovad hoiatavas kirjas esile, kui vähe konkreetseid tooteid laos alles on, või ka lihtsalt seda, et lao seis on madal, ilma täpsemat infot andmata.⁶⁹

1.5.5. Võlts sotsiaaltunnustus

Võlts sotsiaaltunnustus kirjeldab erinevaid toodetele või teenustele “inimeste poolt” antud tunnustusi, mille eesmärk on toodet või teenust näidata teiste inimeste hulgas populaarsena. Näideteks võltsidest sotsiaaltunnustustest on liialdatud arvustused ja tootehinnangud, aga ka

⁶⁵ Brignull, H., Leiser, M., Santos, C., & Doshi, K. (2023, April 25). *Deceptive patterns – user interfaces designed to trick you*. deceptive.design. Retrieved 27.03.2025, from <https://www.deceptive.design/types>

⁶⁶ C-102/20 StWL Städtische Werke Lauf a.d. Pegnitz. Punktid 64-75. <https://eur-lex.europa.eu/legal-content/ET/TXT/HTML/?uri=CELEX:62020CJ0102>

⁶⁷ Brignull, H., Leiser, M., Santos, C., & Doshi, K. (2023, April 25). *Deceptive patterns – user interfaces designed to trick you*. deceptive.design. Retrieved 27.03.2025, from <https://www.deceptive.design/types>

⁶⁸ EC study Lk. 47.

⁶⁹ EC study Lk. 47.

aktiivsussõnumid.⁷⁰ Aktiivsussõnumid edastavad toodet vaatavale kasutajale teateid selle kohta, et teine isik on toote just ostnud. See tekitab usaldust tootes ning samuti pakilisust tehingu tegemisel, kuna tundub, et teised kasutajad ostavad asja eest ära.

Lisaks võib sotsiaaltunnustuseks pidada näiteks soovitusi stiilis “kasutajad ostavad tihti koos selle tootega ka teise toote” või “pärast selle toote vaatamist, otsustasid kasutajad teise toote ostmise kasuks”. Ka juhul, kui tegemist on tõese infoga, võib see mõjutada kasutajat sooritama suuremas mahus oste, kui eelarves ette nähtud oli. Võltsi sotsiaaltunnustuse alla saab liigitada ka näiteks negatiivsete arvustuste eemaldamise praktika, mis jätab tootest võltsilt parema mulje.

Võltsi sotsiaaltunnustuse näol on tegemist mustriga, mis on tehisintellekti poolt võimendatud, kuna teksti tootva tehisintellekti abil saab kiiresti genereerida toote arvustusi, mida on keeruline eraldada päris arvustustest.

1.5.6. Võltis pakilisus

Võltis pakilisus kujutab kasutajale võltsi ajalimiidi esitamist, mille jooksul ta kas tehingu või otsuse tegema peab. Ajalimiidi otsa saades võib see lihtsalt otsast peale alata või muul moel sisutühi olla.⁷¹ Näiteks võib suure odavmüügi kampaania korduda alalõpmata, näidates tooteid pidevalt piiratud aja jooksul allahinnatutena.

Võltis pakilisus on teiseks levinuimaks e-poodides esinevaks tumedaks mustriks, mida on kasutanud Aliexpress, Amazon ja teised poed.⁷²

1.5.7. Sunnitud tegevus

Sunnitud tegevus kujutab tumedat mustrit, kus kasutaja on sunnitud mingi soovitava funktsiooni kasutamiseks midagi ebasoovitavat tegema. Näiteks nõustuma küpsistega, et

⁷⁰ Brignull, H., Leiser, M., Santos, C., & Doshi, K. (2023, April 25). *Deceptive patterns – user interfaces designed to trick you*. deceptive.design. Retrieved 27.03.2025, from <https://www.deceptive.design/types>

⁷¹ Brignull, H., Leiser, M., Santos, C., & Doshi, K. (2023, April 25). *Deceptive patterns – user interfaces designed to trick you*. deceptive.design. Retrieved 27.03.2025, from <https://www.deceptive.design/types>

⁷² EC study Lk. 47.

veebilehel olevat sisu näha.⁷³ Või nõustuma reklaamide isikustamisega, mille ainsaks alternatiiviks on maksta reklaamide isikustamata jätmise eest.

1.5.8. Keerukas tühistamine

Keerukat tühistamist on tumedate mustrite kontekstis nimetatud ka “prussakate motelliks”. See kujutab olukorda, kus teenuse või tellimusega liitumine on kerge või odav, kuid tühistamine on oluliselt keerukam, misõttu kasutajad võivad tühistamisest loobuda või pikema perioodi eest maksta, kui algselt plaanitud.⁷⁴

Näiteks keerukast tühistamisest on võtted, mis lubavad tühistamist vaid ebamõistlikult vara enne tellimuse lõppemist või nõuavad füüsilise kirja saatmist või füüsiliselt ettevõttesse kohale tulekut tellimuse lõpetamiseks.

1.5.9. Peidetud kulud

Peidetud kulude tume muster ootab toote koguhinna esitamisega, kuni huvitatud ostja on aega ja vaeva näinud ning ostuprotsessi lõpetamas.⁷⁵ Näiteks tundub lennupilet konkurendiga võrreldes odav, kuid peale dokumentide andmete sisestamist ilmnevad üksteise järel erinevad tasud, mida reklaamitud hind ei kajastanud kuid millest loobuda ei saa.

1.5.10. Peidetud tellimus

Peidetud tellimus kujutab kasutaja teadmata talle jätkuva tellimuse müüki. Kasutajale ei saadeta teateid tema makstava tellimuse kohta, et vältida tellimuse tühistamist ja maksete lõppemist.⁷⁶

⁷³ Brignull, H., Leiser, M., Santos, C., & Doshi, K. (2023, April 25). *Deceptive patterns – user interfaces designed to trick you*. deceptive.design. Retrieved 27.03.2025, from <https://www.deceptive.design/types>

⁷⁴ Brignull, H., Leiser, M., Santos, C., & Doshi, K. (2023, April 25). *Deceptive patterns – user interfaces designed to trick you*. deceptive.design. Retrieved 27.03.2025, from <https://www.deceptive.design/types>

⁷⁵ Brignull, H., Leiser, M., Santos, C., & Doshi, K. (2023, April 25). *Deceptive patterns – user interfaces designed to trick you*. deceptive.design. Retrieved 27.03.2025, from <https://www.deceptive.design/types>

⁷⁶ Brignull, H., Leiser, M., Santos, C., & Doshi, K. (2023, April 25). *Deceptive patterns – user interfaces designed to trick you*. deceptive.design. Retrieved 27.03.2025, from <https://www.deceptive.design/types>

1.5.11. Näägutamine

Näägutamine kujutab tumedat mustrit, mis segab kasutajat muude tegevuste sooritamisel palvetega midagi muud teha.⁷⁷

Näiteks on Instagram kasutajaid näägutanud, et nad oma mobiiltelefonis Instagrami saadetavad teavitused sisse lülitaksid, pakkudes keelduvaks variandiks vaid valikut “mitte praegu”.⁷⁸

1.5.12. Takistus

Takistuse tume muster teeb mingi protsessi nimelt kasutaja jaoks raskemaks, et vähendada tõenäosust, et kasutaja protsessi edukalt lõpetab.⁷⁹ Näiteks võib soovitud privaatsusvaliku peita sügavale privaatsusmenüüdesse, kust kasutaja seda hõlpsasti üles ei leia. Või näiteks panna kasutaja klikkima eraldi ruudukest iga reklaamifirma kohta, kellega ta ei soovi oma andmeid jagada.

1.5.13. Eelvalimine

Eelvalimisega on tegemist, kui kasutajale esitatakse vaikimisi ära märgitud valik. Kasutaja ei pruugi valiku tingimustesse süveneda või võib usaldada, et tema eest on tehtud populaarseim või kõige kasulikum valik.⁸⁰ Eelvalimise tumedat mustrit kasutatakse tihti näiteks küpsiste nõusoleku kogumisel.

1.5.14. Hiilimine

Hiilimise tume muster kujutab olukorda, kus kasutajale olulist infot peidetakse tema eest või viivitatakse selle jagamisega, et mõjutada teda tegema tehingut, mida ta kogu infot teades

⁷⁷ Brignull, H., Leiser, M., Santos, C., & Doshi, K. (2023, April 25). *Deceptive patterns – user interfaces designed to trick you*. deceptive.design. Retrieved 27.03.2025, from <https://www.deceptive.design/types>

⁷⁸ Brignull, H., Leiser, M., Santos, C., & Doshi, K. (2023, April 25). *Deceptive patterns – user interfaces designed to trick you*. deceptive.design. Retrieved 27.03.2025, from <https://www.deceptive.design/types>

⁷⁹ Brignull, H., Leiser, M., Santos, C., & Doshi, K. (2023, April 25). *Deceptive patterns – user interfaces designed to trick you*. deceptive.design. Retrieved 27.03.2025, from <https://www.deceptive.design/types>

⁸⁰ Brignull, H., Leiser, M., Santos, C., & Doshi, K. (2023, April 25). *Deceptive patterns – user interfaces designed to trick you*. deceptive.design. Retrieved 27.03.2025, from <https://www.deceptive.design/types>

teinud poleks. Hiilimise variantideks on näiteks nn. ostukorvi hiilimise muster, mille käigus lisatakse ostuprotsessi lõpus ostukorvi lisatoode, või ka reklaamitud toote äravahetus teise tootega.⁸¹

1.5.15. Eksitav sõnastus

Eksitava sõnastuse tume muster kasutab ära asjaolu, et veebilehe külastajad loevad tihti tekste kiiruga ning ei pruugi süveneda sõnastusse piisavalt, et selle reaalsel tähendust tuvastada.⁸²

Eksitava sõnastuse tumeda mustri näiteks on ka olukorrad, kus keeldumist sõnastatakse topelteitusega: “Ma ei soovi, et minu infot ei jagataks partnerettevõtetega.”

1.5.16. Visuaalne takistus

Visuaalse takistuse tumeda mustri on tegu juhul, kui kasutajale vajalik teave on veebilehel teoorias olemas, kuid praktikas visuaalselt peidetud või varjatud tema eest.⁸³

Näiteks võib veebileht olulise info edastada halvastiloetavas pisikes kirjas, mis ka värvi poolest ei eristu taustast,⁸⁴ või paigutada selle informatsiooni veebilehe alumisse äärde, kuhu kasutaja ei pruugi kerida.

1.6. Tumede mustrite liigitamine

Peale tumede mustrite mõiste sõnastamise on tehtud ka mitmeid kaitseid tumedaid mustreid liigitada⁸⁵, kuid seegi on osutunud keeruliseks. On levinud arusaam, et kõikehõlmavat ja põhjalikku liigitust tumedatest mustritest pole võimalik teha, kuna pidevalt mõeldakse uusi

⁸¹ Brignull, H., Leiser, M., Santos, C., & Doshi, K. (2023, April 25). *Deceptive patterns – user interfaces designed to trick you*. deceptive.design. Retrieved 27.03.2025, from <https://www.deceptive.design/types>

⁸² Brignull, H., Leiser, M., Santos, C., & Doshi, K. (2023, April 25). *Deceptive patterns – user interfaces designed to trick you*. deceptive.design. Retrieved 27.03.2025, from <https://www.deceptive.design/types>

⁸³ Brignull, H., Leiser, M., Santos, C., & Doshi, K. (2023, April 25). *Deceptive patterns – user interfaces designed to trick you*. deceptive.design. Retrieved 27.03.2025, from <https://www.deceptive.design/types>

⁸⁴ Brignull, H., Leiser, M., Santos, C., & Doshi, K. (2023, April 25). *Deceptive patterns – user interfaces designed to trick you*. deceptive.design. Retrieved 27.03.2025, from <https://www.deceptive.design/types>

⁸⁵ Luguri and Strahilevitz 2021

mustreid ja võtteid välja ning iga liigitus põhineb liigitaja vajadustel.⁸⁶ Sellegipoolest on mitmete erinevate aspektide järgi liigitusi tehtud.

Näiteks on Euroopa Komisjoni 2022. aasta uuringus on välja pakutud uus käitumisökonomikal baseeruv võimalikult kõikehõlmav tumedate mustrite liigitus, mis põhineb kahel aspektil: millist valikarhitektuuri komponenti tume muster puudutab ning millise valiku tegemise komponendi kaudu üritatakse tarbija käitumises muutust saavutada.⁸⁷

Eelmainitud liigituse valikarhitektuur koosneb kolmest komponendist:

- a) valiku tegemise keerukuse suurendamisest, näiteks sundides tarbijat muutma vaikimisi märgitud valikuid oma huvidega vastavusse viimiseks;
- b) hinna keerukuse suurendamisest, näiteks avaldades hinna komponendid ja lisatasud järk-järgult ostu sooritamise protsessi jooksul;
- c) toote omaduste keerukuse suurendamisest, näiteks peites toote või teenuse funktsiooni kasutaja jaoks ootamatusse kohta.⁸⁸

Valiku tegemises muutust taotlevateks komponentideks on kasutaja eelarve piirangu mõjutamine, mille all võib silmas pidada ka näiteks ajalist eelarvet, ja toote eelistuste mõjutamine.⁸⁹ See taksonoomia on sobilik tumedate mustrite liigituseks ärilises kontekstis, kus tarbija läheb mingit ostu sooritama ning mustrist tulenevat kahju saab materiaalses mõttes hinnata.

Leiser ja Santos on tumedad mustrid jaotanud kolmeastmelise hierarhiaga taksonoomiasse nende nähtavuse alusel.⁹⁰ Need kolm astet on nähtavuse kahanemise järjekorras:

- a) nähtavad tumedad mustrid, mille mõju kasutajale on kergesti tuvastatav, nagu näiteks vaikimisi märgitud valikud;
- b) tumedamad mustrid, mida kasutaja ei märka ning mis võivad vajada mustri tuvastamiseks eksperte, näiteks nõusoleku andmata jätmise valiku peitmine erinevate kasutajaliidese elementide taha;

⁸⁶ OECD. Dark commercial patterns. 2022. Lk 11.

⁸⁷ EC Study 2022 +++ Lk. 35.

⁸⁸ EC Study 2022 +++ Lk. 35.

⁸⁹ EC Study 2022 +++ Lk. 35.

⁹⁰ Leiser, Dr Mark and Santos, Cristiana, Dark Patterns, Enforcement, and the Emerging Digital Design Acquis: Manipulation beneath the Interface, Vol. 15 No. 1 (2024): BILETA Special Issue. Lk. 5. Available at SSRN: <https://ssrn.com/abstract=4431048>

c) kõige tumedamad mustrid, mis viivad läbi kõige salakavalamaid kasutaja mõjutamisi, põhinevad keerukatel algoritmidel ning jagunevad omakorda kaheks:

- i) deterministlikeks mustriteks, mille puhul on kasutajale suunatud negatiivne mõju ette määratud, ning mis kasutab eesmärkide saavutamiseks ära kasutaja kognitiivseid nihkeid ning nende kohta kogutud andmetest tuvastatavaid haavatavusi;
- ii) stohhastilisteks mustriteks, mille puhul pole kasutajale suunatud negatiivne mõju ette määratud, muster suudab kohaneda kasutaja käitumisega ning süsteemi opereerimispõhimõtted on keeruline tuvastada.⁹¹

Võrreldes Euroopa Komisjoni tarbija õigustele suunatud liigitusega, on Leiseri ja Santose taksonoomia sobilikum tehisintellektil põhinevate tumedate mustrite hindamiseks, kuna eristab neid nii tuvastavuse kui ka võimete poolest, mis on ka minu tehisintellekti põhiste tumedate mustrite käsitlemise aluseks, ning seetõttu võtan selle kolmeastmelise hierarhia aluseks ka oma mudeli koostamisel 3. peatükis.

⁹¹ Leiser, Dr Mark and Santos, Cristiana, Dark Patterns, Enforcement, and the Emerging Digital Design Acquis: Manipulation beneath the Interface, Vol. 15 No. 1 (2024): BILETA Special Issue. Lk. 5. Available at SSRN: <https://ssrn.com/abstract=4431048>

2. ÜLEVAADE TUMEDATE MUSTRITE KÄSITLUSEST EUROOPA LIIDU ÕIGUSES

Olemasolevad õigusaktid, mis tumedate mustrite hulka kuuluvaid võtteid digikontekstis käsitlevad, teevad seda laias laastus kahel viisil. Esimeseks on taunitavate teguviiside abstraktsem loetlemine, nagu seda tehakse näiteks digiteenuste määruse 25. artikli esimeses lõikes: “Digiplatvormide pakkujad ei disaini, korralda ega käita oma internetipõhiseid kasutajaliideseid viisil, mis petab nende teenuse saajaid või manipuleerib nendega või viisil, mis muul viisil moonutab oluliselt või kahjustab nende teenuse saajate võimet teha sõltumatuid ja teadlikke otsuseid.” See lähenemine jätab laia subsumeerimisruumi ka tulevikus väljamõeldavate ebaetiliste praktikate puhul normi kohaldamiseks.

Teiseks variandiks on konkreetsete tumedate mustrite loetlemine, nagu sama määruse 25. artikli kolmandas lõikes, mis toob välja komisjoni pädevuse anda välja suuniseid konkreetsete tavades suhtes – näiteks teenuse lõpetamise etapi keerukamaks tegemine, kui seda oli kasutajaks registreerumine. Selline konkreetne väljatoomine jätab vähem ruumi diskussiooniks, kas kasutajaliides on manipuleeriv, kas tarbija võimekust teha teadlikke otsuseid on kahjustatud, jne. Samuti teeb see mustri keelatus *ex ante* hindamise oluliselt lihtsamaks, kuna sõltub konkreetse võtte olemasolu hindamisest, mitte selle mõjust kasutajale. Kuid selline konkreetse võtte täpne kirjeldamine võib uute tehnoloogiliste arengutega kiiresti iganeda.

Seetõttu on tumedate mustrite käsitlemisel otstarbekas kasutada mõlemat varianti kombineeritult, nagu seda teeb näiteks ebaausate kaubandustavade direktiiv: kaubandustavad jagatakse abstraktsemate kriteeriumite alusel eksitavateks ja agressiivseteks ning direktiivi lisa sisaldab üksikasjalikumat nimekirja igal juhul ebaausatest kaubandustavadest.

Käesolev peatükk annab kronoloogilises järjestuses ülevaate erinevatest tarbijakaitset, tehisintellekti ja andmekaitset puudutavatest Euroopa Liidu direktiividest ja määrustest, mis otseselt või kaudselt reguleerivad digiplatvormidel leiduvaid tumedaid mustreid. Kõik neist kujutavad olulisi värskendusi varasemalt kehtinud õigusaktidele. Suures osas piiravad tumedate mustrite kasutamist siiani tarbijate õiguste kaitset käsitlevad õigusaktid, mida on

mõnel juhul ka uuendatud, et hõlmata konkreetseid digikeskkonnas levinud tumedaid mustreid.⁹²

2.1. E-privaatsuse direktiiv

Vanimaks õigusaktiks on Euroopa Parlamendi ja Nõukogu direktiiv 2002/58/EÜ⁹³, mis käsitleb isikuandmete töötlemist ja eraelu puutumatuse kaitset elektroonilise side sektoris, tuntud ka kui e-privaatsuse direktiiv. Tumedaid mustreid laiemalt direktiiv ei käsitle, küll aga näeb ette, et info salvestamine kasutaja seadmele peaks toimuma kasutaja eelneva nõusolekuga.⁹⁴ See mõjutab muuhulgas ka küpsiste salvestamist, v.a. küpsiseid, mis on vajalikud kasutaja poolt valitud teenuse teostamiseks, näiteks e-poes ostukorvi salvestamiseks. Peale praktilise ja vajaliku külje kujutavad küpsised ka ohtu isiku isiku privaatsusele, võimaldades profileerimist, jälgimist erinevatel külastatavatel veebilehtedel jms. Kogutud infot saab edasi kasutada erinevate tumedate mustrite välja töötamises ning konkreetsele isikule kohandamises.

Veel annab eelmainitud direktiiv suunised pealesunnitud teabe reguleerimiseks.⁹⁵ Pealesunnitud teabena kirjeldatakse inimsekkumist mittevajavaid automatiseeritud sidesüsteeme, mis teevad või saadavad automaatkõnesid, fakse või e-maile, mille saamiseks kasutaja pole nõusolekut andnud. Tuuakse välja, et peale otseturunduseks eelneva nõusoleku andmise peaks kliendil ka olema selge, lihtne ja tasuvaba võimalus keelata elektrooniliste kontaktandmete edasine kasutamine. Seeläbi käsitleb direktiiv ka levinud “keeruka tühistamise”⁹⁶ tumedat mustrit, ehk olukorda, mil teenusega liitumine on oluliselt kergem ja mugavam, kui sellest loobumine.

Lisaks direktiivile on komisjon 2017. aastal vastu võtnud ka e-privaatsuse määruse eelnõu⁹⁷, mille järgi koostatava määruse jõustumisega tunnistatakse kehtetuks praegune e-privaatsuse

⁹² Fitness check. Lk 55.

⁹³ EUROOPA PARLAMENDI JA NÕUKOGU DIREKTIIV 2009/136/EÜ, 25. november 2009, <https://eur-lex.europa.eu/legal-content/ET/TXT/HTML/?uri=CELEX:32009L0136>

⁹⁴ E-privaatsuse direktiiv, art 5 lg 3, preambuli põhjendus 25.

⁹⁵ E-privaatsuse direktiiv art 13

⁹⁶ Hard to cancel/ opt out. OECD lk 8.

⁹⁷ Määruse ettepanek, mis käsitleks privaatsust ja elektroonilist side. 10.01.2017. <https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-privacy-and-electronic-communications>

direktiiv. See keskendub elektroonilise side teenuse pakkujatele Euroopa Liidus, kes töötlevad suhtlusinfot, nagu näiteks WhatsApp, Facebook Messenger jne. Määrus on planeeritud tagama elektrooniliste sideteenuste kasutajatele traditsiooniliste telekommunikatsioonioperaatorite kasutajatega võrdse kaitse ning harmoniseerima e-privatsuse direktiivist tulenevad põhimõtted ja sätted vahepeal jõustunud isikuandmete kaitse üldmäärusega.⁹⁸

Tumede mustrite kontekstis on eelnõust asjakohane osa, mis puudutab küpsiste salvestamist ja nende lubamist. Eelnõu toob põhjendustes välja, et sideteenuste lõppkasutajad on üle koormatud pidevate küpsiste salvestamist puudutavate nõusoleku andmise palvetega ja pakub välja lihtsustatud ja kasutajasõbraliku küpsiste salvestamise mudeli. Selle kohaselt võiks määrusega anda kasutajatele võimalus väljendada nõusolekut küpsiste talletamiseks läbi veebibrauseri või muu rakenduse sätete, mis oleksid kolmandate osapoolte jaoks siduvad. Kasutaja valiks näiteks brauseri installeerimise ajal erineva tasemega privaatsusseadete hulgast endale sobivaima ning brauser edastaks kasutaja eelistuse veebilehele, lubades või keelates automaatselt erineva eesmärgiga küpsised.⁹⁹

See lähenemine ennetaks mitmeid erinevaid tumedaid mustreid, mida kasutatakse, et veebilehe külastajat veenda, eksitada või sundida küpsiseid vastu võtma – nagu näiteks näägutamine¹⁰⁰, ehk korduv sätetega nõustumise palumine, või võlts hierarhia¹⁰¹, ehk eksitava kujundusega keeldumis-ja vastuvõtmisnupud. Teiseks viib selline lähenemine privaatsusseadete üle otsustamise hetke, mille kasutaja on valinud oma veebibrauseri seadistamiseks. Seetõttu on parem tõenäosus, et kasutajal on huvi ja aega süveneda privaatsustingimuste olemusse ja teha teadlik valik.

See vastandub hetkel kehtivale süsteemile, kus küpsiste nõusoleku palve on teisejärgulise tähtsusega vahelesegajaks põhitegevusele, mille eesmärgil kasutaja veebilehe avanud on. Kolmanda praktilise kaalutlusena eemaldaks privaatsussätete etteseadistamine brauseris ajaakna, mil veebileht on ekraanile laetud, kuid kasutaja pole veel küpsiste sätteid läbi

⁹⁸Euroopa Andmekaitsekoostöögrupi avaldus e-privatsuse määruse läbivaatamise ja selle mõju kohta üksikisikute kaitsele seoses nende elektroonilise side puutumatus ja konfidentsiaalsusega. 25.05.2018. https://www.edpb.europa.eu/our-work-tools/our-documents/statements/statement-edpb-revision-privacy-regulation-and-its-impact_en

⁹⁹Eelnõu punkt 22-23, lk 17

¹⁰⁰Nagging ing. k. OECD Lk 25.

¹⁰¹False hierarchy ing k. OECD Samas Lk 17.

lugenud ega valikut teinud. Etteseadistatuse korral saaks veebileht kasutaja privaatsuseelistusi arvesse võtta juba veebilehe algsel laadimisel.

2.2. Ebaausate kaubandustavade direktiiv

Teiseks antud töö kontekstis asjakohaseks direktiiviks on Euroopa Parlamendi ja Nõukogu direktiiv 2005/29/EÜ, mis käsitleb ettevõtja ja tarbija vaheliste tehingutega seotud ebaausaid kaubandustavasid, edaspidi lühidalt ebaausate kaubandustavade direktiiv. Võrreldes e-privaatsuse direktiiviga ei piirdu see direktiiv konkreetsete võtete piiramisega ning käsitleb tumedaid mustreid laiemalt, võttes sihikule kaubandustavad, “mis on otseselt seotud tarbija poolt toodete suhtes tehtavate tehinguotsuste mõjutamisega”.¹⁰² Kuigi direktiiv keskendub eeskätt kaubanduse ja turustamisega seotule, kohalduvad paljud selles toodud põhimõtted ebaausate tavade hindamiseks erinevatele tumedatele muustritele.¹⁰³

Seda seetõttu, et direktiiv defineerib kaubandustavasid kui “ettevõtjapoolne tegevus, tegevusetus, teguviis või esitusviis, kommertsteadaanne, sealhulgas reklaam ja turustamine, mis on otseselt seotud toote reklaamimise, müügi või tarnimisega tarbijatele”¹⁰⁴, kusjuures reguleerimisala hõlmab tarbija ja ettevõtja vahelisi tehinguotsuseid enne toote või teenusega seotud äritehingu tegemist, peale äritehingu tegemist ning selle tegemise ajal.¹⁰⁵ Tehinguotsuse all mõeldakse tarbija mis tahes otsust toote ostmise, õigusvahendite kasutamise, tegutsemise või tegutsemisest hoidumise kohta.¹⁰⁶

See tähendab, et tehinguotsus, mida tarbija ebaausa mõjuta teinud poleks, võib olla ka vaid poodi sisenemine.¹⁰⁷ Tegemist on eriti laia mõistega, mis ei vaja tingimata lepingulist suhet ega toote ostu, et kohalduda.¹⁰⁸ Seega hõlmab ebaausate kaubandustavade definitsioon lisaks

¹⁰² preambul 7.

¹⁰³ EC study 2022 lk 70

¹⁰⁴ UCPD Art 2 punkt d

¹⁰⁵ Samas UCPD Art 3 lg 1

¹⁰⁶ UCPD art 2 punkt k

¹⁰⁷ Trento Sviluppo srl, Centrale Adriatica C-281/12 p 35-38
<https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62012CJ0281>

¹⁰⁸ EC study 2022 lk 70

ka tumedaid mustreid, mis seisnevad tarbija käitumise mõjutamises üldisemalt – näiteks reklaami või lingi klikkimine, teenuse kasutamise jätkamine või lõputult edasi sirvimine.¹⁰⁹

Peale laia *ratione materiae* on ebaausate kaubandustavade direktiivil veel üks äärmiselt tarbijasõbralik lähenemine. Nimelt lähtub see keskmise tarbija mõistest ning ei sea tingimuseks, et konkreetse tarbija käitumist oleks moonutatud – piisab tõenäosusest, et keskmine tarbija on ebaausalt mõjutatud tegema otsust, mida ta muul juhul teinud poleks.¹¹⁰ Samuti ei ole Euroopa kohus antud direktiivi kontekstis üldjuhul pidanud vajalikuks mõju keskmisele tarbijale hinnata ekspertarvamuse või tarbijauuringute kaudu, vaid on lihtsalt lähtunud mõistlikult informeeritud, tähepaneliku ja kriitilise keskmise tarbija eeldatavatest ootustest.¹¹¹¹¹²

Keskmise tarbija instrumendi kasutamise tõttu on ebaausate kaubandustavade direktiivi ka kritiseeritud. Nimelt on problemaatiline, et tavade ebaausust mõõdetakse keskmise tarbija standardi järgi, kuna see jätab välja tavad, mis mõjutavad ebaproportsionaalselt standardist mõnevõrra allapoole jäävaid tarbijad, kes on ka keskmisest haavatavamad.¹¹³¹¹⁴

Direktiivi viienda artikli 3. punktis on seda puudujääki ka korrigeeritud, seades erandina haavatavate tarbijarühmade mõjutamise korral standardiks selle haavatava grupi keskmise esindaja. Haavatavateks loetakse tarbijaid, kes oma vaimse või füüsilise puude, vanuse või kergeusklikkuse tõttu on eriti vastuvõtlikud nende majanduskäitumise moonutamisele. Autorile jääb siinkohal segaseks, kuidas täpsemalt sisustada keskmise kergeuskliku standardit ning puudub ka sellekohane kohtupraktika.

Teisest küljest, juhul kui see keskmise kergeuskliku tarbija mõiste sisustataks, võiks sellest olla kasu ka tumedate mustrite ebaaususe hindamisel, kuna kergeusklikke või digikeskkonnas

¹⁰⁹ Guidance on the interpretation and application of Directive 2005/29/EC of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in the internal market lk 32 (Text with EEA relevance) (2021/C 526/01) <https://op.europa.eu/en/publication-detail/-/publication/c608ff7-687a-11ec-9136-01aa75ed71a1/language-en>

¹¹⁰ Samas Lk 32

¹¹¹ c-210/96 p 31. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:61996CJ0210>

¹¹² Guidance on the interpretation and application of Directive 2005/29/EC of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in the internal market lk 32 (Text with EEA relevance) (2021/C 526/01) <https://op.europa.eu/en/publication-detail/-/publication/c608ff7-687a-11ec-9136-01aa75ed71a1/language-en>

¹¹³ OECD lk 16.

¹¹⁴ Vulnerable consumers briefing 2021 Nikolina Šajn European Parliamentary Research Service Lk 2

kergeusklikult käituvaid isikuid võib mõiste definitsioonist olenevalt olla rohkem, kui muude direktiivis kaitstud haavatavate gruppide esindajaid. Kui kaubandustava ebaaususe hindamisstandardiks on keskmiselt mõistlik, tähelepanelik ja kriitiline isik, siis kaitseb see tarbijaskonna ülemist poolt, kes oma keskmisest veelgi parema tähelepanelikkuse, mõistlikkuse ja kriitilisusega saab paremini vältida endale kahjulike otsuste tegemist. Samas mõnevõrra alla keskmise tähelepanelikud tarbijad jäetakse kaitseta. Muidugi on selles osas teisel kaalukaasil ärimine huvi ning pole mõistlik piirata kogu ettevõtlusvabadust ühe grupi võimaliku valesti mõistmise või tõlgendamise tõttu.

Direktiivi 5. artikkel seab üldklausliks, et kaubandustava on ebaaus, kui see on vastuolus ametialase hoolikuse nõuetega ja moonutab tõenäoliselt oluliselt keskmise tarbija majanduskäitumist. Sama artikli neljas punkt liigitab ebaausad kaubandusvõtted kaheks: esmalt agressiivseteks ja eksitavateks tavadeks, millest viimased omakorda jagunevad eksitavateks tegevusteks ja eksitavateks tegevusetusteks.¹¹⁵

Agressiivsete kaubandustavade alla kuuluvad võtted nagu ahistamine; sund, k.a. füüsilise jõu läbi ning tarbija liigne mõjutamine.¹¹⁶ See liigitus on nii kattuv tumedate mustritega, et Leiser ja Yang on selle võtnud aluseks oma tumedate mustrite liigituse loomisel.¹¹⁷ Ka Euroopa Komisjoni 2022. aasta uuringus on koostatud tumedate mustrite taksonoomia, mis põhineb eksitavatel ja agressiivsetel võtetel.¹¹⁸

Lisaks toob direktiiv esimeses lisas ära ka loetelu tavadest, mis on ebaausad kõigil tingimustel ning mille keelatus ei vaja seetõttu põhjalikku hindamist. Kuigi kogu direktiivi ülevõtmine on olnud harmoniseeritud, on selle loetelu puhul nõutud otsene ülevõtmine liikmesriikide poolt, ning loetelu võib muuta vaid direktiivi muutmisega.¹¹⁹ Mitmed neist tavadest kujutavad konkreetseid tumedaid mustreid, nagu näiteks seitsmes tava: “Vale väide, et toode on saadaval ainult väga piiratud aja jooksul [...]” – tegemist on võltsi nappusega.

¹¹⁵UCPD art 5-9, vt ka preambul 14-16.

¹¹⁶Samas.

¹¹⁷ Leiser & Yang ++ Lk 14

¹¹⁸ EC study LK 38

¹¹⁹ Behavioral study EC 2022? Lk 71.
<https://op.europa.eu/en/publication-detail/-/publication/606365bc-d58b-11ec-a95f-01aa75ed71a1/language-en>

Agressiivsete kaubandustavade loetelu 26. punkti on Euroopa Kohus käsitlenud ka 2021. aasta eelotsuses, mis puudutas reklaamsõnumite kuvamist päris e-kirjadele sarnaneval kujul ja nende hulgas kasutaja elektronpostkastis, mis loeti järjekindlaks ja soovimatuks pakkumise tegemiseks ning ebaausaks kaubandustavaks antud direktiivi lisa 26. punkti kontekstis.¹²⁰ Kuna tegemist on ühtlasi alajaotuses 1.5.3. käsitletud peidetud reklaami tumeda mustriga, kujutab see eelotsus näidet ebaausate kaubandustavade direktiivi kohaldamisest digitaalkontekstis leitava tumeda mustri kohta.¹²¹

Kokkuvõtlikult on ebaausate kaubandustavade direktiivi näol tegemist laiaulatuslikult tumedaid mustreid reguleeriva õigusaktiga, mis on mõjutanud tugevalt nii tumedate mustrite liigitust kui ka hilisemaid tumedaid mustreid käsitlevaid õigusakte, nagu näiteks antud töö kontekstis olulisimat tehisintellekti määrust¹²² ja digitaalteenuste määrust¹²³.

2.3. Tarbija õiguste direktiiv

Kolmandaks antud töö kontekstis asjakohaseks direktiiviks on Euroopa Parlamendi ja Nõukogu direktiiv 2011/83/EL¹²⁴, mis käsitleb tarbija õigusi lepingu sõlmimisel üldisemalt. Peale äriruumides ja äriruumidest väljas sõlmitud lepingute käsitlemise, käsitleb direktiiv ka kauglepinguid. Digiplatvormidel sõlmitud lepingud kuuluvad kauglepingute alla, kuna tarbija ja kaupleja pole füüsiliselt kohal ning kasutatakse lepingu sõlmimiseni kaugsidevahendit ehk selles kontekstis internetivõrku. Seetõttu on direktiiv relevantne ka digikeskkonnas toimuvate tarbija vaba valiku mõjutuste hindamiseks. Tumedaid mustreid laiemalt direktiiv ei nimeta ega muu nime all puuduta, küll aga reguleerib mõnda konkreetset kaubandusvõtet, mida on uuringutes liigitatud tumedaks mustriks.

¹²⁰ C-102/20 StWL Städtische Werke Lauf a.d. Pegnitz. Punktid 64-75. <https://eur-lex.europa.eu/legal-content/ET/TXT/HTML/?uri=CELEX:62020CJ0102>

¹²¹ Digital fairness check Lk 148.

¹²² Tehisintellekti määruse preambuli 29. põhjendus selgitab, et TI määruses sisalduvad keelud tehisintellekti kasutamiseks on komplementaarsed ebaausate kaubandustavade direktiiviga.

¹²³ Digiteenuste määrus täpsustab preambuli 67. põhjenduses, et selles sisalduvad piirangud kehtivad tumedatele mustritele, mis pole juba kaetud ebaausate kaubandustavade direktiivi või isikuandmete kaitse üldmäärusega.

¹²⁴ Euroopa Parlamendi ja Nõukogu direktiiv 2011/83/EL <https://eur-lex.europa.eu/legal-content/ET/TXT/HTML/?uri=CELEX:32011L0083>

Esiteks rõhutab direktiiv kauglepingute ja väljaspool äriruume sõlmitud lepingute puhul läbipaistvust kogukulude arvutamisel ja näitamisel tarbijale.¹²⁵ Kogukulude, s.o. maksude, transpordi hinna, teenusetasu jms, võimalikult varakult tarbijale näitamine reguleerib “peidetud kulude” tumedat mustrit, mille käigus kauba tõelist hinda tarbijale näidatakse alles maksmisprotsessi käigus.¹²⁶

Peale kogukuludest teavitamise sisaldab tarbija õiguste direktiivi 6. artikkel ka teisi kauglepingute puhul kehtivaid tarbija teavitamisnõudeid. Nimelt peab kaupleja tarbijat selgelt ja arusaadavalt teavitama toote omadustest, kaupleja isikust ja asukohast, kauba eest maksmise ja tellimuse tarnimise korrast jne. Sellise üldise selguse ja arusaadavuse nõude vastu eksivad tumedad mustrid, mis kasutavad tarbijat segadusse ajavat sõnastust, kujundust või teabe peitmist.

Näitena sellisest mustrist on Poola konkurentsi ja tarbijakaitse amet 2024. aastal trahvinud Amazon EU SARL-i 31 miljoni Poola zloti väärtuses tarbijate eksitamise tõttu. Nimelt esitas ostuplatvorm tarbijatele võltsi teavet toodete vähese saadavuse ja kohaletoimetamise kiiruse osas, mis pole kooskõlas tarbija selge ja arusaadava teavitamise põhimõttega – tegemist on alajaotuses 1.5.4. käsitletud võltsi nappuse tumeda mustriga. Samuti esitas ostuplatvorm halvasti loetavas hallis kirjas valgel taustal teabe, et ostuleping loetakse sõlmituks alates kauba teelevanekust, mitte kauba eest maksmisest.¹²⁷ See on vastuolus tarbija selge teavitamise põhimõttega ning kujutab visuaalse häire tumedat mustrit, kuna vajalik informatsioon oli küll kirjas, kuid peideti tarbija eest seda visuaalselt raskemini kättesaadavaks tehes.

Lisaks sätestab direktiiv 22. artiklis nõude, et tarbijalt igasuguse lisatasu võtmiseks, mis lisanduks peamise lepingulise kohustuse eest kokku lepitud tasule, on vajalik tarbija sõnaselge nõusolek sellise lisatasuga. Veelgi täpsemalt on tarbijal õigus selline lisatasu tagasi saada, kui kaupleja on järeldanud tarbija nõusolekut talle esitades “vaikimisi valikuid, mille tarbija peab tagasi lükkama, et vältida lisatasu maksmist”. Tegemist on alajaotuses 1.5.13. käsitletud “eelvalimise” tumeda mustriga, mille käigus esitatakse tarbijale juba ära valitud võimalused,

¹²⁵ Samas 2011/83/EL artikkel 6, lg 1 punkt e.

¹²⁶ EC Study 2022 Lk 73.
<https://op.europa.eu/en/publication-detail/-/publication/606365bc-d58b-11ec-a95f-01aa75ed71a1/language-en>

¹²⁷ Office of Competition and Consumer protection. Pln 31 million fine for Amazon. 2024.
<https://uokik.gov.pl/en/pln-31-million-fine-for-amazon>

näiteks tingimustega nõustumise puhul juba märgistatud kastid.¹²⁸ Tarbija ei pruugi seetõttu valiku olemasolu märgata või võib usaldada, et tegemist on enamike tarbijate poolt tehtud standardvalikuga või tema huvides pakutava valikuga – muidugi juhul, kui kasti märgistust saab üldse muuta ning valikuks nimetada. Samuti võib see säte kohalduda “peidetud tellimuse” tumedale mustriale, mille käigus tarbijale müüakse tellimust tema teadmata või selge nõusolekuta.

Tarbijakaitsenormide ajakohastamise käigus on tarbija õiguste direktiivi muudetud nn. “omnibuss” direktiiviga EL 2019/2161.¹²⁹ Muutustega täpsustati, et direktiiv kohaldub ka lepingutele, kus tarbija ei maksa teenuse eest tasu, vaid jagab selle asemel oma andmeid.¹³⁰ See muutus laiendas direktiivi kohaldumist digiplatvormidele, mille ärimudel põhineb kasutajate andmete kogumisel, tähelepanu hoidmisel ja muude teenuste vahendamisel – näiteks sotsiaalmeedia, otsingumootorid jne. See on oluline tumedate mustrite perspektiivist, kuna neid ei kasutata mitte vaid tarbija suunamiseks ostu soorituse poole, vaid ka näiteks tema andmete töötamise alase nõusoleku saamiseks.

Veel on välja pakutud nii tarbija õiguste direktiivi kui ka ebaausate kaubandustavade direktiivi osas, et need võiksid sisaldada üldist põhimõtet, mis keelab direktiivides toodud kohustustest kõrvale hiilimise, näiteks läbi lepinguliste tingimuste, tehniliste lahenduste või kasutaja valikuvabaduse mõjutamise, teisiti öeldes ka tumedate mustrite kasutamise kaudu.¹³¹¹³² Selline säte peegeldaks digiturgude määruks olevat samasisulist põhimõtet, mis rõhutab määruks tulenevate kohustuste täitmisele vastu töötamisest hoidumise tähtsust.¹³³¹³⁴

¹²⁸ Samas. Lk 73.

¹²⁹ EL 2016/679. Preambul 31-35. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32019L2161>

¹³⁰ EC study 2022 Lk 74
<https://op.europa.eu/en/publication-detail/-/publication/606365bc-d58b-11ec-a95f-01aa75ed71a1/language-en>

¹³¹ BEUC. 2022. “Dark patterns” and the EU Consumer Law acquis. Recommendations for better enforcement and reform. https://www.beuc.eu/sites/default/files/publications/beuc-x-2022-013_dark_patterns_paper.pdf

¹³² EC study 2022 Lk 74
<https://op.europa.eu/en/publication-detail/-/publication/606365bc-d58b-11ec-a95f-01aa75ed71a1/language-en>

¹³³ DMA artikkel 13 p 4, Preambul 70. <https://eur-lex.europa.eu/eli/reg/2022/1925/oj/eng>

¹³⁴ BEUC. 2022. “Dark patterns” and the EU Consumer Law acquis. Recommendations for better enforcement and reform. https://www.beuc.eu/sites/default/files/publications/beuc-x-2022-013_dark_patterns_paper.pdf

2.4. Isikuandmete kaitse üldmäärus

Asjakohastest määrustest kronoloogiliselt esimeseks on Euroopa Parlamendi ja Nõukogu määrus (EL) 2016/679, ehk edaspidi isikuandmete kaitse üldmäärus või GDPR. See rõhutab andmekorje ja -käitluse läbipaistvuse ja turvalisuse vajalikkust ning nõuab kasutaja vabalt antud teadlikku luba tema andmete kasutamiseks. Määruse asjakohasus antud töö kontekstis seisneb erinevates tumedaid mustreid ennetavates ja piiravates põhimõtetes, mis puudutavad isikuandmete käitlemist ning automaatsete otsuste tegemist.

Esiteks sisaldab isikuandmete kaitse üldmääruse 5. artikkel põhimõtet, et isikuandmete töötlus peab toimuma seadusega kooskõlas, õiglaselt ja läbipaistvalt. Õiglane töötlus tähendab, et isikuandmeid ei või töödelda kahjulikul, diskrimineerival, ettearvamatul või eksitaval viisil.¹³⁵ Läbipaistev töötlus tähendab, et töötlus ja sellega seonduv teave peab olema selge, arusaadav, lühike ja kergesti kättesaadav.¹³⁶ Seda nõuet rikuvad mitmed tumedad mustrid, näiteks teave andmine arusaamatus sõnastuses või teises keeles, mis liigitub alajaotuses 1.5.15. käsitletud “eksitava sõnastuse” tumeda mustri alla ning rikub läbipaistva töötluse põhimõtet.

Isikuandmete kaitse üldmääruse 7. artiklist tulenev vabatahtlikult antud nõusoleku põhimõte piirab selliste tumedate mustrite kasutamist, mis eksitaks, manipuleeriks või sunniks isikut oma andmete töötluseks nõusolekut andma. Näiteks on Euroopa Kohus Planet49 asjas leidnud, et kasutaja eest vaikimisi ära märgitud ruudud ei kujuta endast kehtivat nõusolekut. Lisaks vaikimisi märgitud ruutudele oli töötluseks nõusoleku andmata jätmine pikk protsess, kus kasutaja pidi 57 erinevat partnerettevõtet ükshaaval kustutama.¹³⁷¹³⁸ Esimesel juhul on tegemist 1.5.13. käsitletud eelvaliku tumeda mustriga ning teisel juhul alajaotuses 1.5.12. käsitletud takistust seadva tumeda mustriga. Nagu varem mainitud, esinevad tumedad mustrid tihti koos, avaldades kasutajale kumulatiivset mõju.¹³⁹

¹³⁵ EC Study 2022 Lk 76

¹³⁶ Samas. EC Study 2022 Lk 76

¹³⁷ Euroopa Kohtu otsus C-673/17. Punktid 59-63.
<https://eur-lex.europa.eu/legal-content/ET/TXT/HTML/?uri=CELEX:62017CJ0673>

¹³⁸ EC Study 2022 Lk. 78.

¹³⁹ Santos, Cristiana, Viktorija Morozovaite, and Silvia De Conca. 2025. “No Harm No Foul: How Harms Caused by Dark Patterns Are Conceptualised and Tackled under EU Data Protection, Consumer and Competition Laws.” *Information & Communications Technology Law*, February, Lk. doi:10.1080/13600834.2025.2461958.

Töö kontekstis tuleks mainida ka, et tumedate mustrite abil isikuandmete kaitse üldmäärusest tulenevatest kaitsenõuetest mööda hiilimine on nii levinud, et kasutajad ei pruugi eristada, millised praktikad nende õigusi rikuvad, või on leppinud oma andmete jagamisega kui paratamatusega.¹⁴⁰ Sellele probleemile on reageerinud näiteks Prantsusmaa andmekaitse alane järelvalveasutus CNIL, kes on 2022. aastal trahvinud populaarseid digiplatvorme Facebook ja Google, kuna nende küpsistega nõusoleku küsimised vajasisid nõustumiseks kasutajalt üht klikki, kuid keeldumiseks mitmeid.¹⁴¹ Tegemist on alajaotuses 1.5.12. kirjeldatud “takistuse” tumeda mustriga, kus soovitud tegevus tehakse kasutajale kiireks ja kergeks, kuid soovimatu tegevus aeglasemaks ja keerulisemaks.

Võrreldes eelnimetatud õigusaktidega on isikuandmete kaitse üldmäärusel olulise mõjuga roll just tehisintellekti kasutamise seotud tumedate mustrite puhul. Seda sellepärast, et GDPR piirab mitmeid tehisintellekti kasutavate tumedate mustrite aspekte: kogutavate isikuandmete hulka, kogumise tingimusi ja lubamist, töötluse eesmärke ning automaatsete otsuste tegemist. See pidurdab ja ennetab tehisintellekti kasutavate tumedate mustrite efektiivsust ja ulatust, näiteks reklaamide personaliseerimise ja kasutaja profileerimise puhul.

2.5. Digiteenuste määrus

Teiseks olulisemaks määruseks on 16. novembril 2022 jõustunud Euroopa Parlamendi ja Nõukogu määrus (EL) 2022/2065, mis käsitleb digiteenuste ühtset turgu, edaspidi digiteenuste määrus või DSA¹⁴² määrus. Töö seisukohast on see oluline, kuna sätestab väga suurte digiplatvormide terminoloogia ning suure kasutajaskonnaga kaasnevad kõrgendatud nõuded ja vastutuse. Samuti sisaldab DSA määrus esimest eksplitsiitset viidet tumedate mustrite terminile Euroopa Liidu õigusaktide hulgas ning eksitava või manipuleeriva kasutajaliidese disaini keeldu.

¹⁴⁰ EC study 2022. Lk 86

¹⁴¹ Deliberation of the restricted committee No. SAN-2021-023 of 31 December 2021 concerning GOOGLE LLC and GOOGLE IRELAND LIMITED https://www.cnil.fr/sites/cnil/files/atoms/files/deliberation_of_the_restricted_committee_no_san-2021-023_of_31_december_2021_concerning_google_llc_and_google_ireland_limited.pdf

¹⁴² Digital Services Act. Ing. k.

Digiteenuste määrus eristab muudest platvormidest väga suured digiplatvormid ehk VLOP-id¹⁴³ ja väga suured otsingumootorid ehk VLOSE-id¹⁴⁴. Need tähendavad platvorme, millel on Euroopa Liidus rohkem kui 45 miljonit kasutajat kuus, s.t rohkem kui 10% Euroopa Liidu elanikkonnast. Käesoleva aasta seisuga on neid platvorme ja otsingumootoreid kokku 25, kusjuures neist viiendiku moodustavad Google'i pakutavad teenused nagu otsingumootor, Youtube, äpipood jne.¹⁴⁵ Suure võimuga digiturul kaasneb suur vastutus ning digiteenuste määrus seab VLOP-idele ja VLOSE-dele kõrgemad standardid, kui väiksematele platvormidele, millel puudub selline kasutajaskond ja ühiskondlik mõju. Nimelt peavad suuremad digiplatvormid sooritama riskihindamisi ohtliku sisu osas, korraldama igaaastase sõltumatu auditeerimise, pakkuma kasutajatele profileerimisvaba soovitusüsteemi valikut, täitma kõrgemaid läbipaistvusnõudeid jms.

Veel ühe olulise nüansina eristab määrus 3. artiklis mõisteid defineerides teenusesaajaid tarbijatest. Tarbijate all peetakse silmas tavapäraselt tarbijakaitseõiguses kasutatavat mõistet, ehk on tegemist füüsiliste isikutega, kes tegutsevad väljaspool kaubandus-, ettevõtlus-, käsitööndus- ja kutsetegevust. Teenusesaajate all mõeldakse füüsilisi või juriidilisi isikuid, kes kasutavad vahendusteenust, eelkõige kas teabe otsimiseks või selle kättesaadavaks tegemiseks. Teisisõnu erinevalt tarbijakaitseõiguse alastest õigusaktidest, ulatub digiteenuste määrase kaitseala ka juriidiliste isikuteni. See on oluline, kuna võimaldab seeläbi ka juriidiliste isikute kaitset tumedate mustrite alla kuuluvate manipuleerivate ja eksitavate disainivõtete eest. Nagu nähtub ka eelnevate õigusaktide ülevaadetest, toetutakse tumedate mustrite keelamisel või piiramisel suuresti just tarbija õiguste kaitsele. Kuid tumedad mustrid võivad mõjutada nii füüsilisi kui juriidilisi isikuid, eriti kui tegemist on näiteks väikeettevõtjatega, kellel ei pruugi olla õiguslikku või tehnilist võimekust tuvastada, et konkreetne valik, mille poole neid suunatakse, ei ole nende parimates huvides.

Tumedate mustrite reguleerimise seisukohast on olulisim digiteenuste määrase 25. artikkel, mis keskendub digiplatvormide kasutajaliidese disainile ja korraldusele ning selliste manipulatiivsete või eksitavate disainivõtete keelamisele, mis võiksid mõjutada teenuse saaja võimekust vabasid ja teadlikke otsuseid teha. Sama artikli kolmas lõige jätab komisjonile võimaluse konkreetsete praktikate puhul suuniste välja andmiseks ning toob ka kolm

¹⁴³ *Very Large Online Platform*. Ing. k.

¹⁴⁴ *Very Large Online Search Engine*. Ing. k.

¹⁴⁵ <https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses>

konkreetses näidet manipuleerivast disainist, mille puhul võib suuniseid anda. Esimeseks näiteks on teatavate valikute esile tõstmine otsuse küsimise puhul, mis kujutab endast võltsi hierarhia tumedat mustrit. Teiseks näiteks on korduv häiriv taotlemine, et teenusesaaja teeks valiku, mille ta juba teinud on, mis vastab näägutamise tumedale mustrile. Kolmandaks näiteks on teenuse lõpetamise keerukamaks tegemine, kui teenusega liitumine, mis vastab raskendatud tühistamise tumedale mustrile.

Digiteenuste määruse 25. artikli teine lõige välistab manipuleeriva või eksitava kasutajaliidese disaini keelu kohaldumise praktikate puhul, mis on juba kaetud kas ebaausate kaubandustavade direktiiviga või isikuandmete kaitse üldmäärusega. See on tekitanud mõnevõrra segadust küsimuses, milliste praktikate puhul digiteenuste määrus üldse kohaldub, kuna ebaausate kaubandustavade direktiivi lai ja abstraktne käsitlus hoomab enamikke tarbijat manipuleerivaid või eksitavaid võtteid.¹⁴⁶

Siiski on Euroopa Komisjon digiteenuste määruse 25. artikli rikkumist ette heitnud X-ile, ehk varasema nimega Twitterile, kuna X kui väga suur online platvorm antud määruse mõistes hakkas kõigile soovijatele müüma siniseid kontrollmärke, mis varasemalt tähistasid tuntud isikute autentseid kontosid. See võttis platvormi kasutajatelt võimaluse teha teadlikke otsuseid selle kohta, kas konkreetne konto ja selle sisu on autentne.¹⁴⁷¹⁴⁸ Autori hinnangul on tegemist variandiga võltsi sotsiaaltõestuse tumedast mustrist, kuna märgi ostanud konto esineb X-i kasutaja jaoks eristamatuna usaldusväärsetest kontrolli läbinud kontodest.

Lisaks sisaldab digiteenuste määrus erinevaid läbipaistvusnõudeid, mis ennetavad spetsiifilisi tumeda mustri tüüpe. Näiteks sisaldab 26. artikkel nõuet, et digiplatvormi kasutajaliidestest esitatav reklaam peab olema igale teenusesaajale selgelt tuvastatav reklaamina. Sellise nõude vastu eksib peidetud reklaami tumeda mustri kasutamine.

Määruse 27. artikkel nõuab läbipaistvust ka soovitusüsteemide osas, mille kohaselt teenusesaajale peab selgitama, mis parameetrite alusel soovitusi tehakse ning millised on teenusesaaja võimalused neid parameetreid muuta või mõjutada. Väga suurtele

¹⁴⁶ Digital fitness check Lk 150.

¹⁴⁷ Komisjon saadab esialgsed järeldused X-le digiteenuste õigusakti rikkumise kohta. Pressiteade. 12. juuli 2024. https://ec.europa.eu/commission/presscorner/detail/en/ip_24_3761

¹⁴⁸ Digital fitness check Lk 150.

digiplatvormidele ja otsingumootoritele kohaldub 38. artiklist tulenev kõrgem standard ning nad peavad teenuse saajale andma vähemalt ühe valikuna sellise soovitusüsteemi, mis ei põhine tema profileerimisel. See lähenemine aitab vältida tumedaid mustreid, mis kasutavad profileerimist näiteks konkreetsele isikule teenusest sõltuvust tekitava sisu soovitamiseks.

Soovitusüsteemi on kirjeldatud digiteenuste määruse 3. artiklis kui “täielikult või osaliselt automatiseeritud süsteem, mida digiplatvorm kasutab selleks, et soovitada oma internetipõhises kasutajaliideses teenusesaajatele konkreetset teavet või prioritseerida seda, sealhulgas teenusesaaja algatud otsingu tulemusena või muul alusel kuvatava teabe suhtelist järjekorda või esiletõstmist määrates”. Seda definitsiooni võib kõrvutada tehisintellekti käsitleva määruse 3. artiklis sisalduva ning ka käesoleva töö esimeses peatükis mainitud tehisintellektisüsteemi mõistega. Järeldub, et digiteenuste määruse käsitletavad soovitusüsteemid liigituvad ühtlasi ka tehisintellektisüsteemiks tehisintellekti käsitleva määruse mõttes. Nimelt on ka soovitusüsteemid projekteeritud töötama erineval autonoomsuse tasemel ning järeldama saadud sisendist ehk teenusesaaja infost, tehtud valikutest jne, milliseid väljundeid genereerida, ehk soovitusüsteemi puhul soovitusi, mis võivad mõjutada virtuaalset keskkonda.

DSA määruse *ex ante* lähenemine soovitusüsteemidest tulenevatele võimalikele riskidele või ohtudele prioritseerib soovitusüsteemi läbipaistvust ja kontrollitavust teenuse saaja perspektiivist ning vähendab seeläbi informatsioonilist asümmeetriat, mis valitseb suurte digiplatvormide ja üksikisikute vahel. Sellega võrreldes lähtub TI määruse tehisintellektisüsteemi mõistega hõlmatud soovitusüsteem riskipõhisest lähenemisest, mis keskendub põhiõiguste ja turvalisuse kaitsesele olenevalt riski tasemest ja kahju tekkest.

2.6. Digiturgude määrus

Kolmandaks määruseks on 1. novembril 2022 jõustunud Euroopa Parlamendi ja Nõukogu määrus (EL) 2022/1925, mis moodustab eelkäsitletud digiteenuste määrusega harmoonilise terviku ning käsitleb konkurentsile avatud ja õiglaseid turge digisektoris, edaspidi digiturgude määrus või DMA¹⁴⁹ määrus. Digiturgude määrus keskendub digimaailma niinimetatud

¹⁴⁹ Digital Markets Act. Ing k.

päasuvalitsejatele, kes omavad olulisi digiteenuseid vahendavaid positsioone, nagu näiteks otsingumootorid, äpipoeid, videote jagamise platvormid ja sõnumiteenuste pakkujad.

Üheks digiturgude määrase erinevuseks võrreldes digiteenuste määrasega, on kasutajate jaotamine mitte tarbijateks ja teenusesaajateks, vaid lõppkasutajateks ja ärikasutajateks. Lõppkasutaja tähendab selles kontekstis “füüsilist või juriidilist isikut, kes kasutab põhiplatvormiteenuseid muul viisil, kui ärikasutajana.”¹⁵⁰ Ärikasutaja seejuures on “füüsiline või juriidiline isik, kes tegutseb äri- või kutsetegevuse raames ja kasutab põhiplatvormiteenuseid.”¹⁵¹ Seega kohaldub ka digiturgude määrasest tulenev kaitse peale füüsiliste isikute ka juriidilistele isikutele, piirdumata vaid tarbija kaitsega.

Omapärase nüansina sisaldab digiturgude määrase 13. artikkel kõrvalehoidmise vastaseid meetmeid, mis keelavad pääsuvalitsejatel neile pandud kohustustest kõrvale hiilida oma teenuseid osadeks jagades või “lepinguliste, kaubanduslike, tehniliste või muude vahenditega” killustada. Sarnast kohustustest kõrvalehoidmise vastast meetet on BEUC soovitanud lisada ka teistesse tumedaid mustreid käsitlevatesse õigusaktidesse, näiteks ebaausate kaubandustavade direktiivi.¹⁵²

Digiturgude määrase kolmas peatükk keskendub konkurentsi piiravate või ebaausate praktikate reguleerimisele. Selles peatükis sisalduv 5. artikkel sätestab eelnimetatud pääsuvalitsejate kohustused, kaasa arvatud näiteks 2. lõikest tulenev keeld korrata samasisulise nõusoleku küsimist rohkem, kui kord aastas, mis kujutab endast näägutamisele vastava tumeda mustri reguleerimist.

2.7. Andmemäärus

Neljandaks töö seisukohast asjakohaseks määraseks on 11. jaanuaril 2024. jõustunud Euroopa Parlamendi ja Nõukogu määrus (EL) 2023/2854, ehk edaspidi andmemäärus. See käsitleb õiglast ligipääsu andmetele ja andmete kasutamist. Määruse seos tumedate mustritega seisneb

¹⁵⁰ Digital Markets Act. Art. 3 punkt 20.

¹⁵¹ Digital Markets Act. Art. 3 punkt 21.

¹⁵² BEUC. 2022. “Dark patterns” and the EU Consumer Law acquis. Recommendations for better enforcement and reform. https://www.beuc.eu/sites/default/files/publications/beuc-x-2022-013_dark_patterns_paper.pdf Lk. 11.

asjaolus, et see keelab andmevaldajatel tumedate mustrite kasutamise neile pandud kohustustest kõrvale hiilimiseks.

Täpsemalt sätestab andmemääruse 4. artikli esimene lõige andmevaldajatele kohustuse tagada kasutajale teenuse või toote kasutamisega loodud andmetele juurdepääs. Sama artikli 4. lõige rõhutab, et: “Andmevaldajad ei tohi muuta kasutajate käesoleva artikli kohaste valikuvõimaluste või õiguste kasutamist põhjendamatult keeruliseks, sealhulgas pakkudes kasutajatele valikuvõimalusi mitteneutraalsel viisil või õõnestades või kahjustades kasutaja sõltumatust, otsuste tegemist või valikuvõimalusi digitaalse kasutajaliidese või selle osa struktuuri, kujunduse, funktsiooni või toimimisviisi kaudu.” Tegemist on üsna põhjaliku kirjeldusega tumedate mustrite omadustest ja tunnustest, millele lisandub ka 6. artiklis sisalduv sarnane tumedate mustrite kasutamist keelustav kohustus kolmandate isikute jaoks, kes kasutaja andmeid vastu võtavad.

2.8. Tehisintellekti käsitlev määrus

Töö seisukohast olulisimaks määruseks on Euroopa Parlamendi ja Nõukogu määrus (EL) 2024/1689, ehk edaspidi tehisintellekti käsitlev määrus või TI määrus, mis anti välja 13. juunil 2024. aastal ning jõustus 2. augustil 2024. aastal. Selle määruse loomisega asus Euroopa Liit rahvusvahelisse juhtpositsiooni tehisintellekti käsitleva õigusraamistiku loojana. Tegemist on horisontaalselt kohalduva õigusaktiga, mis ei asenda tarbijakaitselisi või muid õigusakte, vaid komplementeerib neid.¹⁵³

Enne seda 2021. aastal väljaantud tehisintellekti käsitleva määruse mõjuhinna seadis tehisintellekti arendamise ja kasutamise põhiprobleemidest teisele kohale võimaluse, et tehisintellekti kasutus suurendab kodanike põhiõiguste ja Euroopa Liidu väärtuste rikkumise ohtu.¹⁵⁴ Põhiõiguste kaitset on toonitatud korduvalt ka tehisintellekti määruse preambulis kui ka regulatiivosa esimeses artiklis, mis sätestab määruse eesmärgiks “parandada siseturu toimimist ning edendada inimkeskse ja usaldusväärse tehisintellekti kasutuselevõttu, tagades

¹⁵³ Tehisintellekti käsitlev määrus, preambuli punkt 9.

¹⁵⁴ Tehisintellekti käsitleva määruse mõjuhinna. LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS. 2021. Lk 13.

<https://ec.europa.eu/newsroom/dae/redirection/document/75792>

samal ajal tervise, ohutuse ja põhiõiguste hartas sätestatud põhiõiguste, sealjuures demokraatia, õigusriigi põhimõtte ja keskkonnakaitse kõrgetasemelise kaitse tehisintellektisüsteemide kahjuliku mõju vastu liidus, ning toetada innovatsiooni.“

Hoolimata igakülgsest põhiõiguste kaitsmise eesmärgi toonitamisest, ei anta selle määrusega mingisuguseid õiguskaitsevahendeid põhiõiguste kandjatele, kellel peaaegu puudub roll tehisintellekti käsitlevas määruses. See ei klapi sellise põhiõigusi tagava määruse eesmärgiga.

155

Tehisintellekti käsitleva määruse preambuli 12. punkt toonitab ka tehisintellektisüsteemi mõiste selget määratlust ning põhinemist tehisintellektisüsteemide põhiomadustel. Nagu varasemalt esimeses peatükis kirjeldatud, ei ole tehisintellektisüsteemi mõiste selle määruse kontekstis väga selgelt määratletud ning pigem on kitsa tehisintellekti definitsiooni tõttu oht lihtsamate ja etteaimatavate tarkvarasüsteemide ülereguleerimiseks sama kõrgete nõuete kaudu.¹⁵⁶

Samuti ei ole tehisintellekti näol tavapäraselt tegemist eraldiseisva süsteemiga, millel on üks funktsioon, mille riske tehisintellekti määruse alusel hinnata saab. Tehisintellekt, nagu näiteks soovitusüsteem, sobitub ülejäänud kasutajaliidese funktsioonidega, millest teda võib olla keeruline eraldada.¹⁵⁷

2.8.1. Tumede mustrite käsitus tehisintellekti määruses

Tehisintellekti käsitleva määruse 5. artikkel on tumede mustrite perspektiivist olulisim ning sätestab sellised tehisintellektisüsteemi kasutusviisid, mis on keelatud riskiga. Seda artiklit on kritiseeritud keelatud tehisintellekti kasutusviise hindavate parameetrite puudumise tõttu, mis jätab segaseks, millistel asjaoludel on osad tehisintellektisüsteemi kasutamise viisid

¹⁵⁵ Regulating AI in Europe: four problems and four solutions <https://www.adalovelaceinstitute.org/wp-content/uploads/2022/03/Expert-opinion-Lilian-Edwards-Regulating-AI-in-Europe.pdf> Lk. 10.

¹⁵⁶ Ebers, Martin. “Truly Risk-Based Regulation of Artificial Intelligence How to Implement the EU’s AI Act.” *European Journal of Risk Regulation*, 2024, 1–20. <https://doi.org/10.1017/err.2024.78>. Lk 12.

¹⁵⁷ Regulating AI in Europe: four problems and four solutions <https://www.adalovelaceinstitute.org/wp-content/uploads/2022/03/Expert-opinion-Lilian-Edwards-Regulating-AI-in-Europe.pdf> Lk. 10.

keelatud ja millistel asjaoludel kõrge riski ning piiratud riski alla liigitatud.¹⁵⁸ See lähenemine pole ka tulevikukindel, kuna ei sisalda võimalust uusi potentsiaalselt keelatava või kõrge riskiga tehisintellektisüsteeme nendesse listidesse lisada.¹⁵⁹

Määruse 5. artikli esimese lõike punktis a keelustatakse “selliste tehisintellektisüsteemide turule laskmine, kasutusele võtmine või kasutamine, milles on kasutatud inimese teadvusest kaugemale ulatuva alalävisele tajule suunatud võtteid või sihilikult manipuleerivaid või petlikke võtteid, mille eesmärk või tagajärg on isiku või isikute rühma käitumise oluline moonutamine, kahjustades oluliselt nende võimet teha teadlik otsus ja pannes nad seeläbi tegema otsuse, mida nad ei oleks muul juhul teinud, viisil, mis põhjustab või mõistliku tõenäosusega põhjustab sellele isikule, teisele isikule või isikute rühmale olulist kahju”.

Võtame selle sätte komponentideks lahti. Tumedad mustrid, mida see säte keelustab, peavad ühteagu olema:

- a) hinnatavad tehisintellektisüsteemi turule laskmise, kasutusele võtmise või kasutamise hetkel;
- b) sisaldama alateadvusele suunatud, sihilikult manipuleerivaid või petlikke võtteid – kuna alateadvuslike võtete mõju pole veel ühetaoliselt teaduslikult tõendatud,¹⁶⁰ peaks tegemist olema sihilikult manipuleerivate või petlike võtetega, mis ei paku kaitset võtete osas, kus kas puudub pahatahtlik komponent või võtte manipuleerivus või petlikkus pole tehisintellektisüsteemi loogika jälgimatuse või erinevate päritoluga funktsioonide kombineerimise tõttu tuvastatav;
- c) sisaldama eesmärgi või tagajärjena isiku või isikute rühma käitumise olulist moonutamist – sarnase sisuga mõiste ebaausate kaubandustavade direktiivi 2. artiklis punktis e kirjeldab tarbijate majanduskäitumise olulist moonutamist kui “kaubandustava järgimist eesmärgiga märgatavalt kahjustada tarbijate võimet teha teadlikke valikuid, pannes tarbija seetõttu tegema tehinguotsust, mida ta muul juhul ei oleks teinud”, teisitiöeldult madalam lävend, kui

¹⁵⁸ Regulating AI in Europe: four problems and four solutions <https://www.adalovelaceinstitute.org/wp-content/uploads/2022/03/Expert-opinion-Lilian-Edwards-Regulating-AI-in-Europe.pdf> Lk. 12.

¹⁵⁹ Samas.

¹⁶⁰ Leiser, Dr Mark and Santos, Cristiana, Dark Patterns, Enforcement, and the Emerging Digital Design Acquis: Manipulation beneath the Interface, Vol. 15 No. 1 (2024): BILETA Special Issue. Lk. 5. Available at SSRN: <https://ssrn.com/abstract=4431048> Lk. 26.

tehisintellekti määrukses, kuna ei sisalda olulise kahju nõuet, vaid lihtsalt teistsugust tehinguotsust;

d) see oluline isiku või isikute rühma käitumise moonutamine peab olema teguriks, mis kahjustab nende võimet teha teadlikku otsust;

e) see teadliku otsuse tegemise võime kahjustamine peab viima otsuseni, mida isik muul juhul teinud ei oleks;

f) otsuse tegemine peab viima olulise kahju põhjustamiseni kas sellele isikule, teisele isikule või isikute rühmale – kuidas on seda piisava olulise kahju mõistet võimalik sisustada enne tehisintellektisüsteemi turule laskmist?

Tegemist on pika põhjuslikku seost taotleva ahelaga, mille komponentide põhjal keelatud tehisintellekti kasutusviisile vastavuse hindamine sõltub täielikult oletavatest mõjudest ja kahjudest, mis isikule tekkida võivad. Sellest ei piisa tehisintellektide põhjustatud tumedate mustrite ohtude hõlmamiseks ega ka isikute põhiõiguste tõhusaks kaitseks.

Teiseks oluliseks sätteks tumedate mustrite kontekstis on 5. artikli 1. lõike punkt b, mis keelustab sellised tehisintellektisüsteemid, mis “kasutavad ära füüsilise isiku või konkreetse isikute rühma mis tahes haavatavusi, mis tulenevad nende vanusest, puudest või konkreetsest sotsiaalsest või majanduslikust olukorrast ning mille eesmärk või tagajärg on oluliselt moonutada selle isiku või sellesse rühma kuuluva isiku käitumist viisil, mis põhjustab või mõistliku tõenäosusega põhjustab sellele või mõnele teisele isikule olulist kahju”.

Need sätted peegeldavad ebaausate kaubandustavade direktiivi sätteid, kuid mõnigate piirangutega. Nimelt oleneb nende manipuleerivate või petlike praktikate keelatus TI määrukses kontekstis sellest, kas võtteid kasutatakse tehisintellektisüsteemi abil. Võrreldes sellega kohaldub ebaausate kaubandustavade direktiiv ka muudele tehnoloogilistele lahendustele, mis tehisintellektisüsteemi mõiste alla ei käi.

Tehisintellekti määrukses sisalduvad haavatavused on samuti direktiivist erinevad, kaitstes isikuid, kes on haavatavad vanuse, vaimse või füüsilise puude või konkreetse sotsiaalse või majandusliku olukorra tõttu.¹⁶¹ See säte ei sisalda nii pikka seoselist ahelat, kui punktis a, kuid sisaldab siiski nõuet, et tehisintellektisüsteem peab ära kasutama loetletud põhjustel isikute

¹⁶¹ EC Study Lk. 83.

rühmal olevaid haavatavusi. Sotsiaalse või majandusliku olukorra põhise haavatavuse väljatoomine on oluline, kuna tihti mõjutavad tumedad mustrid ebaproportsionaalselt näiteks vähem haritud inimesi, kes pole nii teadlikud oma õigustest. Selline haavatavuste käsitus sobib analoogsesse sättesse ebaausate kaubandustavade direktiivis, kuid tehisintellektisüsteemide puhul jääb väheseks. Nimelt on digitaalse asümmeetria kontekstis haavatav iga digitaalne tarbija, mistõttu haavatavuse alusel erandlikult kaitse pakkumine ei peegelda tarbijate realistlikku olukorda digikeskkonnas.¹⁶² Seda enam, et tehisintellektile omane on võime tuvastada konkreetse isiku haavatavused.

Tehisintellekti määruse 5. artikli esimese lõike punktist b võib tõmmata paralleele ebaausate kaubandustavade direktiivi alajaotuses käsitletud haavatava tarbija kontseptsiooniga. Nimelt seab ebaausate kaubandustavade direktiiv erandina haavatavate tarbijarühmade mõjutamise korral standardiks keskmise tarbija asemel selle haavatava grupi keskmise esindaja. Tehisintellekti määruse kontekstis haavatava isiku mõiste ei sisalda keskmise haavatava isiku parameetrit, mida kasutab ebaausate kaubandustavade direktiiv, vaid olulise kahju nõuet nagu ka mitte haavatavate rühmade puhul.

Ebaausate kaubandustavade direktiivis peetakse haavatavateks tarbijaid, kes oma vaimse või füüsilise puude, vanuse või kergeusklikkuse tõttu on eriti vastuvõtlikud nende majanduskäitumise moonutamisele, mille lävend on oluliselt madalam, kui tehisintellekti määruses toodud “olulise kahju” tingimus, mis kohaldub nii tavakasutajatele kui ka haavatavatele isikutele. Tehisintellekti käsitleva määruse preambuli 29. põhjendus defineerib olulist kahju kui “eelkõige sellist, millel on piisavalt oluline kahjulik mõju füüsilisele ja psühholoogilisele tervisele või finantshuvidele”. Seejuures pole täpsustatud, milline kahju on “piisavalt oluline”, et selle põhjustamine isikule või isikute rühmale läbi nende käitumise olulise moonutamise tooks kaasa tehisintellektisüsteemi kasutusele võtmise keelustamise.

2.8.2. Riskipõhine lähenemine tehisintellekti käsitlevas määruses

¹⁶² BEUC. 2022. “Dark patterns” and the EU Consumer Law acquis. Recommendations for better enforcement and reform. https://www.beuc.eu/sites/default/files/publications/beuc-x-2022-013_dark_patterns_paper.pdf Lk. 9.

Tehisintellekti määrus lähtub riskipõhisest lähenemisest. See kujutab endast seda, et erinevad TI kasutusviisid jaotatakse nelja riskikategooriasse: keelatud tehisintellekti kasutusviisid, suure riskiga tehisintellekti kasutusviisid, piiratud riskiga ja madala riskiga kasutusviisid. Suure riski puhul on määrus ette näinud rohkem kontrollmeetmeid, piiratud riski puhul läbipaistvusnõuded ning madala riski puhul vabatahtlikult järgitavad käitumisjuhendid.

Määrust on kritiseeritud, kui mitte reaalselt vastavana riskipõhisele lähenemisele.¹⁶³ Tehisintellekti käsitleva määruse preambuli 26. punktist võib välja lugeda, et õigusnormide liiki ja sisu kohaldatakse vastavalt riskidele ja kahju ulatusele, mida tehisintellektisüsteemid võivad põhjustada. Kuna TI määruse tehisintellektisüsteemi definitsioon hõlmab ka lihtsamaid ja etteaimatavamaid süsteeme, peaks tõesti riskipõhine lähtumine tähendama kõrgemaid kohustusi vähem etteaimatavamatele keerulisematele süsteemidele, kuid see pole nii.¹⁶⁴

Riskipõhist lähenemise vastu räägib ka asjaolu, et seda kasutatakse tavapäraselt olukordades, kus kahju on objektiivselt mõõdetav. Sellest tingituna võib riskipõhine lähenemine vähendada keerulisemalt mõõdetavate õiguste põhise kahju tähtsust.¹⁶⁵ Ka tehisintellekti käsitlevas määruks on näha, et kasutatud piisava “olulise kahju” mõistet, jättes see täpsemalt sisustamata ning deklareerides põhiõiguste kaitset eraldi eesmärgina esimeses artiklis.

Peale selle on kritiseeritud tehisintellektisüsteemidest tulenevate riskide hindamist turule laskmise hetkel, mis lihtsustab nad staatiliseks tooteks, mille risk on ette määratud.¹⁶⁶ Tehisintellekti üks põhitunnuseid on õppimis- ja kohanemisvõime, mistõttu iga tehisintellektisüsteemidega seonduv risk vajab pidevat hindamist.¹⁶⁷

¹⁶³ Ebers, Martin. “Truly Risk-Based Regulation of Artificial Intelligence How to Implement the EU’s AI Act.” *European Journal of Risk Regulation*, 2024, 1–20. <https://doi.org/10.1017/err.2024.78>. Lk 12.

¹⁶⁴ Ebers, Martin. “Truly Risk-Based Regulation of Artificial Intelligence How to Implement the EU’s AI Act.” *European Journal of Risk Regulation*, 2024, 1–20. <https://doi.org/10.1017/err.2024.78>. Lk 12.

¹⁶⁵ Kaminski, Margot E., The Developing Law of AI: A Turn to Risk Regulation (April 12, 2023). The Digital Social Contract: A Lawfare Paper Series (April 2023), U of Colorado Law Legal Studies Research Paper No. 24-5, Lk 14. Available at SSRN: <https://ssrn.com/abstract=4692562> or <http://dx.doi.org/10.2139/ssrn.4692562>

¹⁶⁶ Regulating AI in Europe: four problems and four solutions <https://www.adalovelaceinstitute.org/wp-content/uploads/2022/03/Expert-opinion-Lilian-Edwards-Regulating-AI-in-Europe.pdf> Lk. 10.

¹⁶⁷ Regulating AI in Europe: four problems and four solutions <https://www.adalovelaceinstitute.org/wp-content/uploads/2022/03/Expert-opinion-Lilian-Edwards-Regulating-AI-in-Europe.pdf> Lk. 10.

Ehk kokkuvõtlikult reguleerib tehisintellekti määrus tehisintellektisüsteemide abil kasutatavaid tumedaid mustreid viisil, mis:

- a) hõlmab koos autonoomsete tehisintellektisüsteemidega ka lihtsamaid loogika- ja teadmispõhiseid süsteeme;¹⁶⁸
- b) ei arvesta tehisintellektisüsteemide dünaamilise ja kohaneva olemusega, mille tagajärjel nende kujutatav risk võib muutuda peale turule laskmist;¹⁶⁹
- c) ei anna põhiõiguste kandjatele õiguskaitsevahendeid juhuks, kui nad keelust hoolimata siiski keelatud tehisintellektisüsteemi kasutuse ohvriks langevad;
- d) ei sisusta piisavalt olulise kahju meedet, mille puhul keeld manipuleerivale võttele rakendub;
- e) ei nimeta konkreetseid tehisintellekti kasutatavaid manipuleerivaid võtteid, mis tehisintellektisüsteemi keelatavuse põhjustaks;
- f) ei arvesta kõigi isikute haavatavusega digitaalse asümmeetria kontekstis.

Pakun järgnevas peatükis välja alternatiivse tehisintellekti võimel põhineva tumedate mustrite mudeli, mis neid puudusi tulevikukindlamalt, põhiõigusi kaitsvamalt ning läbipaistvamalt reguleeriks.

¹⁶⁸ Ebers, Martin. “Truly Risk-Based Regulation of Artificial Intelligence How to Implement the EU’s AI Act.” *European Journal of Risk Regulation*, 2024, 1–20. <https://doi.org/10.1017/err.2024.78>. Lk 12.

¹⁶⁹ Regulating AI in Europe: four problems and four solutions <https://www.adalovelaceinstitute.org/wp-content/uploads/2022/03/Expert-opinion-Lilian-Edwards-Regulating-AI-in-Europe.pdf> Lk. 10.

3. TEHISINTELLEKTI VÕIMETE PÕHINE TUMEDATE MUSTRITE KÄSITLUS

Käesolevas peatükis pakun välja alternatiivse võimetepõhise mudeli tehisintellekti võimaldatud ja võimendatud tumedate mustrite käsitlemiseks.

Tehisintellekti käsitleva määruse preambuli kuues punkt seab eeltingimuseks, et “tehisintellekt peab olema inimkeskne tehnoloogia. See peaks olema vahend, mis teenib inimesi ja mille lõppeesmärk on suurendada inimeste heaolu.” Antud mudeliga üritangi tehisintellektide kasutamise käigus prioritseerida inimeste teenimist ning nende heaolu suurendamist.

Selle mudeli eeliseks on lihtsam *ex ante* hinnatavus, kas konkreetsel tehisintellektisüsteemil on olemas piiratud võimekus, võrreldes tehisintellekti määruse läbipaistmatu riski kategooriate süsteemiga, mis nõuavad “piisavalt olulise” kahju hindamist kontekstis, kus ka võimalikud kahju põhjustamiseni viivad manipuleerivad võtted pole kirjeldatud ning ei pruugi olla veel tehisintellektisüsteemi turule laskmise hetkel välja kujunenudki. Võimetepõhine mudel lahendab mitmed tehisintellekti käsitlevas määruses eelnevalt välja toodud kitsaskohad.

Tehisintellekti käsitlev määrus katab põhiliselt kõrge riskiga ning tahtlikult manipuleerivaid tumedaid mustreid kasutavaid süsteeme. Digiteenuste määrus keskendub kasutajaliideses sisalduvatele tumedatele mustritele, ehk visuaalselt petlikele disainivõtetele. Katmata jääb osa, milles risk on madalam kuid siiski kahjulik, või mitte tahtlik kuid siiski kahjulikku mõju avaldav. Samuti tumedad mustrid, mis ei pruugi avalduda ainult kasutajaliidese disainis, vaid ka näiteks veebilehe teksti sisus, tööpõhimõtetes, ajastuses, kasutaja profileerimises ja nii edasi.

Mudeli näol on tegemist ka tehnoloogianeutraalse käsitlusega, mis on oluliseks tunnustatud põhimõtteks erinevate informatsiooniteaduslike süsteemide reguleerimisel, kaasa arvatud

Euroopa Liidus.¹⁷⁰¹⁷¹ Tehnoloogianeutraalsuse põhimõtte kohaselt ei peaks seadusandlus diskrimineerima konkreetset tüüpi tehnoloogiliste funktsioonidega lahenduste vastu, vaid nende funktsioonide eesmärkide põhjal.¹⁷² Kuigi loetlen käesolevas peatükis tehisintellektile – ja mõnele teisele programmilahendusele – omaseid võimeid, oleneb nende võimete kasutamise eesmärgist, kas või kuivõrd peaks konkreetseid võimeid reguleerima.

Ka oma käsitluses võtan aluseks kitsa tehisintellektisüsteemi mõiste, nagu seda on tehisintellekti käsitlevas määruses defineeritud. Nimelt sobib minu mudeliga, kui peale ainult tehisintellektile omaste funktsioonide täitmise hõlmatakse ka üldisest tehisintellektist lihtsamakoelisemaid programme, millel võib sellegipoolest olla sarnane võimekus tänu teiste tumedate mustrite kasutamisele või ka ligipääsu tõttu suurele hulgale isikuandmetele. Sellised programmid vastavad tehisintellekti käsitlevas määruses toodud kitsale tehisintellekti definitsioonile.

Võrreldes tehisintellekti määruses käsitletud tarbija õigustel põhineva tumedate mustrite liigitusega, on Leiseri ja Santose taksonoomia sobilikum tehisintellektile põhinevate tumedate mustrite hindamiseks, kuna eristab neid nii tuvastavuse kui ka võimete poolest, mis on ka minu tehisintellekti põhiste tumedate mustrite käsitluses aluseks.

¹⁷⁰ Anne Veerpalu, “Regulatory challenges to the use of distributed ledger technology: Analysis of the compliance of existing regulation with the principles of technology neutrality and functional equivalence” (PhD thesis, University of Tartu 2021) <https://dspace.ut.ee/bitstreams/12ad2896-93f2-4d23-ac81-c28d50c9f25e/download>. Lk. 28.

¹⁷¹ Ebers, Martin. “Truly Risk-Based Regulation of Artificial Intelligence How to Implement the EU’s AI Act.” *European Journal of Risk Regulation*, 2024, 1–20. <https://doi.org/10.1017/err.2024.78>. Lk 5.

¹⁷² Anne Veerpalu, “Regulatory challenges to the use of distributed ledger technology: Analysis of the compliance of existing regulation with the principles of technology neutrality and functional equivalence” (PhD thesis, University of Tartu 2021) <https://dspace.ut.ee/bitstreams/12ad2896-93f2-4d23-ac81-c28d50c9f25e/download>. Lk. 28.

3.1. Kitsa tehisintellekti võimed, mis võimaldavad või võimendavad tumedate mustrite kasutust.

3.1.1. Profileerimine.

Profileerimine kujutab endast kasutajate tuvastamist ja eristamist nende isikuomaduste, soo, käitumise, haavatavuste ning muude tegurite kaudu. Tehisintellekt suudab seda teha massiliselt ning reaalajas, mis võimaldab kasutada erinevaid tumedaid mustreid just nendel isikutel, kes neile vastuvõtlikumad on. Profileerimist saab kasutada väga täpseks personaliseerimiseks.¹⁷³

3.1.2. Personaliseerimine.

Tehisintellektile on omane võime personaliseerida ehk isikustada kasutajaliidest, suhtlusstiili, teksti sõnastust arvestades konkreetse isiku huvisid. Tumedate mustrite kasutamise võtmes on andmete kogumise hulk kõvasti võimendanud personaliseerimisega kaasnevaid tumedaid mustreid.¹⁷⁴

3.1.3. Pidev arenemise-ja kohanemisevõime.

Tehisintellekti üks põhitunnuseid on õppimis- ja kohanemisevõime, mistõttu iga tehisintellektisüsteemidega seonduv risk vajab pidevat hindamist. Komplexsemaid tehisintellekte iseloomustab võime õppida erinevatest situatsioonidest ning nendega kohaneda, muutes kasutajakogemust. See vajab teenusepakkuja poolt jälgimist, et autonoomselt arenev tehisintellekt ei areneks oma ülesannete täitmise käigus tumedaid mustreid kasutama.¹⁷⁵

¹⁷³ OECD (2022), "Dark commercial patterns", *OECD Digital Economy Papers*, No. 336, OECD Publishing, Paris, <https://doi.org/10.1787/44f5e846-en>. Lk 41.

¹⁷⁴ OECD (2022), "Dark commercial patterns", *OECD Digital Economy Papers*, No. 336, OECD Publishing, Paris, <https://doi.org/10.1787/44f5e846-en>. Lk 41.

¹⁷⁵ Regulating AI in Europe: four problems and four solutions <https://www.adalovelaceinstitute.org/wp-content/uploads/2022/03/Expert-opinion-Lilian-Edwards-Regulating-AI-in-Europe.pdf> Lk. 10.

3.1.5. Paralleelsete kasutajakogemuste testimisvõime.

A/B testimine kujutab endast võtet, mis ei pruugi heatahtliku kasutamise puhul kuuluda tumeda mustri alla. See on kasutajaliidese kujundamise võte, mille käigus näidatakse erinevatele kasutajatele väikse disainilise erinevusega versiooni veebilehe kasutajaliidest. Selle põhjal on eetilisel veebilehe disaineril võimalik hinnata, milline kasutajaliidese versioon kasutajale kõige käepärasem, meeldivam või efektiivsem tundus.

Ebaeetilisel disaineril on võimalik A/B testimist kasutades hinnata, millise disaini või sõnastuse puhul kõige rohkem kasutajaid näiteks oma andmete jagamisega nõustub. Tehisintellekt on seda nähtust oluliselt kiirendanud, ning võimaldab oluliselt efektiivsemalt laia kasutajaskonna peal erinevate disainiliste võtete proovimist.¹⁷⁶

3.2. Väljapakutav mudel

§1. Üldine autonoomiat prioritseeriv kohustus.

Teenusepakkujad disainivad süsteeme, millel on võime kasutaja käitumist mõjutada selliselt, et säilib kasutaja võime teha vabasid, informeeritud, tahtlikke ning tagasipööratavaid valikuid.

§2. Valikute sümmeetria.

Teenusepakkuja tagab, et valikuga nõustumine või sellest keeldumine on kasutaja jaoks sama kättesaadav, selge ja samavõrra kognitiivselt koormav.

§3. Usaldusväärsed soovitusel.

Teenusepakkuja tagab, et kasutatav süsteem või kasutajaliidese disainielement, mis tõstab esile, soovitab või visuaalselt prioritseerib kasutajale antava valiku varianti, teeb seda valiku osas, mis riivab vähem kasutaja põhiõigusi ning on talle kasulik.

§4. Personaliseerimine.

Teenusepakkuja tagab, et veebilehe elemendid, mis on automatiseeritud süsteemi poolt kasutaja valiku mõjutamiseks personaliseeritud, genereeritud, ajastatud või kohandatud, on sellisena selgelt märgitud.

§5. Profiliseerimine.

Keelatud on kasutada süsteeme, mis tuvastavad ja kasutavad ära kasutajate haavatavusi, isikuomadusi, sõltuvusi, harjumusi, väsimust, kognitiivset või emotsionaalset seisundit, et mõjutada neid tegema otsuseid, mis on neile kahjulikud ning mida nad haavatavuse ära kasutamiset ei teeks.

§6. Tehislik sotsiaalsituatsiooni matkimine.

Teenusepakkuja tagab, et ei genereeri tehisintellekti abil sisu, näiteks arvustusi või kommentaare, mida kasutajal pole hõlpsasti võimalik eristada päris kasutaja loodud sisust. Teenusepakkuja ei kasuta ebamääraseid termineid tehisintellektil põhineva kasutajatoe elemendi kohta, mis võivad eksitada kasutajat arvama, et tegemist on suhtlusega päris inimesega.

§7. Peidetud valikuarhitektuur.

Teenusepakkuja tagab, et valikud, mida kasutaja teeb oma õiguste kaitseks, on keskmisele kasutajale veebilehe menüüdest kergesti kättesaadavad. Kui otsuste või valikute tegemisel on kasutajal vaja suhelda juturobotiga, informeerib juturobot kasutajat kõigist kasutajale otsuse tegemisel äratuntavalt olulistest valikuvariantidest ning võimalustest.

§8. Kognitiivne koormamine.

Teenusepakkuja ei sunni kasutajat kordama valikut, mida ta on juba teinud, ega mõjuta kasutajat ümber mõtlema emotsionaalselt manipuleerivate või kasutajat sildistavate loosungitega.

§9. Dünaamiline süsteem.

Teenusepakkuja kohustub tehisintellektil põhinevat arenevat ja õppivat süsteemi regulaarselt hindama ohtlike või kahjulike tumedate mustrite tekkimise ennetamiseks.

3.3. Võrdlus olemasoleva seadusandluse kitsaskohtadega.

Eelnevalt väljatoodud kitsaskohad tumedate mustrite reguleerimisel olid järgnevad.

Esiteks hõlmas TI määrus koos autonoomsete tehisintellektisüsteemidega ka lihtsamaid loogika- ja teadmistepõhiseid süsteeme.¹⁷⁷ Pakutud tumedate mustrite reguleerimise mudel võtab süsteemile või tehisintellektile omaste võimete põhise lähenemise, mistõttu on tehnoloogianeutraalsem ning ei vaja väga konkreetset definitsiooni tehisintellektist, vaid kinnitust, kas konkreetne element, algoritm või komplekssem süsteem on võimeline kasutama või esitama kasutajale tema valikuid mõjutavaid tumedaid mustreid.

Teiseks ei arvestanud TI määrus tehisintellektisüsteemide dünaamilise ja kohaneva olemusega, mille tagajärjel nende kujutatav risk võib muutuda peale turule laskmist.¹⁷⁸ Seda puudust adresseerib mudeli §9, mille kohaselt teenusepakkuja kohustub ise arenevat ja õppivat süsteemi regulaarselt hindama ohtlike või kahjulike tumedate mustrite tekkimise ennetamiseks.

Kolmandaks ei anna TI määrus põhiõiguste kandjatele õiguskaitsevahendeid juhuks, kui nad keelust hoolimata siiski keelatud tehisintellektisüsteemi kasutuse ohvriks langevad. Pakutud mudel seab teenusepakkujale konkreetseid kohustusi, kuid ei too välja kasutajale antavaid õiguskaitsevahendeid.

Neljandaks ei sisustanud tehisintellekti käsitlev määrus piisavalt olulise kahju meedet, mille puhul keeld manipuleerivale võttele rakendub. Väljapakutud võimetepõhine mudel keelab konkreetsete tehisintellektil olevate võimete kasutamist tumeda mustri kujul kasutaja vastu. See tähendab, et olulise kahju mõiste sisustamine ei ole vajalik, et tuvastada, et teenusepakkuja on oma kohustusi rikkunud.

Viiendaks ei nimetanud tehisintellekti käsitlev määrus konkreetseid tehisintellekti kasutatavaid manipuleerivaid võtteid, mis on tehisintellektisüsteemi keelatavuse põhjustaks.

¹⁷⁷ Ebers, Martin. "Truly Risk-Based Regulation of Artificial Intelligence How to Implement the EU's AI Act." *European Journal of Risk Regulation*, 2024, 1–20. <https://doi.org/10.1017/err.2024.78>. Lk 12.

¹⁷⁸ Regulating AI in Europe: four problems and four solutions <https://www.adalovelaceinstitute.org/wp-content/uploads/2022/03/Expert-opinion-Lilian-Edwards-Regulating-AI-in-Europe.pdf> Lk. 10.

Pakutav mudel tõi välja peamised tumedate mustrite võtted, mida kasutatakse, mis võimaldab kasutajal lihtsamini hinnata, kas tema õigusi on rikutud.

Kuuendaks kitsaskohaks oli asjaolu, et tehisintellekti käsitlev määrus ei arvesta kõigi isikute haavatavusega digitaalse asümmeetria kontekstis. Mis tähendab, et iga kasutaja on haavatav olukorras, kus teenusepakkujal või ka tehisintellektisüsteemil on tema kohta oluline kogus infot ning kasutajal pole võimalik leida konkureerivat alternatiivi, mis ei kasutaks tumedaid mustreid. Väljapakutud mudel kaitseb haavatavustena laiemat isikute hulka ning keelab haavatavuste profileerimise ning kasutaja vastu kasutamise üldisemalt.

KOKKUVÕTE

Tehisintellekti kaasamine kasutajaliidese disaini või töösse toob endaga unikaalsed võimalused ja ohud, mis erinevad tavapärastest tumedatest mustritest tulenevalt tehisintellekti olemusest ja võimetest. Käesoleva magistritöö eesmärgiks oli esiteks hinnata, kas tehisintellektipõhiste tumedate mustrite kasutus on olemasoleva Euroopa Liidu seadusandlusega efektiivselt reguleeritud, mille käigus ilmnes erinevaid kitsaskohti. Nende kitsaskohtade katmiseks pakkus töö kolmandas peatükis välja alternatiivse tehisintellektile omaste võimete põhise mudeli nimetatud tehisintellektipõhiste tumedate mustrite reguleerimiseks.

Esmalt kirjeldas töö esimeses peatükis tumedate mustrite arengut, tuvastamist ja liigitamist. Nüüdseks on möödunud viisteist aastat tumedate mustrite esmakordsest kirjeldamisest, mida esimesena tegi kasutajakogemuse disainer Harry Brignull, luues 2010. aasta augustis veebilehe¹⁷⁹, kus arhiveeris, loetles ja liigitas neid manipuleerivaid võtteid ja nendega seotud kohtuasju, artikleid ja seadusakte, et probleemile tähelepanu juhtida.

Selle perioodi jooksul on leidnud aset kolm “lainet” tumedate mustrite alases teadustöös. Esimese lainena üritati tumedaid mustreid kui uusi digiplatvormidega kaasnevaid nähtusi liigitada. Seejärel uuriti nende levikut ja esinemissagedust erinevatel veebilehtedel ning viimaks asuti empiirilisel hindamisel, kuidas mõjuvad need mustrid tarbijatele.¹⁸⁰ Selle aja jooksul on tumedatest mustritest saanud märkimisväärne ja kinnistunud oht digikeskkonnas, mida on uuritud ja arutatud nii käitumisökonoomilises kui ka õiguslikus võtmes. Võrreldes eelnenud lainetega üritas antud töö uue lähenemisena reguleerida tumedaid mustreid normatiivselt.

Probleemi levik süvenes ülemaailmse COVID-19 pandeemia ajal, mil paljud inimesed olid kodus viibimise tõttu sunnitud töötama, oste sooritama ja meelelahutust leidma digikeskkonna erinevate võimaluste kaudu. Euroopa Komisjon avaldas 2020. aastal uue tarbijakaitse tegevuskava, mille eesmärgiks oli tarbijate toimetulekuvõime parandamine ja seeläbi

¹⁷⁹Brignull, H., Leiser, M., Santos, C., & Doshi, K. (2023, April 25). *Deceptive patterns – user interfaces designed to trick you*. deceptive.design. Retrieved 27.03.2025, from <https://www.deceptive.design/>

¹⁸⁰OECD. Dark commercial patterns. 2022. Lk 21.

majanduse kestliku taastumise edendamine peale pandeemiat.¹⁸¹ Tegevuskava raames kajastati ka tumedate mustrite probleemi ning kirjeldati neid kui kaubandustavasid, “millega eiratakse tarbijate õigust teha teadlikke valikuid, kuritarvitatakse nende käitumislise eelarvamusi või kallutatakse otsustusprotsesse.”¹⁸²

Teises peatükis analüüsis autor olemasolevat seadusandlust, mis puudutas kuidagi tumedate mustrite mõistet. Tegevuskava kehtimise perioodil on tumedaid mustreid otseselt või kaudselt juba käsitletud jõustunud digiteenuste, digiturgude ja tehisintellekti määruses ning suure tõenäosusega on neil ka oluline roll veel alles planeeritud digitaalse õigluse määruses.¹⁸³

Kolmandas ning normatiivses osas välja pakutud tehisintellekti käsitlevate tumedate mustrite regulatiivne mudel keskendus tehisintellektil olevate võimete kasutamise piiramisele, mis tähendab tehnoloogianeutraalsemat lähenemist, kui olemasolevad aktid, mis tehisintellekti defineerida on üritanud.

Väljapakutud mudeli eeliseks on lihtsam *ex ante* hinnatavus, kas konkreetsel tehisintellektisüsteemil on olemas piiratud võimekus, võrreldes tehisintellekti määruse läbipaistmatu riski kategooriate süsteemiga, mis nõuavad “piisavalt olulise” kahju hindamist kontekstis, kus ka võimalikud kahju põhjustamiseni viivad manipuleerivad võtted pole kirjeldatud ning ei pruugi olla veel tehisintellektisüsteemi turule laskmise hetkel välja kujunenudki. Võimetepõhine mudel lahendab mitmed tehisintellekti käsitlevas määruses eelnevalt välja toodud kitsaskohad.

Teiseks oluliseks puuduseks oli asjaolu, et tehisintellekti käsitlev määrus katab põhiliselt kõrge riskiga ning tahtlikult manipuleerivaid tumedaid mustreid kasutavaid süsteeme. Digiteenuste määrus keskendub kasutajaliideses sisalduvatele tumedatele mustritele, ehk visuaalselt petlikele disainivõtetele. Katmata jääb osa, milles risk on madalam kuid siiski kahjulik, või mitte tahtlik kuid siiski kahjulikku mõju avaldav. Samuti tumedad mustrid, mis

¹⁸¹ Komisjoni teatis Euroopa Parlamendile ja Nõukogule. Uus tarbijakaitse tegevuskava. 13.11.2020. <https://eur-lex.europa.eu/legal-content/ET/TXT/HTML/?uri=CELEX:52020DC0696>

¹⁸² Komisjoni teatis Euroopa Parlamendile ja Nõukogule. Uus tarbijakaitse tegevuskava. 13.11.2020. <https://eur-lex.europa.eu/legal-content/ET/TXT/HTML/?uri=CELEX:52020DC0696>

¹⁸³ Mission letter to Michael McGrath. Ursula von der Leyen. https://commission.europa.eu/document/download/907fd6b6-0474-47d7-99da-47007ca30d02_en?filename=Mission%20letter%20-%20McGRATH.pdf

ei pruugi avalduda ainult kasutajaliidese disainis, vaid ka näiteks veebilehe teksti sisus, tööpõhimõtetes, ajastuses, kasutaja profileerimises ja nii edasi.

Kolmandas peatükis väljapakutud mudeliga üritas autor tehisintellekte puudutavate tumedate mustrite kasutamise käigus prioritseerida inimeste teenimist ning nende heaolu suurendamist, pannes kasutaja heaolu tagamise kohustuse teenusepakkuja õlgadele. See vastab tehisintellekti käsitleva määruse preambuli kuuendale punktile, mis seab eeltingimuseks, et “tehisintellekt peab olema inimkeskne tehnoloogia. See peaks olema vahend, mis teenib inimesi ja mille lõppeesmärk on suurendada inimeste heaolu.”

Viimasena analüüsis autor 3. peatükis eelnevalt 2. peatükis välja toodud seadusandlike kitsaskohtade katmist uue mudeli abil ning leidis, et kuigi mitmed kitsaskohad olid kaetud, leidis ka kohti, mida saaks parendada, näiteks isikutele õiguskaitsevahendite andmise osas.

CAPABILITY BASED REGULATORY MODEL OF DARK DESIGN PATTERNS RELATED TO ARTIFICIAL INTELLIGENCE

Abstract

There is nothing natural or truly random about the digital environment. Everything that appears on a website visitor's screen is designed for them to view. The layout of drop-down menus, the colour schemes of buttons or text, the boxes that are ticked off in front of the user - all these can subconsciously or even perceptively influence the user's behaviour and choices on a website. When such biased design techniques are used to undermine the autonomy of a website visitor or to manipulate them into making choices that are not in their best interests, they are called dark patterns.

Dark patterns is a term first coined by user experience designer Harry Brignull, who in August 2010 created a website¹⁸⁴ to archive, list and categorise these manipulative techniques and related court cases, articles and legislation, to draw attention to the problem. Almost fifteen years have now passed since the dark patterns were first described. During this period, three 'waves' of dark pattern research have taken place.¹⁸⁵ The first wave attempted to classify dark patterns as new phenomena associated with digital platforms.¹⁸⁶ Then, their spread and frequency on different websites was investigated and, finally, an empirical assessment of their impact on consumers was undertaken.¹⁸⁷ During this time, dark patterns have become a significant and entrenched threat in the digital environment, which has been studied and debated from both a behavioural economics and a legal perspective.

The spread of the problem was exacerbated during the global COVID-19 pandemic, when many people were forced to work, shop and entertain themselves at home through the various options of the digital environment. In 2020, the European Commission published a new

¹⁸⁴Brignull, H., Leiser, M., Santos, C., & Doshi, K. (2023, April 25). *Deceptive patterns – user interfaces designed to trick you*. deceptive.design. Retrieved 27.03.2025, from <https://www.deceptive.design/>

¹⁸⁵ OECD. Dark commercial patterns. 2022. Lk 21.

¹⁸⁶ OECD. Dark commercial patterns. 2022. Lk 21.

¹⁸⁷ OECD. Dark commercial patterns. 2022. Lk 21.

Consumer Agenda,¹⁸⁸ aimed at improving consumer resilience and thereby fostering a sustainable economic recovery after the pandemic.

The Action Plan also addressed the problem of dark patterns, describing them as commercial practices that "disregard consumers' right to make informed choices, abuse their behavioural biases or bias their decision-making processes."¹⁸⁹ During the period of the 2020-2025 Action Plan being in effect, dark patterns have already been directly or indirectly addressed in the Digital Services, Digital Markets and Artificial Intelligence Acts, which have entered into force, and dark patterns are also likely to play an important role in the still-planned Digital Fairness Act.¹⁹⁰

The Organisation for Economic Co-operation and Development (OECD) has released its 2022 Action Plan on Dark Business Patterns, which describes dark patterns as practices that "lead, deceive, coerce or manipulate consumers into making choices that are often not in their best interests."¹⁹¹ Of course, manipulating, misleading or deceiving people as such is not a legally unprecedented or novel challenge. The European Union has dealt with problems related to or similar to dark patterns before, partly through the prism of data protection or consumer protection. For example, the General Data Protection Regulation sets out the parameters under which consent is validly given, and many dark patterns qualify as aggressive or misleading under the Unfair Commercial Practices Directive.

The problem of dark patterns is a wide-ranging and relevant issue, the effective regulation of which directly affects the effectiveness of the protection of other existing legislation in the digital environment. For example, dark patterns have been widely used to mislead consumers into giving their consent to cookies under the GDPR.¹⁹² What would the legal landscape look like in the physical world if contracts contained terms and conditions written in invisible ink or on a separate piece of paper that you had to find yourself in the drawers of a stranger's office? Unless circumvention of the provisions of existing laws is sufficiently prohibited, this

¹⁸⁸ Komisjoni teatis Euroopa Parlamendile ja Nõukogule. Uus tarbijakaitse tegevuskava. 13.11.2020. <https://eur-lex.europa.eu/legal-content/ET/TXT/HTML/?uri=CELEX:52020DC0696>

¹⁸⁹ Komisjoni teatis Euroopa Parlamendile ja Nõukogule. Uus tarbijakaitse tegevuskava. 13.11.2020. <https://eur-lex.europa.eu/legal-content/ET/TXT/HTML/?uri=CELEX:52020DC0696>

¹⁹⁰ https://commission.europa.eu/document/download/907fd6b6-0474-47d7-99da-47007ca30d02_en?filename=Mission%20letter%20-%20McGRATH.pdf

¹⁹¹ OECD (2022), "Dark commercial patterns", *OECD Digital Economy Papers*, No. 336, OECD Publishing, Paris, <https://doi.org/10.1787/44f5e846-en>. Lk 2.

¹⁹² Behavioral study on unfair commercial practices in the digital environment: dark patterns and manipulative personalisation. European Commission. 2022. Lk 45.

is not an isolated problem of circumvention, but a systemic problem with important implications for all legislation shaping the digital environment.

The impact of dark patterns has been boosted by the fact that more data is being collected from website visitors than ever before. The use of dark patterns often goes hand in hand with personalisation,¹⁹³ whereby a website visitor's data and behaviour on the website is used to present more relevant offers or content. Personalisation can be a neutral or positive experience for the user, but can also involve the identification of their vulnerabilities or profiling them, which is particularly damaging in combination with other dark patterns.¹⁹⁴ Indeed, it is common practice for websites to use a number of different dark patterns at the same time, and they rarely occur in isolation.¹⁹⁵ This also means that a user can suffer a variety of harms from dark patterns at once: for example, economic and time-related harm, which can in turn lead to psychological harm.¹⁹⁶

Adding fuel to the fire has been the rapid development and uptake of artificial intelligence based systems over the last few years, which has amplified many of the dark patterns previously present on digital platforms and has also enabled entirely new methods of manipulating consumer choices and habits. Artificial intelligence systems can, among other things, collect and process an unprecedented amount of data, anticipate and adapt to user behaviour in real time, identify the most profitable attention loops for a particular individual, and time and place consent requests at the precise moment and place where a website visitor is most likely to consent to an infringement. Not to mention generating unique articles, photos, reviews and similar content that cannot be effectively identified and removed by previously effective spam filters. All of this makes already established harmful dark patterns even more dynamic, personalised and difficult to catch.

The European Commission's New Consumer Agenda, mentioned earlier, has underlined the need for civil liability measures that would ensure that victims of harm caused by AI are

¹⁹³ Behavioral study on unfair commercial practices in the digital environment: dark patterns and manipulative personalisation. European Commission. 2022. Lk 6.

¹⁹⁴ Helberger, Micklitz H.-W. et al. (2021) "Structural asymmetries in digital consumer markets", study for BEUC, Lk. 110.
https://www.beuc.eu/sites/default/files/publications/beuc-x-2021-018_eu_consumer_protection_2.0.pdf

¹⁹⁵ Behavioral study on unfair commercial practices in the digital environment: dark patterns and manipulative personalisation. European Commission. 2022. Lk 6.

¹⁹⁶ OECD (2022), "Dark commercial patterns", *OECD Digital Economy Papers*, No. 336, OECD Publishing, Paris, <https://doi.org/10.1787/44f5e846-en>. Lk. 24.

afforded protection equivalent to that afforded by other products and services.¹⁹⁷ The recent 2024 Artificial Intelligence Act has by now entered into force, and in this paper I assess the extent to which it has succeeded in providing such equivalent protection, with a specific focus on AI-related dark patterns.

The AI Act uses a risk-based approach and categorises the uses of AI into four growing risk categories according to the harm they could potentially cause:

- (a) minimal risk uses that are not mandatorily regulated;
- (b) limited-risk uses subject to transparency obligations to the user;
- (c) high-risk uses subject to more extensive transparency and testing standards and oversight;
- (d) unacceptable risk uses which are prohibited.

Dark patterns are limited in particular by Article 5 of the AI Act, which deals with the highest level of risk, i.e. unacceptable risk, for AI systems. Namely, the first paragraph of Article 5 prohibits AI systems "which use techniques aimed at the subliminal perception beyond human consciousness, or which use deliberately manipulative or deceptive techniques, the object or effect of which is to cause significant distortion of the behaviour of a person or a group of persons, thereby significantly impairing their ability to make an informed decision and causing them to make a decision that they would not have made otherwise, in a way that causes or is reasonably likely to cause substantial harm to that person, another person or a group of persons".

Such an approach has important shortcomings that exclude from protection many of the harms caused by dark patterns - for example, through the high standard of causing significant harm and the difficulty of causally linking such harm to AI activity. The harm caused by AI is often systemic, widespread, and may only become apparent at a later stage,¹⁹⁸ so that it is not sufficient to assess harm to an individual or group of individuals at the moment the AI system is placed on the market. These and other shortcomings of the AI Act are analysed in more detail.

¹⁹⁷ Komisjoni teatis Euroopa Parlamendile ja Nõukogule. Uus tarbijakaitse tegevuskava. 13.11.2020. <https://eur-lex.europa.eu/legal-content/ET/TXT/HTML/?uri=CELEX:52020DC0696>

¹⁹⁸ Kaminski, Margot E., The Developing Law of AI: A Turn to Risk Regulation (April 12, 2023). The Digital Social Contract: A Lawfare Paper Series (April 2023), U of Colorado Law Legal Studies Research Paper No. 24-5, Lk 3. Available at SSRN: <https://ssrn.com/abstract=4692562> or <http://dx.doi.org/10.2139/ssrn.4692562>

To address the shortcomings, and to more effectively counter the problem of AI-enhanced and enabled dark patterns, in the third chapter I propose a regulative model based on the capabilities inherent in AI when the use of those capabilities corresponds to the characteristics of dark patterns. The proposed model is technology-neutral, more future-proof, and allows for easier *ex ante* evaluation of negative effects.

The aim of this thesis is to assess whether the use of AI-based dark patterns is effectively regulated by the existing EU legislation and to propose an alternative AI capability-based model for regulating these AI-based dark patterns in order to fill the potential gaps in legislation.

The structure of the thesis consists of a descriptive part in the first chapter, which gives an overview of the progression of the problem of dark patterns in the digital environment and the nature of typical dark patterns, and describes the complexity of defining the concept of dark patterns and creating a comprehensive taxonomy. The second chapter consists of an analytical section that assesses the effectiveness of existing EU regulations in protecting the problem in context, and the third chapter contains a normative section that provides recommendations to address the identified bottlenecks and an overview of whether the shortcomings were addressed.

Kasutatud kirjandus

1. Blackie, Daniel. Disability in the Industrial Revolution. <https://library.oapen.org/handle/20.500.12657/30580>
2. Gupta, Maanak, et al. "From ChatGPT to ThreatGPT: Impact of generative AI in cybersecurity and privacy." *IEEE Access* (2023).
3. Lubarsky, Boris. Re-Identification of "Anonymized" Data. 1 GEO. L. TECH. REV. 202 (2017).
4. Mok, Aaron. ChatGPT will no longer comply if you ask it to repeat a word 'forever'—after a recent prompt revealed training data and personal info. <https://www.businessinsider.com/chatgpt-ai-refuse-to-respond-prompt-asking-repeat-word-forever-2023-12>
5. Schwab, Klaus. "The Fourth Industrial Revolution." *Foreign Affairs*, 12 December 2015, <https://www.foreignaffairs.com/world/fourth-industrial-revolution>. Accessed 22 December 2023.
6. The impact of the General Data Protection Regulation (GDPR) on artificial intelligence. EPRS. June 2020.
7. Brignull, H., Leiser, M., Santos, C., & Doshi, K. (2023, April 25). *Deceptive patterns – user interfaces designed to trick you*. deceptive.design. Retrieved 27.03.2025, from <https://www.deceptive.design/>
8. OECD (2022), "Dark commercial patterns", *OECD Digital Economy Papers*, No. 336, OECD Publishing, Paris, <https://doi.org/10.1787/44f5e846-en>.
9. Behavioral study on unfair commercial practices in the digital environment: dark patterns and manipulative personalisation. European Commission. 2022.
10. Komisjoni teatis Euroopa Parlamendile ja Nõukogule. Uus tarbijakaitse tegevuskava. 13.11.2020. <https://eur-lex.europa.eu/legal-content/ET/TXT/HTML/?uri=CELEX:52020DC0696>
11. Mission letter to Michael McGrath. Ursula von der Leyen. https://commission.europa.eu/document/download/907fd6b6-0474-47d7-99da-47007ca30d02_en?filename=Mission%20letter%20-%20McGRATH.pdf
12. Helberger, Micklitz H.-W. et al. (2021) "Structural asymmetries in digital consumer markets", study for BEUC. https://www.beuc.eu/sites/default/files/publications/beuc-x-2021-018_eu_consumer_protection_2.0.pdf
13. Kaminski, Margot E., The Developing Law of AI: A Turn to Risk Regulation (April 12, 2023). The Digital Social Contract: A Lawfare Paper Series (April 2023), U of Colorado Law Legal Studies Research Paper No. 24-5, Lk 3. Available at SSRN: <https://ssrn.com/abstract=4692562> or <http://dx.doi.org/10.2139/ssrn.4692562>
14. Emma Calvert. Food marketing needs rules with teeth. 2021. The European Consumer Organisation.

- https://www.beuc.eu/sites/default/files/publications/beuc-x-2021-084_food_marketing_to_children_needs_rules_with_teeth.pdf
15. Consumer empowerment in the digital economy: A critical analysis of the Cameroonian
 16. law on consumer protection in the digital age. Akama Samuel Penda. International Journal of Law. 2022. <https://www.lawjournals.org/assets/archives/2022/vol8issue4/8-4-14-240.pdf>
 17. Consumer market study on online market segmentation through personalised pricing/offers in the European Union. Final report. 2018. https://commission.europa.eu/publications/consumer-market-study-online-market-segmentation-through-personalised-pricingoffers-european-union_en
 18. Consumer market study on online market segmentation through personalised pricing/offers in the European Union. Final report. 2018. https://commission.europa.eu/publications/consumer-market-study-online-market-segmentation-through-personalised-pricingoffers-european-union_en
 19. Behavioral study on unfair commercial practices in the digital environment: dark patterns and manipulative personalisation. European Commission. 2022.
 20. Stigler Committee on Digital Platforms: Final Report. 2019.
 21. Brynjolfsson, Erik, and Michael D. Smith. "Frictionless Commerce? A Comparison of Internet and Conventional Retailers." *Management Science*, vol. 46, no. 4, 2000, pp. 563–85. *JSTOR*, <http://www.jstor.org/stable/2661602>. Accessed 5 Apr. 2025. Lk 1.
 22. Perkins et al v. LinkedIn Corp. 13-CV-04303-LHK.
 23. Helberger, Micklitz H.-W. et al. (2021) "Structural asymmetries in digital consumer markets", study for BEUC, Lk. 108. https://www.beuc.eu/sites/default/files/publications/beuc-x-2021-018_eu_consumer_protection_2.0.pdf

Lihtlitsents lõputöö reprodutseerimiseks ja üldsusele kättesaadavaks tegemiseks

Mina, _____,
Saara Arianne Avesti

1. annan Tartu Ülikoolile tasuta loa (lihtlitsentsi) minu loodud teose

TEHISINTELLEKTIGA SEOTUD TUMEDATE MUSTRITE REGULEERIMINE VÕIMETEPÕHISE MUDELI ABIL

(lõputöö pealkiri)

Mario Rosentau

mille juhendaja(d) on _____ ,
(juhendaja nimi)

reprodutseerimiseks eesmärgiga seda säilitada, sealhulgas lisada Tartu Ülikooli digitaalarhiivi kuni autoriõiguse kehtivuse lõppemiseni;

2. annan Tartu Ülikoolile loa teha punktis 1 nimetatud teos üldsusele kättesaadavaks Tartu Ülikooli veebikeskkonna, sealhulgas digitaalarhiivi kaudu Creative Commons'i litsentsiga CC BY NC ND 4.0, mis lubab autorile viidates teost reprodutseerida, levitada ja üldsusele suunata ning keelab luua tuletatud teost ja kasutada teost ärieesmärgil, kuni autoriõiguse kehtivuse lõppemiseni;
3. olen teadlik, et punktides 1 ja 2 nimetatud õigused jäävad alles ka autorile;
4. kinnitan, et lihtlitsentsi andmisega ei riku ma teiste isikute intellektuaalomandi ega isikuandmete kaitse õigusaktidest tulenevaid õigusi.

Saara Arianne Avestik
29.04.2026