



Brüssel, 29.7.2025
C(2025) 5052 final

KOMISJONI TEATIS

**Komisjoni suunised määruses (EL) 2024/1689 (tehisintellektimäärus) kehtestatud
tehisintellekti keelatud kasutusviiside kohta**

SISUKORD

1. Taust ja eesmärgid	1
2. Ülevaade keelatud tehisintellekti kasutusviisidest	2
2.1. Tehisintellektimääruse artiklis 5 loetletud keelud.....	2
2.2. Keeldude õiguslik alus	4
2.3. Sisuline kohaldamisala: tehisintellektisüsteemi turule laskmise, kasutusele võtmise või kasutamiseiga seotud kasutusviisid.....	4
2.4. Isikuline kohaldamisala: vastutav osaleja	5
2.5. Väljajätmine tehisintellektimääruse kohaldamisalast	7
2.5.1. Riikliku julgeoleku, kaitse- ja sõjalised eesmärgid.....	7
2.5.2. Õigusala ja õiguskaitseala koostöö kolmandate riikidega	9
2.5.3. Teadus- ja arendustegevus	9
2.5.4. Isiklik, mitte kutseline tegevus.....	11
2.5.5. Tasuta ja avatud lähtekoodiga litsentside alusel avaldatud tehisintellektisüsteemid	12
2.6. Keeldude ja suure riskiga tehisintellektisüsteemide nõuete koostoime	12
2.7. Keeldude kohaldamine üldotstarbeliste tehisintellektisüsteemide ja sihtotstarbeliste süsteemide suhtes.....	13
2.8. Keeldude ja muude liidu õigusaktide vastastikune mõju	14
2.9. Tehisintellektimääruse artikli 5 jõustamine	17
2.9.1. Turujärelevalveasutused.....	17
2.9.2. Karistused	18
3. Tehisintellektimääruse artikli 5 lõike 1 punktid a ja b – kahjulik manipuleerimine, pettus ja ärakasutamine	18
3.1. Põhjendus ja eesmärgid.....	19
3.2. Tehisintellektimääruse artikli 5 lõike 1 punktis a sätestatud keelu põhikomponendid – kahjulik manipuleerimine	19
3.2.1. Alalävisele tajule suunatud, sihipäraselt manipuleerivad või petlikud võtted	20
3.2.2. Eesmärgiga moonutada oluliselt isiku või isikute rühma käitumist.....	25
3.2.3. Põhjustab (mõistliku tõenäosusega) olulist kahju	28
3.3. Tehisintellektimääruse artikli 5 lõike 1 punktis b sätestatud keelu põhikomponendid – haavatavuse kahjulik ärakasutamine	33
3.3.1. Vanusest, puudest või konkreetsest sotsiaalsest või majanduslikust olukorrast tingitud haavatavuste ärakasutamine	34
3.3.2. Eesmärk või tagajärg on käitumise oluline moonutamine	39
3.3.3. Põhjustab (mõistliku tõenäosusega) olulist kahju	39
3.4. Tehisintellektimääruse artikli 5 lõike 1 punktides a ja b sätestatud keeldude vastastikune mõju	43
3.5. Kohaldamisalast välja jäävad olukorrad	44
3.5.1. Seaduslik veenmine.....	44

3.5.2.	Manipuleerivad, petlikud ja eksploateerivad tehisintellektisüsteemid, mis tõenäoliselt ei tekita olulist kahju	46
3.6.	Koostoime muude liidu õigusaktidega	47
4.	Tehisintellektimääruse artikli 5 lõike 1 punkt c – sotsiaalpunktide andmine	51
4.1.	Põhjendus ja eesmärgid	51
4.2.	Sotsiaalpunktide andmise keelu põhimõisted ja komponendid	51
4.2.1.	Sotsiaalpunktide andmine: hindamine või liigitamine sotsiaalse käitumise või isiku- või iseloomuomaduste alusel teatud aja jooksul	53
4.2.2.	Sotsiaalpunktid peavad tooma kaasa kohtlemise, mis on mitteseotud sotsiaalses kontekstis kahjustav või ebasoodne ja/või sotsiaalse käitumise kaalukusega võrreldes põhjendamatu või ebaproportsionaalne	55
4.2.3.	Sõltumata sellest, kas neid pakuvad või kasutavad avaliku või erasektori osalejad	60
4.3.	Kohaldamisalast välja jäävad olukorrad	61
4.4.	Koostoime teiste liidu õigusaktidega	64
5.	Tehisintellektimääruse artikli 5 lõike 1 punkt d – KURITEGUDE prognoosimine ja individuaalne riskianalüüs	65
5.1.	Põhjendus ja eesmärgid	66
5.2.	Keelu põhimõisted ja komponendid	66
5.2.1.	Kuriteo toimepanemise riski hindamine või prognoosimine	67
5.2.2.	Üksnes füüsilise isiku profiilianalüüsil või tema isikuomaduste ja erijoonte hindamisel põhinev tegevus	68
5.2.3.	Tehisintellektisüsteemide välistamine, et toetada inimhinnangut, mis põhineb objektiivsetel ja kontrollitavatel faktidel, mis on otseselt seotud kuritegeliku tegevusega	71
5.2.4.	Millises ulatuses võib eraõiguslike osalejate tegevus kuuluda kohaldamisalasse	72
5.3.	Kohaldamisalast välja jäävad olukorrad	73
5.3.1.	Asukohapõhine või georuumiline või kohapõhine kuritegevuse prognoosimine	73
5.3.2.	Tehisintellektisüsteemid, mis toetavad inimhinnanguid, tuginedes kuritegeliku tegevusega seotud objektiivsetele ja kontrollitavatele faktidele	74
5.3.3.	Tehisintellektisüsteemid, mida kasutatakse kuritegevuse prognoosimiseks ja hindamiseks seoses juriidiliste isikutega	76
5.3.4.	Haldusrikkumiste individuaalsete prognooside tegemiseks kasutatavad tehisintellektisüsteemid	76
5.4.	Koostoime teiste liidu õigusaktidega	77
6.	Tehisintellektimääruse artikli 5 lõike 1 punkt e – näokujutiste kindla suunitluseta ekstraheerimine	78
6.1.	Põhjendus ja eesmärgid	78
6.2.	Keelu põhimõisted ja komponendid	78
6.2.1.	Näotuvastuse andmebaasid	79
6.2.2.	Näokujutiste kindla suunitluseta ekstraheerimine	79
6.2.3.	Internetist ja videovalve salvestistest	80

6.3.	Kohaldamisalast välja jäävad olukorrad	80
6.4.	Koostoime teiste liidu õigusaktidega	81
7.	Tehisintellektimääruse artikli 5 lõike 1 punkt f – emotsioonituvastus.....	81
7.1.	Põhjendus ja eesmärgid.....	81
7.2.	Keelu põhimõisted ja komponendid	82
7.2.1.	Tehisintellektisüsteemid emotsioonide tuletamiseks	83
7.2.2.	Keelu piiramine töökoha ja haridusasutustega.....	86
7.2.3.	Erandid meditsiinilistel ja ohutusega seotud põhjustel	88
7.3.	Soodsamad liikmesriikide õigusaktid	90
7.4.	Kohaldamisalast välja jäävad olukorrad	90
8.	Tehisintellektimääruse artikli 5 lõike 1 punkt g: biomeetriline liigitamine teatavate tundlike omaduste puhul	91
8.1.	Põhjendus ja eesmärgid.....	92
8.2.	Keelu põhimõisted ja komponendid	92
8.2.1.	Biomeetrilise liigitamise süsteem	93
8.2.2.	Isikuid liigitatakse individuaalselt nende biomeetriliste andmete alusel	94
8.2.3.	Et tuletada või järeldada nende rassi, poliitilisi vaateid, ametiühingusse kuulumist, usulisi või filosoofilisi veendumusi, seksuaalelu või seksuaalset sättumust.....	95
8.3.	Kohaldamisalast välja jäävad olukorrad	95
8.4.	Koostoime muude liidu õigusaktidega.....	96
9.	Tehisintellektimääruse artikli 5 lõike 1 punkt h – reaajas toimuva biomeetrilise kaugtuvastamise süsteemid õiguskaitse eesmärgil.....	97
9.1.	Põhjendus ja eesmärgid.....	98
9.2.	Keelu põhimõisted ja komponendid	98
9.2.1.	Biomeetrilise kaugtuvastuse mõiste.....	99
9.2.2.	Reaalajas	102
9.2.3.	Avalikult juurdepääsetav ruum	102
9.2.4.	Õiguskaitse eesmärk	104
9.3.	Erandid keelust.....	106
9.3.1.	Põhjendus ja eesmärgid.....	106
9.3.2.	Kolme liiki raskete kuritegude ohvrite ja kadunud isikute sihipärane otsimine	107
9.3.3.	Otseste elu ähvardavate ohtude ja terrorirünnakute ärahoidmine	108
9.3.4.	Teatud kuritegudes kahtlustatavate isikute asukoha kindlaksmääramine ja tuvastamine	111
10.	Kaitsemeetmed ja erandite tegemise tingimused (tehisintellektimääruse artikli 5 lõiked 2–7)....	113
10.1.	Sihimärgiks olev isik ja kaitsemeetmed (tehisintellektimääruse artikli 5 lõige 2).....	114
10.1.1.	Põhiõigustele avalduva mõju hindamine	116
10.1.2.	Lubatud biomeetrilise kaugtuvastamise süsteemide registreerimine	121

10.2.	Eelneva loa vajadus.....	121
10.2.1.	Eesmärk.....	122
10.2.2.	Peamine põhimõte Eelnev luba õigusasutuselt või sõltumatult haldusasutuselt.....	123
10.3.	Ametivõimude teavitamine iga kord, kui reaalajas toimuva biomeetrilise kaugtuvastamise süsteemi kasutatakse avalikult juurdepääsetavas ruumis õiguskaitse eesmärgil	129
10.4.	Vajadus riigisiseste õigusaktide järele, mis jäävad tehisintellektimääruse erandite piiridesse	129
10.4.1.	Põhimõte: vaja on riigisisest õigusakti, mis annab õigusliku aluse kõigi või mõne(de) erandi(te) jaoks loa andmiseks.....	129
10.4.2.	Riigisisene õigus peab järgima tehisintellektimääruse artikli 5 lõike 1 punktis h sätestatud piiranguid ja tingimusi	130
10.4.3.	Üksikasjalikud riigisisest õigusaktid loa taotlemise, andmise ja kasutamise kohta	131
10.4.4.	Üksikasjalikud riigisisest õigusaktid, mis käsitlevad järelevalvet ja aruandlust seoses loa andmisega	132
10.5.	Riiklike turujärelevalveasutuste ja liikmesriikide andmekaitseasutuste aastaaruanded..	132
10.6.	Komisjoni aastaaruanded	133
10.7.	Kohaldamisalast välja jäävad olukorrad	133
10.8.	Kasutusnäited	135
11.	Kohaldamine	137
12.	Komisjoni suuniste läbivaatamine ja ajakohastamine.....	137

1. TAUST JA EESMÄRGID

- (1) Euroopa Parlamendi ja nõukogu 13. juuni 2024. aasta määrus (EL) 2024/1689, millega nähakse ette tehisintellekti käsitlevad ühtlustatud õigusnormid (tehisintellektimäärus),¹ jõustus 1. augustil 2024. Tehisintellektimäärusega kehtestatakse ühtlustatud õigusnormid tehisintellekti (AI) turule laskmise, kasutusele võtmise ja kasutamise kohta liidus². Selle eesmärk on edendada innovatsiooni ja tehisintellekti kasutusele võtmist, tagades samal ajal tervise, ohutuse ja põhiõiguste, sealhulgas demokraatia ja õigusriigi põhimõtete kõrgetasemelise kaitse liidus.
- (2) Tehisintellektimäärus määrus järgib riskipõhist lähenemisviisi, liigitades tehisintellektisüsteemid nelja erinevasse riskikategooriasse:
 - (i) vastuvõetamatu risk: tehisintellektisüsteemid, mis kujutavad endast vastuvõetamatut ohtu põhiõigustele ja liidu väärtustele, on tehisintellektimääruse artikli 5 kohaselt keelatud;
 - (ii) suur risk: tervisele, ohutusele ja põhiõigustele suurt ohtu kujutavate tehisintellektisüsteemide suhtes kehtib hulk nõudeid ja kohustusi. Need süsteemid on liigitatud „suure riskiga“ süsteemideks vastavalt tehisintellektimääruse artiklile 6 koostoimes sama määruse I ja III lisaga;
 - (iii) läbipaistvuse risk: tehisintellektisüsteemide suhtes, mis tekitavad piiratud läbipaistvusrisiki, kohaldatakse tehisintellektimääruse artikli 50 alusel läbipaistvuskohustusi;
 - (iv) risk on minimaalne või puudub: tehisintellektisüsteemid, mis kujutavad endast minimaalset või olematut riski, ei reguleerita, kuid pakkujad ja juurutajad võivad vabatahtlikult järgida vabatahtlikke tegevusjuhendeid³.
- (3) Vastavalt tehisintellektimääruse artikli 96 lõike 1 punktide b peab komisjon vastu võtma suunised tehisintellektimääruse artiklis 5 keelatud kasutusviiside praktilise rakendamise kohta. Neid keelde hakatakse kohaldama kuus kuud pärast tehisintellektimääruse jõustumist, st alates 2. veebruarist 2025.
- (4) Nende suuniste eesmärk on suurendada õiguslikku selgust ja anda ülevaade sellest, kuidas komisjon tõlgendab tehisintellektimääruse artiklis 5 sätestatud keelde, et tagada nende järjepidev, tõhus ja ühtne kohaldamine. Need peaksid olema praktilised juhised, mis aitavad tehisintellektimääruses sätestatud pädevaid asutusi oma jõustamistegevuses ning tehisintellektisüsteemide pakkujatel ja juurutajatel tagada oma kohustuste täitmise. Neis püütakse tõlgendada keelde proportsionaalselt, et saavutada tehisintellektimääruse eesmärgid, s.o põhiõiguste ja ohutuse kaitsmine, edendades samal ajal innovatsiooni ja tagades õiguskindluse.

¹ Euroopa Parlamendi ja nõukogu 13. juuni 2024. aasta määrus (EL) 2024/1689, millega nähakse ette tehisintellekti käsitlevad ühtlustatud õigusnormid (tehisintellekti käsitlev määrus) (ELT L, 2024/1689, 12.7.2024).

² Tehisintellektimääruse artikkel 1.

³ Tehisintellektimääruse artikkel 95.

- (5) Need suunised ei ole siduvad. Tehisintellektimääruse autoriteetse tõlgenduse võib lõppkokkuvõttes anda ainult Euroopa Liidu Kohus.
- (6) Nende suuniste koostamisel lähtuti komisjoni korraldatud laiaulatusliku konsultatsiooniprotsessi käigus kogutud vastustest, mille andsid mitmesugused sidusrühmad, nt tehisintellektisüsteemide pakkujad ja juurutajad, kodanikuühiskonna organisatsioonid, akadeemilised ringkonnad, ametiasutused, ettevõtjate ühendused jne. Konsulteeriti ka Euroopa tehisintellekti nõukoja liikmesriikide ja Euroopa Parlamendiga. Käesolevad suunised vaadatakse korrapäraselt läbi, võttes arvesse tehisintellektimääruse artikli 5 praktilisest rakendamisest saadud kogemusi ning tehnoloogia ja turu arengut.
- (7) Tehisintellektimääruse artikli 5 kohaldamine nõuab iga juhtumi puhul eraldi hindamist, mille puhul võetakse nõuetekohaselt arvesse iga juhtumiga seotud konkreetset olukorda. Seetõttu on nendes suunistes toodud näited üksnes soovituslikud ja ei piira iga juhtumi puhul vajadust sellise hindamise järele.

2. ÜLEVAADE KEELATUD TEHISINTELLEKTI KASUTUSVIISIDEST

- (8) Tehisintellektimääruse artikliga 5 keelatakse teatavate tehisintellektisüsteemide turule laskmine, kasutusele võtmine või kasutamine manipuleerimiseks, ärakasutamiseks, sotsiaalseks kontrolliks või jälgimiseks, mis oma olemuselt rikub põhiõigusi ja liidu väärtusi. Tehisintellektimääruse põhjenduses 28 selgitatakse, et sellised kasutusviisid on eriti kahjulikud ja kuritarvituslikud ning tuleks keelata, sest need on vastuolus selliste liidu väärtustega nagu inimväärikuse austamine, vabadus, võrdsus, demokraatia ja õigusriik ning Euroopa Liidu põhiõiguste hartas (edaspidi „harta“) sätestatud põhiõigustega, kaasa arvatud õigusega mittediskrimineerimisele (harta artikkel 21) ja võrdsusele (artikkel 20), andmekaitsele (harta artikkel 8) ning era- ja perekonnaelu austamisele (harta artikkel 7), aga ka lapse õigustega (harta artikkel 24). Tehisintellektimääruse artikli 5 keeldude eesmärk on kaitsta ka õigust sõna- ja teabevabadusele (harta artikkel 11), kogunemis- ja ühinemisvabadusele (harta artikkel 12), mõtte-, südametunnistuse- ja usuvabadusele (harta artikkel 10), õigust tõhusale õiguskaitsevahendile ja õiglasele kohtulikule arutamisele (harta artikkel 47) ning süütuse presumptsiooni ja kaitseõigust (harta artikkel 48).

2.1. Tehisintellektimääruse artiklis 5 loetletud keelud

- (9) Ülevaade keeldudest

Säte	Keeld	Sisu
Artikli 5 lõike 1 punkt a	Kahjulik manipuleerimine ja pettus	Tehisintellektisüsteemid, milles on kasutatud inimese teadvusest kaugemale ulatuvale alalävisele tajule suunatud võtteid või sihilikult manipuleerivaid või petlikke võtteid, mille eesmärk või tagajärg on isiku või isikute rühma käitumise oluline moonutamine viisil, mis põhjustab või mõistliku tõenäosusega põhjustab sellele isikule, teisele isikule või isikute rühmale olulist kahju

Artikli 5 lõike 1 punkt b	Haavatavuste kahjulik ärakasutamine	Tehisintellektisüsteemid, mis kasutavad ära vanusest, puudest või konkreetsest sotsiaalsest või majanduslikust olukorrast tulenevaid haavatavusi ning mille eesmärk või tagajärg on oluliselt moonutada käitumist viisil, mis põhjustab või mõistliku tõenäosusega põhjustab olulist kahju
Artikli 5 lõike 1 punkt c	Sotsiaalpunktide andmine	Tehisintellektisüsteemid, millega hinnatakse või liigitatakse füüsilisi isikuid või isikute rühmi teatava aja jooksul, tuginedes nende sotsiaalsele käitumisele või isiku- või iseloomuomadustele, kusjuures sotsiaalpunktide tulemuseks on kahjustav või ebasoodne kohtlemine sotsiaalses kontekstis, mis ei ole seotud kontekstiga, milles andmed algselt loodi või koguti, või mis ei ole põhjendatud või on võrreldes sotsiaalse käitumisega ebaproportsionaalne
Artikli 5 lõike 1 punkt d	Isiku kuritegevuse riski hindamine ja prognoosimine	Tehisintellektisüsteemid, mis hindavad või prognoosivad riski, et inimene paneb toime kuriteo, tuginedes üksnes profiilialalüüsile või isikuomaduste ja erijoonte hindamisele, välja arvatud selleks, et toetada inimhinnangut, mis tugineb kuritegeliku tegevusega otseselt seotud objektiivsetele ja kontrollitavatele faktidele
Artikli 5 lõike 1 punkt e	Kindla suunitluseta ekstraheerimine näotuvastuse andmebaaside arendamiseks	Tehisintellektisüsteemid, mis loovad või laiendavad näotuvastuse andmebaase internetist või videovalve salvestistest näokujutiste kindla suunitluseta ekstraheerimise kaudu
Artikli 5 lõike 1 punkt f	Emotsioonituvastus	Tehisintellektisüsteemid, mis tuletavad emotsioone töökohal või haridusasutustes, välja arvatud meditsiinilistel või ohutusega seotud põhjustel
Artikli 5 lõike 1 punkt g	Biomeetriline liigitamine	Tehisintellektisüsteemid, mis liigitavad inimesi nende biomeetriliste andmete põhjal, et järeldada või tuletada nende rassi, poliitilisi vaateid, ametiühingusse kuulumist, usulisi või filosoofilisi veendumusi, seksuaalelu või seksuaalset sättumust, välja arvatud seaduslikult saadud biomeetriliste andmete märgistamine või filtreerimine, sealhulgas õiguskaitse valdkonnas
Artikli 5 lõike 1 punkt h	Reaalajas toimuv biomeetriline kaugtuvastamine	Tehisintellektisüsteemid avalikult juurdepääsetavas ruumis reaalajas toimuva biomeetrilise kaugtuvastamise süsteemide kasutamine õiguskaitse jaoks, välja arvatud juhul, kui see on vajalik konkreetsete ohvrite sihipäraseks otsimiseks, konkreetsete ohtude, sealhulgas terrorirünnakute ärahoidmiseks, või konkreetsetes õigusrikkumises kahtlustatava isiku otsimiseks (täpsemad

menetlusnõuded, sealhulgas loa saamiseks, on sätestatud tehisintellektimääruse artikli 5 lõigetes 2–7)

2.2. Keeldude õiguslik alus

- (10) Tehisintellektimäärus määrus tugineb kahele õiguslikule alusele: Euroopa Liidu toimimise lepingu (edaspidi „ELi toimimise leping“) artikkel 114 (siseturu õiguslik alus) ja ELi toimimise lepingu artikkel 16 (andmekaitse õiguslik alus). ELi toimimise lepingu artikkel 16 on õiguslikuks aluseks isikuandmete töötlemise erieeskirjadele seoses keeluga kasutada biomeetrilise kaugtuvastamise süsteeme õiguskaitse eesmärgil, biomeetrilise liigitamise süsteeme õiguskaitse eesmärgil ja individuaalset riskihindamist õiguskaitse eesmärgil⁴. Kõigi muude tehisintellektimääruse artiklis 5 loetletud keeldude õiguslik alus on ELi toimimise lepingu artikkel 114.

2.3. Sisuline kohaldamisala: tehisintellektisüsteemi turule laskmise, kasutusele võtmise või kasutamisega seotud kasutusviisid

- (11) Tehisintellektimääruse artikliga 5 keelatud kasutusviisid on seotud konkreetsete tehisintellektisüsteemide turule laskmise, kasutusele võtmise või kasutamisega⁵. Reaalajas toimuva biomeetrilise kaugtuvastamise süsteemide puhul kohaldatakse tehisintellektimääruse artikli 5 lõike 1 punktis h sätestatud keeldu ainult nende kasutamise suhtes. Tehisintellektimääruse artikli 3 punktis 1 on määratletud, mida tähendab „tehisintellektisüsteem“. Suunistes tehisintellektisüsteemi määratluse kohta on esitatud komisjoni tõlgendus selle määratluse kohta.
- (12) Vastavalt tehisintellektimääruse artikli 3 punktile 9 on tehisintellektisüsteemi **turule laskmine** „tehisintellektisüsteemi [...] liidu turul esmakordselt kättesaadavaks tegemine“. „Kättesaadavaks tegemine“ on määratletud kui süsteemi „tasu eest või tasuta tarnimine liidu turule kaubandustegevuse käigus kas turustamiseks või kasutamiseks“⁶. See hõlmab tehisintellektisüsteemi kättesaadavaks tegemist sõltumata tarnimise viisist, näiteks juurdepääs süsteemile ja selle teenusele rakendusliidese („API“) kaudu, pilve kaudu, otse allalaadimise teel, füüsilise koopiana või füüsilistesse toodetesse integreeritud kujul.

Näiteks väljaspool liitu kolmanda riigi pakkuja poolt välja töötatud biomeetrilise kaugtuvastamise süsteem lastakse esmakordselt liidu turule, kui seda pakutakse tasu eest või tasuta ühes või mitmes liikmesriigis. Selliseks turule laskmiseks võib pakkuda juurdepääsu süsteemile veebipõhise rakendusliidese või muu kasutajaliidese kaudu.

⁴ Tehisintellektimääruse põhjendus 3. ELi toimimise lepingu artiklil 16 põhinevate keeldude puhul kehtivad Iirimaa ja Taani suhtes kaks asjakohast loobumisklauslit. Euroopa Liidu lepingule ja ELi toimimise lepingule lisatud protokolli nr 21 (Ühendkuningriigi ja Iirimaa seisukoha kohta vabadusel, turvalisusel ja õigusel rajaneva ala suhtes) alusel Iirimaaale antud kaalutlusõiguse alusel võib Iirimaa otsustada mitte kohaldada õigusnorme, mis käsitlevad keeldu kasutada õiguskaitse eesmärgil reaalajas toimuvat biomeetrilist kaugtuvastamist avalikus ruumis, ning selle artikliga seotud menetlusnorme (tehisintellektimääruse artikli 5 lõiked 2–6) (vt põhjendus 40). Taani saab Euroopa Liidu lepingu ja ELi toimimise lepingu protokolli nr 22 kohaldamisel kasutada loobumiskokkuleppeid ning võib otsustada, et ta ei kohalda ELi toimimise lepingu artiklil 16 põhinevaid keelde täies ulatuses (vt põhjendus 41).

⁵ Nende mõistete määratlusi vt komisjoni 2022. aasta teatise „Sinine raamat ELi toote-eeskirjade rakendamise kohta“ (2022/C 247/01) punktist 2.

⁶ Tehisintellektimääruse artikli 3 punkt 10.

- (13) Tehisintellektimääruse artikli 3 punktis 11 on **kasutusele võtmine** määratletud kui „tehisintellektisüsteemi tarnimine esmakordseks kasutamiseks otse juurutajale või oma tarbeks, et kasutada seda sihtotstarbeliselt liidus“, mis hõlmab nii tarnimist esmakordseks kasutamiseks kolmandatele isikutele kui ka ettevõttesisest arendamist ja juurutamist. Süsteemi sihtotstarve on „kasutus, kaasa arvatud kasutamise konkreetne kontekst ja tingimused, mille jaoks pakkuja on tehisintellektisüsteemi kasutusjuhendis, reklaam- või müügimaterjalides või avaldustes ning tehnilistes dokumentides esitatud teabe kohaselt ette näinud“⁷.

Näiteks loob pakkuja väljaspool liitu biomeetrilise kaugtuvastamise süsteemi ja tarnib selle süsteemi esmakordseks kasutamiseks õiguskaitseasutusele või liikmesriigis asuvale eraettevõtjale, mille tulemusena võetakse see kasutusele.

Näiteks töötab ametiasutus asutusesiselt välja hindamissüsteemi ja hakkab seda juurutama, et prognoosida majapidamistoetuse saajate pettuse riski, mislähvi võetakse süsteem kasutusele.

- (14) Kuigi tehisintellektisüsteemi „**kasutamine**“ ei ole tehisintellektimääruses selgesõnaliselt määratletud, tuleks seda mõista laias tähenduses nii, et see hõlmab süsteemi kasutamist või juurutamist mis tahes hetkel selle elutsükli jooksul pärast turule laskmist või kasutusele võtmist. See võib hõlmata ka tehisintellektisüsteemi integreerimist tehisintellektisüsteemi kasutava(te) isiku(te) teenustesse ja protsessidesse, sealhulgas osana keerukamate süsteemidest, protsessidest või taristust. Kuigi tehisintellektisüsteemide pakkujad peavad enne oma tehisintellektisüsteemide turule laskmist kaaluma mõistlikult prognoositavaid kasutustingimusi (kavandatud kasutus ja mõistlikult prognoositav väärkasutamine),⁸ jäävad süsteemi seadusliku kasutamise tingimustega arvestamise eest vastutama juurutajad⁹. Tehisintellektimääruse artikli 5 kohaldamisel tuleks viidet kasutamisele mõista nii, et see hõlmab tehisintellektisüsteemi mis tahes väärkasutamist (olgu see mõistlikult prognoositav või mitte), mis võib endast kujutada keelatud kasutusviisi¹⁰.

Näiteks on keelatud tehisintellektisüsteem, mida tööandja kasutab emotsioonide tuletamiseks töökohal, välja arvatud juhul, kui seda kasutatakse meditsiinilistel või ohutusega seotud eesmärkidel (tehisintellektimääruse artikli 5 lõike 1 punkt f). Keeld kehtib juurutajate suhtes sõltumata sellest, kas pakkuja (süsteemi pakkuja) on oma lepingulistes suhetes juurutajaga (tööandjaga), st kasutustingimustes, sellise kasutamise välistanud.

2.4. Isikuline kohaldamisala: vastutav osaleja

- (15) Tehisintellektimääruses eristatakse tehisintellektisüsteemide puhul erinevaid operaatorite kategooriaid: pakkujad, juurutajad, importijad, turustajad ja toote

⁷ Tehisintellektimääruse artikli 3 punkt 12.

⁸ Vt tehisintellektimääruse artikli 3 punktid 12 ja 13.

⁹ Nende mõistete määratlusi vt komisjoni 2022. aasta teatise „Sinine raamat ELi toote-eeskirjade rakendamise kohta“ (2022/C 247/01) punktist 2.8.

¹⁰ Tehisintellektimääruse põhjendus 28.

valmistajad. Nendes suunistes keskendutakse ainult pakkujatele ja juurutajatele, arvestades tehisintellektimääruse artiklis 5 sätestatud keelatud kasutusviiside ulatust.

- (16) Tehisintellektimääruse artikli 3 punkti 3 kohaselt on **pakkujad** füüsilised või juriidilised isikud, ametiasutused, ametkonnad või muud organid, kes arendavad või kellel on tehisintellektisüsteeme ja kes lasevad neid liidu turule või võtavad neid kasutusele oma nime või kaubamärgi all¹¹ (vt eespool punkt 2.3). Väljaspool liitu asutatud või asuvate pakkujate suhtes kohaldatakse tehisintellektimääruse sätteid, kui nad lasevad kõnealused süsteemid liidus turule või võtavad need kasutusele¹² või kui tehisintellektisüsteemi väljundit kasutatakse liidus¹³. Enne tehisintellektisüsteemide turule laskmist või kasutusele võtmist peavad pakkujad tagama, et need vastavad kõigile asjakohastele nõuetele.

Näiteks biomeetrilise kaugtuvastamise süsteemi pakkuja on süsteemi valmistaja, kes turustab süsteemi liidus oma kaubamärgi all. Sellise süsteemi pakkujaks võib olla ka ametiasutus, kes arendab süsteemi välja asutusesiseselt ja võtab selle kasutusele oma tarbeks.

- (17) **Juurutajad** on füüsilised või juriidilised isikud, ametiasutused, ametkonnad või muud organid, kes kasutavad tehisintellektisüsteeme oma volituste alusel, välja arvatud juhul, kui tehisintellektisüsteemi kasutatakse isikliku, mitte kutselise tegevuse jaoks¹⁴. Tehisintellektisüsteemiga seotud volituste all tuleks mõista süsteemi juurutamise otsuse ja selle tegeliku kasutamise viisi eest vastutuse võtmist. Juurutajad kuuluvad tehisintellektimääruse kohaldamisalasse, kui nad on asutatud või asuvad liidus,¹⁵ või kolmandas riigis asumise korral siis, kui tehisintellektisüsteemi väljundit kasutatakse liidus¹⁶.
- (18) Kui tehisintellektisüsteemi juurutaja on juriidiline isik, kelle alluvuses süsteemi kasutatakse, st õiguskaitseasutus või eraõiguslik turvaettevõtte, ei tohiks selle isiku menetluste raames ja kontrolli all tegutsevaid töötajaid pidada juurutajateks. Juriidiline isik jääb juurutajaks ka siis, kui ta kaasab süsteemi käitamisega tema nimel ja vastutusel ning tema kontrolli all tegutsevad kolmandad isikud (nt töövõtjad, koosseisuvälised töötajad).
- (19) Operaatorid võivad täita tehisintellektisüsteemi puhul samal ajal rohkem kui ühte rolli. Näiteks kui operaator arendab ise oma tehisintellektisüsteemi, mida ta seejärel kasutab,

¹¹ Tehisintellektimääruse artikli 3 punktid 3, 9 ja 11. Seoses suure riskiga tehisintellektisüsteemidega on tehisintellektimääruse artiklis 25 ette nähtud, et „1. Turustajat, importijat, juurutajat või muud kolmandat isikut käsitletakse käesoleva määruse kohaldamisel suure riskiga tehisintellektisüsteemi pakkujana ning tema suhtes kohaldatakse artiklist 16 tulenevaid pakkuja kohustusi mis tahes järgmisel juhul: a) ta lisab juba turule lastud või kasutusele võetud suure riskiga tehisintellektisüsteemile oma nime või kaubamärgi, ilma et see piiraks selliste lepinguliste kokkulepete kohaldamist, milles sätestatakse, et kohustused on muul viisil jaotatud; b) nad teevad suure riskiga tehisintellektisüsteemi, mis on juba turule lastud või kasutusele võetud, olulise muudatuse viisil, et see jääb suure riskiga tehisintellektisüsteemiks vastavalt artiklile 6; c) nad muudavad tehisintellektisüsteemi, sealhulgas üldotstarbelisse tehisintellektisüsteemi, mida ei ole liigitatud suure riskiga tehisintellektisüsteemiks ja mis on juba turule lastud või kasutusele võetud, sihtotstarvet, nii et asjaomasest tehisintellektisüsteemist saab suure riskiga tehisintellektisüsteem vastavalt artiklile 6.“

¹² Tehisintellektimääruse artikli 2 lõike 1 punkt a.

¹³ Tehisintellektimääruse artikli 2 lõike 1 punkt c.

¹⁴ Tehisintellektimääruse artikli 3 punkt 4.

¹⁵ Tehisintellektimääruse artikli 2 lõike 1 punkt b.

¹⁶ Tehisintellektimääruse artikli 2 lõike 1 punkt c.

loetakse teda nii selle süsteemi pakkujaks kui ka juurutajaks, isegi kui seda süsteemi kasutavad ka teised juurutajad, kellele süsteem on antud tasuta eest või tasuta.

- (20) Tehisintellektimääruse pidevat järgimist nõutakse tehisintellekti elutsükli kõigis etappides. See eeldab liidu turule lastud või liidus kasutusele võetud tehisintellektisüsteemide pidevat jälgimist ja ajakohastamist, et tagada, et tehisintellektisüsteem vastab kogu oma elutsükli jooksul tehisintellektimäärusele ja et sellega ei kaasne tehisintellektimääruse artikli 5 kohaselt keelatud kasutusviis. Tehisintellektisüsteemide pakkujatel ja juurutajatel on erinevad kohustused sõltuvalt nende rollist ja kontrollist süsteemi projekteerimise, arendamise ja tegeliku kasutamise üle, et vältida keelatud kasutusviisi. Iga keelu puhul tuleks neid rolle ja kohustusi tõlgendada proportsionaalselt, võttes arvesse, kes väärtusahelas on kõige paremini võimeline võtma konkreetseid ennetus- ja leevendusmeetmeid ning tagama tehisintellektisüsteemide nõuetekohase arendamise ja kasutamise kooskõlas tehisintellektimääruse eesmärkide ja lähenemisviisiga.

2.5. Väljajätmine tehisintellektimääruse kohaldamisalast

- (21) Tehisintellektimääruse artiklis 2 on sätestatud rida üldisi erandeid, mis on tehisintellektimääruse artiklis 5 loetletud keeldude praktilise kohaldamise täielikuks mõistmiseks asjakohased.

2.5.1. Riikliku julgeoleku, kaitse- ja sõjalised eesmärgid

- (22) Tehisintellektimääruse artikli 2 lõike 3 kohaselt ei kohaldata määrust selliste valdkondade suhtes, mis ei kuulu liidu õiguse kohaldamisalasse, ning see ei mõjuta ühelgi juhul liikmesriikide pädevust seoses riikliku julgeolekuga, olenemata üksuse liigist, kellele liikmesriigid on usaldanud nende pädevustega seotud ülesannete täitmise. Tehisintellektimääruse kohaldamisalast jäetakse selgesõnaliselt välja tehisintellektisüsteemid, mis lastakse turule, võetakse kasutusele või mida kasutatakse muudatustega või ilma muudatusteta üksnes sõjalisel, kaitse- või riikliku julgeoleku eesmärgil, olenemata seda tegevust teostava üksuse liigist. Seega sõltub erandi kehtimine tehisintellektisüsteemi eesmärkidest või kasutusalaadest, mitte selle süsteemi abil tegutsevatest üksustest, mis võivad hõlmata ka eraettevõtjaid, kellele liikmesriigid on usaldanud nende pädevustega seotud ülesannete täitmise.
- (23) Euroopa Liidu Kohtu kohtupraktika kohaselt viitab mõiste „riigi julgeolek“ „esmatähtsale huvile kaitsta riigi põhifunktsioone ja ühiskonna põhihuve ning hõlmab selliste tegevuste – nagu terrorism – ennetamist ja mahasurumist, mis võivad tõsiselt destabiliseerida riigi põhilisi põhiseaduslikke, poliitilisi, majanduslikke või sotsiaalseid struktuure, eriti juhul, kui need kujutavad endast otsest ohtu ühiskonnale, elanikkonnale või riigile kui sellisele“¹⁷. Riiklik julgeolek ei hõlma näiteks liiklusohutusega seotud tegevusi¹⁸ ega kohtu korraldust või õigusemõistmist¹⁹. Euroopa Liidu Kohus on

¹⁷ Kohtuotsus, Euroopa Kohus, 6. oktoober 2020, La Quadrature du Net jt, C-511/18, C-512/18 ja C-520/18, EU:C:2020:791, punkt 135; Kohtuotsus, Euroopa Kohus, 5. juuni 2023, komisjon vs. Poola, C-204/21, EU:C:2023:442, punkt 318, milles viidatakse otsusele kohtuasjades C-439/19, punkt 67, ja C-306/21, punkt 40.

¹⁸ Kohtuotsus, Euroopa Kohus, 22. juuni 2021, Latvijas Republikas Saeima, C-439/19, EU:C:2021:504, punkt 68.

¹⁹ Kohtuotsus, Euroopa Kohus, 5. juuni 2023, komisjon vs. Poola, C-204/21, EU:C:2023:442, punkt 319.

märkinud, et „ehkki liikmesriikide pädevusse kuulub oma oluliste julgeolekuhuvide määratlemine ja asjakohaste meetmete kehtestamine oma sise- ja välisjulgeoleku tagamiseks, ei saa [...] asjaolu, et liikmesriigi meede on võetud riigi julgeoleku kaitsmise eesmärgil, tingida seda, et liidu õigus ei ole kohaldatav, ning vabastada liikmesriike vajadusest seda õigust järgida“²⁰.

- (24) Selleks, et tehisintellektimääruse artikli 2 lõike 3 teises lõigus sätestatud erandit saaks kohaldada, peab tehisintellektisüsteem olema turule lastud, kasutusele võetud või seda kasutatakse üksnes sõjalisel, kaitse- või riikliku julgeoleku eesmärgil. Määruse põhjenduses 24 on selgitatud põhjalikumalt, kuidas tuleks tõlgendada mõistet „üksnes“ ning millistel juhtudel võib sellisel eesmärgil kasutatav tehisintellektisüsteem siiski kuuluda tehisintellektimääruse kohaldamisalasse.

Näiteks kui sõjalisel, kaitse- või riikliku julgeoleku eesmärgil turule lastud, kasutusele võetud või kasutatavat tehisintellektisüsteemi kasutatakse (ajutiselt või alaliselt) muudel eesmärkidel, näiteks tsiviil- või humanitaareesmärkidel, õiguskaitse või avaliku julgeoleku eesmärgil, kuulub selline süsteem tehisintellektimääruse kohaldamisalasse. Sellisel juhul peaks üksus, kes kasutab tehisintellektisüsteemi muudel eesmärkidel, tagama tehisintellektisüsteemi vastavuse tehisintellektimäärusele, välja arvatud juhul, kui süsteem on määrusega juba kooskõlas, mida tuleb enne sellist kasutamist kontrollida.

- (25) Lisaks on tehisintellektimääruse põhjenduses 24 selgitatud, et tehisintellektisüsteemid, mis on turule lastud või kasutusele võetud määruse kohaldamisalast välja jäetud eesmärgil, nimelt sõjalisel, kaitse- või riikliku julgeoleku eesmärgil, ja ühel või mitmel määruse kohaldamisalasse kuuluval eesmärgil (nn **kahesuguse kasutusega** süsteemid), näiteks tsiviileesmärgil või õiguskaitse eesmärgil, kuuluvad kõnealuse määruse kohaldamisalasse. Nende süsteemide pakkujad peaksid tagama, et nad järgivad tehisintellektimääruse nõudeid.

Näiteks kui ettevõtte pakub biomeetrilise kaugtuvastamise süsteemi mitmesugustel eesmärkidel, sealhulgas õiguskaitse ja riikliku julgeoleku jaoks, on see ettevõtte sellise kahesuguse kasutusega süsteemi pakkuja ja peab tagama selle vastavuse tehisintellektimääruse nõuetele.

- (26) Asjaolu, et tehisintellektisüsteem võib kuuluda tehisintellektimääruse kohaldamisalasse, ei tohiks siiski mõjutada riigi julgeoleku, sõjalise ja kaitsetegevusega tegelevate üksuste võimet kasutada seda süsteemi riigi julgeoleku, sõjalisel ja kaitse-eesmärgil, olenemata sellest, millist liiki üksus seda tegevust ellu viib²¹.

Näiteks kui riiklik julgeolekuasutus või eraettevõtja saab riiklikult luureasutuselt ülesande kasutada reaajas toimuva biomeetrilise kaugtuvastamise süsteemi riikliku julgeoleku eesmärkidel (näiteks luureandmete kogumiseks), jääb selline kasutamine tehisintellektimääruse kohaldamisalast välja.

²⁰ Kohtuotsus, Euroopa Kohus, 6. oktoober 2020, Privacy International, C-623/17, EU:C:2020:790, punkt 44.
²¹ Tehisintellektimääruse põhjendus 24.

- (27) Riikliku julgeoleku erandi selge piiritlemine on eriti oluline juhul, kui tehisintellektisüsteeme lastakse turule, võetakse kasutusele või kasutatakse õiguskaitse eesmärgil viisil, mis kuulub tehisintellektimääruse kohaldamisalasse. See on asjakohane seoses keeluga, mis käsitleb üksikisikute kuritegevusega seotud prognoose ja hinnanguid ning reaajas toimuva biomeetrilise kaugtuvastamise süsteemide kasutamist õiguskaitse eesmärkidel, mis on sätestatud vastavalt tehisintellektimääruse artikli 5 lõike 1 punktides d ja h. Politsei ja muude õiguskaitseasutuste ülesanne on kuritegude tõkestamine, avastamine, uurimine ja nende eest vastutusele võtmine või kriminaalkaristuste täitmisele pööramine, sealhulgas avalikku julgeolekut ähvardavate ohtude eest kaitsmine ja nende ennetamine²². Kui tehisintellektisüsteeme kasutatakse sellistel eesmärkidel, kuuluvad need tehisintellektimääruse kohaldamisalasse.
- (28) Europoli ja muude liidu julgeolekuasutuste, näiteks Frontexi tegevus kuulub tehisintellektimääruse kohaldamisalasse.

2.5.2. Õigusala ja õiguskaitseala koostöö kolmandate riikidega

- (29) Tehisintellektimääruse artikli 2 lõike 4 kohaselt ei kohaldata tehisintellektimäärust kolmanda riigi ametiasutuste või rahvusvaheliste organisatsioonide suhtes, kui need ametiasutused või organisatsioonid kasutavad tehisintellektisüsteeme liidu või ühe või mitme liikmesriigiga sõlmitud rahvusvahelise koostöö või õiguskaitse ja õigusala koostöö alaste lepingute raames, tingimusel et selline kolmas riik või rahvusvaheline organisatsioon pakub piisavaid kaitsemeetmeid üksikisikute põhiõiguste ja -vabaduste kaitseks. Vajaduse korral võib see erand hõlmata selliste eraõiguslike üksuste tegevust, kellele kolmandad riigid on usaldanud konkreetsete ülesannete täitmise sellise õiguskaitse- ja õigusala koostöö toetamiseks²³. Selleks, et erandit kohaldataks, peavad need koostööraamistikud või rahvusvahelised lepingud sisaldama ka piisavaid kaitsemeetmeid üksikisikute põhiõiguste ja -vabaduste kaitseks, mida peavad hindama õiguskaitse ja õigusemõistmise valdkonnas kasutatavate tehisintellektisüsteemide järelevalve pädevusega turujärelevalveasutused²⁴. Tehisintellektimääruse põhjenduses 22 on täpsustatud, et vastuvõtavad riiklikud ametiasutused ning liidu institutsioonid, organid ja asutused, kes tehisintellekti selliseid väljundeid liidus kasutavad, vastutavad selle tagamise eest, et väljundite kasutamine oleks kooskõlas liidu õigusega. Kui tulevikus vaadatakse kõnealused rahvusvahelised lepingud läbi või sõlmitakse uusi, peaksid lepinguosalisel tegema kõik endast oleneva, et viia need lepingud vastavusse tehisintellektimääruse nõuetega.

2.5.3. Teadus- ja arendustegevus

- (30) Tehisintellektimääruse artikli 2 lõike 8 kohaselt ei kohaldata tehisintellektimäärust „tehisintellektisüsteemide või tehisintellektimudelitega seotud teadus-, testimis- või arendustegevuse suhtes enne nende turule laskmist või kasutusele võtmist“. See erand on kooskõlas tehisintellektimääruse turupõhise loogikaga, mida kohaldatakse tehisintellektisüsteemide suhtes pärast nende turule laskmist või kasutusele võtmist.

²² Tehisintellektimääruse artikli 3 punkt 46.

²³ Vt tehisintellektimääruse põhjendus 22.

²⁴ Vt tehisintellektimääruse põhjendus 22 ja artikli 74 lõige 8.

Näiteks teadus- ja arendustegevuse etapis on tehisintellekti arendajatel vabadus katsetada ja testida uusi funktsioone, mis võivad hõlmata võtteid, mida võib pidada manipuleerivaks ja mis on hõlmatud tehisintellektimääruse artikli 5 lõike 1 punktiga a, kui neid kasutatakse tarbijale suunatud rakendustes. Tehisintellektimäärus võimaldab sellist katsetamist, tunnistades, et varajases etapis toimuv teadus- ja arendustegevus on oluline tehisintellekti tehnoloogiate täiustamiseks ja selle tagamiseks, et need vastavad enne turule laskmist ohutus- ja eetikanormidele.

- (31) Nagu on selgitatud tehisintellektimääruse põhjenduses 25, on määruse eesmärk toetada innovatsiooni ning selles tunnistatakse teadusuuringute tähtsust tehisintellekti tehnoloogia arendamisel ja teaduse arengule ja innovatsioonile kaasaaitamisel. Seetõttu on tehisintellektimääruse artikli 2 lõikes 6 sätestatud, et määrust „ei kohaldata tehisintellektisüsteemide või -mudelite, sealhulgas nende väljundite suhtes, mis on spetsiaalselt välja töötatud ja kasutusele võetud üksnes teadus- ja arendustegevuse eesmärgil“.

Näiteks võivad teadusuuringud, mis käsitlevad kognitiivseid ja käitumuslikke reaktsioone tehisintellekti juhitud alalävisele tajule suunatud või petlikele stiimulitele, anda väärtuslikke teadmisi inimese ja tehisintellekti vahelisest suhtlusest, andes teavet tulevikus turvalisemate ja tõhusamate tehisintellekti rakenduste loomiseks. Sellised teadusuuringud on lubatud, kuna need on tehisintellektimääruse kohaldamisalast välja jäetud, olenemata tehisintellektimääruse artikli 5 lõike 1 punktis a sätestatud keelust.

- (32) Tehisintellektimääruse artikli 2 lõikes 8 sätestatud erand ei piira siiski kohustust järgida kõnealust määrust juhul, kui tehisintellektisüsteem lastakse turule või võetakse kasutusele sellise teadus- ja arendustegevuse tulemusena²⁵. See erand ei hõlma ka tegelikes tingimustes testimist tehisintellektimääruse²⁶ tähenduses.

Näiteks omavalitsus, kes soovib testida näotuvastustarkvara, kasutades selleks karnevali ajal tänavatel biomeetrilise kaugtuvastamise süsteemi, värbab vabatahtlikke, keda süsteem tuvastab tegelikes tingimustes. Kuna tegelikes tingimustes testimine ei kuulu tehisintellektimääruse artikli 2 lõike 8 kohase erandi alla, peab kavandatud testimine olema täielikult kooskõlas tehisintellektimääruse biomeetrilise kaugtuvastamise süsteemidele esitatavate nõuetega, välja arvatud juhul, kui süsteemi testitakse tehisintellekti jaoks mõeldud regulatiivliivakastis või kooskõlas erikorraga tegelikes tingimustes testimiseks väljaspool liivakasti, nagu on nähtud ette tehisintellektimääruse artiklites 60 ja 61²⁷.

- (33) Teadus- ja arendustegevus (sh juhul, kui see ei kuulu tehisintellektimääruse kohaldamisalasse) peaks igal juhul toimuma kooskõlas teadusuuringute tunnustatud

²⁵ Tehisintellektimääruse põhjendus 25.

²⁶ Tehisintellektimääruse artikli 3 punkti 57 järgi tähendab „tegelikes tingimustes testimine“ tehisintellektisüsteemi ajutist testimist „selle sihtotstarbe jaoks tegelikes tingimustes väljaspool laborit või muul moel simuleeritud keskkonda, eesmärgiga koguda usaldusväärseid ja stabiilseid andmeid ning hinnata ja kontrollida tehisintellektisüsteemi vastavust käesoleva määruse nõuetele“. Tehisintellektimäärus näeb ette erikorra sellise tegelikes tingimustes testimise jaoks, mis ei kvalifitseeru määruse tähenduses tehisintellektisüsteemi turule laskmiseks või kasutusele võtmiseks, tingimusel et kõik artiklis 57 või 60 sätestatud tingimused on täidetud, sealhulgas testimises osalevate isikute vaba ja teadliku nõusoleku saamine jne; vt tehisintellektimääruse artikkel 60.

²⁷ Tehisintellektimäärus määrab sisaldab üksikasjalikke ja konkreetseid kohustusi seoses tehisintellekti regulatiivliivakastide ja tegelikes tingimustes testimisega. Vt tehisintellektimääruse artikkel 57 jj.

eetiliste ja kutsestandarditega ning see peaks toimuma kooskõlas kohaldatava liidu õigusega²⁸ (nt andmekaitsealased õigusaktid, mida kohaldatakse edasi).

2.5.4. Isiklik, mitte kutseline tegevus

- (34) Tehisintellektimääruse artikli 2 lõikes 10 on ette nähtud, et määrust ei kohaldata isikliku, mitte kutsetegevuse käigus tehisintellektisüsteeme kasutavate füüsilistest isikutest juurutajate kohustuste suhtes. Ka mõiste „juurutaja“ määratlus välistab selgesõnaliselt sellises tegevuses osalevad kasutajad (vt punkt 2.4 eespool). Igasugust tegevust, mille kaudu füüsiline isik saab regulaarselt majanduslikku kasu või on muul viisil seotud kutse-, äri-, kaubandus-, ametialase või vabakutselise tegevusega, tuleks käsitada kutselise tegevusena. Mõiste „isiklik“ kirjeldab muud kui kutselist tegevust, mis tähendab, et isiku tegevus peaks olema isiklik ja ei tohiks olla kutseline. Seega ei tohiks erand hõlmata näiteks kuritegevust, kuna seda ei tohiks pidada puhtalt isiklikuks.

Näiteks isik, kes kasutab kodus näotuvastussüsteemi (nt juurdepääsu kontrollimiseks ja kodu sissepääsu ohutuse tagamiseks), ei kuulu tehisintellektimääruse artikli 2 lõike 10 kohaldamisalasse ja seega ei kohaldata tema suhtes tehisintellektimääruse kohaseid juurutajate kohustusi isegi juhul, kui ta on kohustatud edastama salvestatud materjali (või osa sellest) õiguskaitseasutustele.

Seevastu füüsiline isik, kes kasutab tehisintellektisüsteemi kutsetegevuseks, näiteks vabakutselised, ajakirjanikud, arstid jne, peaks täitma tehisintellektimääruses kehtestatud näotuvastussüsteemide juurutajatele tulenevaid kohustusi. Mis tahes kasutamine füüsiliste isikute poolt, kui nad tegutsevad kutsealaselt tegutseva juurutaja nimel või volitusel, kuulub samuti tehisintellektimääruse kohaldamisalasse.

Lisaks ei saa kuritegevust pidada puhtalt isiklikuks tegevuseks, isegi kui sellega ei taotleta ega saavutata majanduslikku kasu. Muu ebaseadusliku tegevuse, näiteks tarbijakaitse- või andmekaitseseaduste ja riigisiseste haldusaktide rikkumise puhul kohaldatakse tehisintellektimääruses sätestatud erandit, kuid muud asjaomased õigusraamistikud jäävad kehtima.

- (35) Tehisintellektimääruse artikli 2 lõikes 10 sätestatud erandit kohaldatakse ainult juurutajate kohustuste suhtes, kui nad kasutavad süsteemi üksnes isiklikuks, mitte kutseliseks tegevuseks. Süsteem kui selline jääb süsteemi turule laskvate või kasutusele võtvate pakkujate, muude kutseliste juurutajate ja muude vastutavate osaliste, näiteks importijate ja turustajate kohustuste puhul tehisintellektimääruse kohaldamisalasse.

Näiteks emotsioonituvastussüsteem, kui see on ette nähtud füüsiliste isikute poolt puhtalt isiklikuks, mitte kutseliseks tegevuseks, on endiselt tehisintellektimääruse artikli 6 kohane suure riskiga tehisintellektisüsteem ja peab olema täielikult kooskõlas tehisintellektimäärusega. Juurutaja suhtes, kes kasutab seda puhtalt isiklikul, mitte kutselisel eesmärgil (nt autistlik isik), ei kohaldata siiski tehisintellektimääruses ette nähtud konkreetseid kohustusi juurutajatele ja selline kasutamine ei kuulu määruse kohaldamisalasse.

2.5.5. Tasuta ja avatud lähtekoodiga litsentside alusel avaldatud tehisintellektisüsteemid

- (36) Vastavalt tehisintellektimääruse artikli 2 lõikele 12 ei kohaldata määrust tehisintellektisüsteemide suhtes, mis on tarbimisse lubatud vaba ja avatud lähtekoodiga litsentside alusel,²⁹ välja arvatud juhul, kui need lastakse turule või võetakse kasutusele suure riskiga tehisintellektisüsteemidena või tehisintellektisüsteemina, mis kuulub artikli 5 (tehisintellekti keelatud kasutusviisid) või artikli 50 (teatavate tehisintellektisüsteemide läbipaistvuskohustused) kohaldamisalasse. See tähendab, et tehisintellektisüsteemide pakkujad ei saa seda erandit kasutada, kui nende turule lastud või kasutusele võetud tehisintellektisüsteem kujutab endast tehisintellektimääruse artikli 5 järgi keelatud kasutusviisi.

2.6. Keeldude ja suure riskiga tehisintellektisüsteemide nõuete koostoime

- (37) Tehisintellektimääruse artikliga 5 keelatud tehisintellekti kasutusviiside kaalumisel tuleks lähtuda tehisintellektisüsteemidest, mis on liigitatud tehisintellektimääruse artikli 6 kohaselt suure riskiga tehisintellektisüsteemideks, eelkõige III lisas loetletud süsteemidest³⁰. See tuleneb sellest, et suure riskiga tehisintellektisüsteemide kasutamine võib mõnel juhul kvalifitseeruda keelatud kasutusviisiks, kui kõik tehisintellektimääruse artiklis 5 sätestatud ühe või mitme keelu tingimused on täidetud. Samas kvalifitseerub enamik tehisintellektimääruse artiklis 5 loetletud erandite alla kuuluvaid tehisintellektisüsteeme suure riskiga süsteemideks.

Näiteks emotsioonituvastussüsteemid, mis ei vasta artikli 5 lõike 1 punktis f sätestatud keelu tingimustele, liigitatakse tehisintellektimääruse artikli 6 lõike 2 ja III lisa punkti 1 alapunkti c kohaselt suure riskiga tehisintellektisüsteemideks. Samamoodi loetakse teatavaid tehisintellektipõhiseid hindamissüsteeme, näiteks krediidihindamise või riskihindamise süsteeme tervise- ja elukindlustuses, suure riskiga tehisintellektisüsteemideks, kui need ei vasta tehisintellektimääruse artikli 5 lõike 1 punktis c loetletud keelu tingimustele³¹. Teine näide suure riskiga süsteemidest on tehisintellektisüsteemid, mis hindavad isikuid ja määravad kindlaks, kas neil on õigus saada olulisi avalikke teenuseid ja hüvesid, näiteks tervishoiuteenuseid ja sotsiaalkindlustushüvitisi³². Kui sellised süsteemid hõlmavad vastuvõetamatut sotsiaalpunktide andmist ja vastavad tehisintellektimääruse artikli 5 lõike 1 punktis c sätestatud tingimustele, on nende turule laskmine, kasutusele võtmine ja kasutamine liidus keelatud.

Sellistel juhtudel peaks pakkuja poolne riskihindamine ja -juhtimine ning muude suure riskiga tehisintellektisüsteemide suhtes kehtivate nõuete (nt andmete haldamine, läbipaistvus ja inimjärelvalve) täitmine, samuti juurutaja kohustused seoses asjakohase kasutamisega vastavalt kasutusjuhendile ja inimjärelvalvega (artikkel 26)

²⁹ Tehisintellektimääruse põhjenduses 102 on selgitatud, et tarkvara ja andmete avaldamine vaba ja avatud lähtekoodiga litsentsi alusel võimaldab neid avalikult jagada ning kasutajad saavad neile või nende muudetud versioonidele vabalt juurde pääseda, neid kasutada, muuta ja ümber jagada.

³⁰ Selles loetelus on hõlmatud biomeetriaal põhinevad tehisintellektisüsteemid, samuti tehisintellektisüsteemid, mida kasutatakse konkreetsel eesmärgil teatud valdkondades, nagu tööhõive, haridus, juurdepääs avalikele ja erateenustele, õiguskaitse jne.

³¹ Sellele on selgesõnaliselt viidatud tehisintellektimääruse põhjenduses 58 ja III lisas.

³² Tehisintellektimääruse põhjendus 58.

ning mõnel juhul põhiõigustele avalduva mõju hindamine (artikkel 27) aitama tagada, et turule lastud või kasutusele võetud suure riskiga tehisintellektisüsteem on seaduslik ja ei kujuta endast keelatud kasutusviisi.

- (38) Lõpuks võivad tehisintellektisüsteemid, mida erandkorras ei peeta tehisintellektimääruse artikli 6 lõike 3 alusel suure riskiga süsteemideks, kuigi nad kuuluvad III lisa kohaste suure riskiga kasutusjuhtumite hulka, siiski jääda tehisintellektimääruse artiklis 5 sätestatud keeldude kohaldamisalasse. Tehisintellektimääruse artikli 6 lõike 3 kohaselt võib ainult leida, et tehisintellektisüsteem ei ole suure riskiga, kuid see ei välista selliste tehisintellektisüsteemide suhtes tehisintellektimääruse ja keeldude kohaldamist.

2.7. Keeldude kohaldamine üldotstarbeliste tehisintellektisüsteemide ja sihtotstarbeliste süsteemide suhtes

- (39) Keeldu kohaldatakse mis tahes tehisintellektisüsteemi suhtes, olenemata sellest, kas see on „sihtotstarbeline“³³ või „üldotstarbeline“ (st mis võib täita erinevaid eesmärgi), kas see on mõeldud otseseks kasutamiseks või integreerimiseks teistesse tehisintellektisüsteemidesse³⁴. Sellest tulenevalt peaks iga ettevõtja võtma meetmeid, mille jaoks tal on parimad võimalused vastavalt oma rollile ja kontrollile, mis tal süsteemi üle väärtusahelas on, et tagada tehisintellektisüsteemide vastutustundlik ja ohutu pakkumine ja kasutamine, tasakaalustades nende riske ja kasu, pidades silmas tehisintellektimääruse kahe eesmärgi saavutamist.
- (40) Seega oodatakse juurutajatelt, et nad ei kasutaks ühtki tehisintellektisüsteemi tehisintellektimääruse artiklis 5 keelatud viisil, sealhulgas et nad ei hoiaks kõrvale süsteemi pakkujate rakendatud kaitsemeetmetest. Kuigi kahju tuleneb sageli sellest, kuidas tehisintellektisüsteeme praktikas kasutatakse, on pakkujatel ka kohustus mitte lasta turule või võtta kasutusele tehisintellektisüsteeme, sealhulgas üldotstarbelisi tehisintellektisüsteeme, mis käituvad või mida kasutatakse mõistliku tõenäosusega otseselt tehisintellektimääruse artikli 5 kohaselt keelatud viisil³⁵. Sellega seoses eeldatakse, et pakkujad võtavad tõhusaid ja kontrollitavaid meetmeid kaitsemeetmete rakendamiseks ning sellise kahjuliku käitumise ja väärkasutuse ennetamiseks ja leevendamiseks, kuivõrd see on mõistlikult prognoositav ning sellised meetmed on teostatavad ja proportsionaalsed, sõltuvalt konkreetsest tehisintellektisüsteemist ja juhtumi asjaoludest. Samuti eeldatakse, et pakkujad välistavad oma lepingulistest suhetes juurutajatega (st tehisintellektisüsteemi kasutustingimustes) tehisintellektisüsteemi kasutamise keelatud viisil ning annavad asjakohast teavet juurutajatele mõeldud kasutusjuhendis ja vajaliku inimjärelvalve kohta.

³³ Tehisintellektimääruse artikli 3 punktis 12 on see määratletud kui „kasutus, kaasa arvatud kasutamise konkreetne kontekst ja tingimused, mille jaoks pakkuja on tehisintellektisüsteemi kasutusjuhendis, reklaam- või müügmaterjalides või avaldustes ning tehnilistes dokumentides esitanud teabe kohaselt ette näinud“.

³⁴ Vt tehisintellektimääruse artikli 3 punkt 66.

³⁵ See tuleneb eelkõige kõigist tehisintellektimääruse artiklis 5 loetletud keeldude viidetest „turule laskmisele“ või „kasutusele võtmisele“, välja arvatud artikli 5 lõike 1 punktis h sätestatud reaalarajas toimuva biomeetrilise kaugtuvastamise süsteemide keeld, mida kohaldatakse ainult kasutamise suhtes.

Näiteks võib üldotstarbeline tehisintellektisüsteem, mida kasutatakse juturobotina, kasutada manipuleerivaid ja petlikke võtteid, mis võivad tõenäoliselt tekitada olulist kahju. Selleks, et vältida tehisintellektisüsteemi keelatud käitumist ja kasutamist, mille puhul on mõistlikult tõenäoline, et sellega manipuleeritakse, petetakse ja tekitatakse olulist kahju kooskõlas tehisintellektimääruse artikli 5 lõike 1 punktiga a, peab pakkuja võtma asjakohaseid ja proportsionaalseid meetmeid (nt asjakohane ohutu ja eetiline projekteerimine, tehniliste ja muude kaitsemeetmete integreerimine, kasutuspiirangud, läbipaistvus ja kasutajate kontroll, asjakohane teave kasutusjuhendis), enne kui tehisintellektisüsteem turule lastakse (tehisintellektimääruse artikli 5 lõike 1 punkt a), et tagada, et juturobot ei tekita kasutajatele või teistele isikutele või isikute rühmadele olulist kahju (vt ka punkt 3.2.3.c).

- (41) Teatud juhtudel, eelkõige juhul, kui keelud on seotud süsteemi väga konkreetse eesmärgiga,³⁶ võivad pakkujatel olla muude ennetus- ja leevendusmeetmete integreerimiseks piiratud võimalused ning nad peavad tuginema eelkõige juurutajatele asjakohaste juhiste ja teabe andmisele, nõutavale inimjärelvalvele ning süsteemi keelatud kasutamise piiramisele. Vajaduse korral võivad sellised meetmed hõlmata ka järelvalvet selle piirangu järgimise üle, sõltuvalt sellest, milliste vahendite kaudu tehisintellektisüsteemi tarnitakse ja millist teavet pakkujal võimaliku väärkasutuse kohta on. Mis tahes võimalikud järelvalvemeetmed väärkasutuse tuvastamiseks ei tohiks olla samaväärsed juurutajate tegevuse üldise järelvalvega ja peaksid olema kooskõlas liidu õigusega.

Näiteks ei tohiks juurutajad üldotstarbelist tehisintellektisüsteemi, mis suudab tuvastada või tuletada emotsioone, kasutada töökohal või haridusasutustes, välja arvatud juhul, kui selle suhtes kohaldatakse erandit meditsiinilistel või ohutusega seotud põhjustel. Siiski ei pruugi pakkuja teada, millises konkreetses kontekstis süsteemi emotsioonituvastuse funktsiooni kasutatakse ja kas selle puhul võib kohaldada erandit tehisintellektimääruse artikli 5 lõike 1 punktis f sätestatud keelust. Sellised pakkujad võivad siiski oma kasutustingimustes selgesõnaliselt välistada sellise keelatud kasutamise ja lisada kasutusjuhendisse asjakohase teabe juurutajate juhendamiseks. Samuti eeldatakse, et nad võtavad asjakohaseid meetmeid, kui nad saavad teada, et konkreetsed juurutajad kuritarvitavad süsteemi sel konkreetisel keelatud eesmärgil, näiteks kui sellisest kuritarvitamisest teatatakse või kui pakkuja saab sellest muul viisil teada, mis võib juhtuda, kui süsteemi kasutatakse otse pakkuja kontrolli all oleva platvormi kaudu ja pakkuja teeb selles kontrolle.

2.8. Keeldude ja muude liidu õigusaktide vastastikune mõju

- (42) Tehisintellektimäärus määrus on määrus, mida kohaldatakse horisontaalselt kõikides sektorites, ilma et see piiraks muude liidu õigusaktide kohaldamist, eelkõige põhiõiguste kaitse, tarbijakaitse, tööhõive, töötajate kaitse ja tooteohutuse valdkonnas³⁷. Tehisintellektimäärus täiendab selliseid õigusakte oma ennetava ja ohutusloogika kaudu (tehisintellektisüsteeme ei tohi turule lasta ega kasutada teatud

³⁶ Tehisintellektimääruse artikli 5 lõike 1 punktid d–h.

³⁷ Tehisintellektimääruse artikkel 2 ja põhjendus 9.

viisil) ning pakub täiendavat kaitset, käsitledes konkreetseid kahjulikke tehisintellekti kasutusviise, mis ei pruugi olla muude seadustega keelatud. Lisaks sellele võimaldavad tehisintellektimääruses sätestatud keelud tegeleda tehisintellektisüsteemide elutsükli varasemate etappidega (st turule laskmine ja kasutusele võtmine) ja juurutamisega (st kasutamine) ning seega võtta meetmeid tehisintellekti väärtusahela eri etappides tehisintellekti kasutamisega seotud kahjulike kasutusviiside vastu.

- (43) Samal ajal ei mõjuta tehisintellektimäärus keelde, mis kehtivad juhul, kui tehisintellekti kasutusviis kuulub muude liidu õigusaktide alla³⁸. Seega, isegi kui tehisintellektisüsteem ei ole tehisintellektimäärusega keelatud, võib selle kasutamine olla keelatud või ebaseaduslik muude liidu esmaste või teiseste õigusaktide alusel (nt konkreetsel juhul põhiõiguste eiramise tõttu, näiteks kui puudub õiguslik alus isikuandmete töötlemiseks, mis on nõutav andmekaitseõiguse alusel, liidu õigusega keelatud diskrimineerimine jne). Seega ei ole tehisintellektimääruses sätestatud keeldude järgimine piisav tingimus, mis näitaks muude tehisintellektisüsteemide pakkujate ja juurutajate suhtes kohaldatavate liidu õigusaktide järgimist.

Näiteks töökohal kasutatavate tehisintellektipõhiste emotsioonituvastussüsteemide suhtes, mille puhul kohaldatakse erandit tehisintellektimääruse artikli 5 lõike 1 punktis f sätestatud keelust, kuna neid kasutatakse meditsiinilistel või ohutusega seotud põhjustel, kohaldatakse jätkuvalt andmekaitseseadust ning liidu ja riigisisest õigust tööhõive ja töötingimuste, sealhulgas töötervishoiu ja tööohutuse kohta, milles võidakse näha ette muid piiranguid ja kaitsemeetmeid seoses selliste süsteemide kasutamisega³⁹.

- (44) Kui konkreetsed tegevused, mis on seotud tehisintellektisüsteemide turule laskmise või kasutamisega, kuuluvad ka muude liidu õigusaktide kohaldamisalasse, on tehisintellektimääruse eesmärk tagada erinevate sätete järjepidev rakendamine. Lisaks võimaldab see tõhusat koostööd tehisintellektimääruse jõustamise eest vastutavate pädevate asutuste ning tehisintellektimääruse artikli 77 ja muude sätete alusel põhiõigusi kaitsvate asutuste vahel. Üldisemalt on asjaomased asutused Euroopa Liidu lepingu artikli 4 lõike 3 järgi kohustatud tegema lojaalset koostööd, kui nad täidavad oma vastavaid ülesandeid liidu õiguse alusel.
- (45) Keeldude kontekstis on eriti oluline tehisintellektimääruse ja liidu andmekaitseõiguse vastastikune mõju, kuna tehisintellektisüsteemid töötlevad sageli teavet, mis on seotud tuvastatud või tuvastatavate füüsiliste isikutega („isikuandmed“)⁴⁰. Sõltuvalt keelust ja kontekstist on selliste süsteemidega seoses kõige asjakohasemad õigusaktid määrus (EL) 2016/679 füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta (isikuandmete kaitse üldmäärus), direktiiv (EL) 2016/680, mis käsitleb füüsiliste isikute kaitset seoses pädevates asutustes isikuandmete töötlemisega süütegude tõkestamise, uurimise, avastamise ja nende eest vastutusele võtmise või kriminaalkaristuste täitmisele pööramise eesmärgil ning selliste

³⁸ Tehisintellektimääruse artikli 5 punkt 8.

³⁹ Vt ka tehisintellektimääruse põhjendus 9.

⁴⁰ Tehisintellektimääruse artikli 2 lõike 7; vt ka tehisintellektimääruse põhjendus 10.

andmete vaba liikumist (õiguskaitse direktiiv), ning määrus (EL) 2018/1725, mis käsitleb füüsiliste isikute kaitset isikuandmete töötlemisel liidu institutsioonides, organites ja asutustes ning isikuandmete vaba liikumist (ELi isikuandmete kaitse määrus). Tehisintellektimääruse artikli 2 lõike 7 kohaselt ei mõjuta kõnealune määrus neid õigusakte ning neid kohaldatakse jätkuvalt koos tehisintellektimäärusega, mis on kooskõlas ELi andmekaitsealase õigustikuga ja täiendab seda. Euroopa Liidu Kohus on selgitanud mitmeid ELi andmekaitse normide aspekte ja Euroopa Andmekaitse nõukogu on võtnud vastu rea suuniseid (nt „profiilanalüüsi“ mõiste kohta),⁴¹ mis on tehisintellektimääruse artikli 5 lõike 1 punktis d sätestatud keelu puhul eriti asjakohane, kuna seal kasutatakse sama mõistet).

- (46) Mis puudutab keelde/piiranguid biomeetrilise liigitamise süsteemide ja reaalajas toimuva biomeetrilise kaugtuvastamise süsteemide kasutamise kohta õiguskaitse eesmärkidel, siis kehtib tehisintellektimäärus *lex specialis* õiguskaitse direktiivi artikli 10 suhtes, reguleerides seega ammendaval viisil sellist kasutamist ja asjaomaste biomeetriliste andmete töötlemist⁴². Seoses sellega ei ole tehisintellektimääruse eesmärk anda õiguslikku alust isikuandmete töötlemiseks direktiivi (EL) 2016/680 artikli 8 alusel. Lisaks tehisintellektimääruses sätestatud tingimustele kohaldatakse kõiki muid kõnealuse direktiivi sätteid, eelkõige õiguskaitse eesmärkidel reaalajas (toimuva biomeetrilise kaugtuvastamise) süsteemide kasutamise suhtes, kui see on lubatud, kui tehisintellektimääruse artikli 5 lõike 1 punktis h sätestatud piiratud eranditest ei tulene teisiti. Üldisemalt peavad õiguskaitse direktiivi järgima ka pädevad õiguskaitseasutused (st õiguskaitse direktiivi artikli 3 punkti 7 kohased pädevad asutused) mis tahes isikuandmete töötlemise korral, kui nad töötlevad andmeid õiguskaitse eesmärgil.
- (47) Tehisintellektimääruse artikli 2 lõike 9 järgi kohaldatakse ELi tarbijakaitse- ja ohutus alaseid õigusakte ka edaspidi täies ulatuses nende õigusaktide kohaldamisalasse kuuluvate tehisintellektisüsteemide suhtes.

Näiteks:

- ettevõtjate (sealhulgas füüsiliste isikute, kes tegutsevad kutsetöötajana ettevõtja ja tarbija vahelistes suhetes) sotsiaalpunktide andmise tavadid võib samuti pidada ebaõiglaseks ja seega tarbijaõigusega (st direktiiviga 2005/29/EÜ) vastuolus olevaks;
- kui tehisintellektisüsteemi kasutatakse emotsioonide tuletamiseks, peab see olema kooskõlas ka määrusega (EL) 2017/745 (meditsiiniseadmete määrus), kui tehisintellektisüsteemi kasutatakse meditsiiniliseks diagnoosimiseks või raviks.

- (48) Lisaks kohaldatakse tehisintellekti käsitlevat määrust koos asjakohaste kohustustega vahendusteenuste pakkujate suhtes, kes integreerivad tehisintellektisüsteeme või mudeleid oma teenustesse, mida reguleerib määrus (EL) 2022/2065 (digiteenuste määrus). Täpsemalt on tehisintellektimääruse artikli 2 lõikes 5 märgitud, et

⁴¹ Vt ka artikli 29 alusel asutatud andmekaitse tööühm, suunised automatiseeritud töötusel põhinevate üksikotsuste tegemise ja profiilanalüüsi kohta määruse 2016/679 kohaldamisel, 6. veebruar 2018, WP251rev.01, mille on heaks kiitnud ka Euroopa Andmekaitse nõukogu.

⁴² Tehisintellektimääruse põhjendus 38.

tehisintellektimäärus ei mõjuta digiteenuste määruse II peatükis sätestatud teenuseosutajate vastutust käsitlevate sätete kohaldamist.

- (49) Lisaks sellele ei piira tehisintellektimääruse keelud mis tahes vastutust, mida pakkuja või juurutaja võib kanda tekitatud kahju eest kooskõlas kohaldatavate liidu või riigisiseste õigusaktidega vastutuse kohta⁴³.
- (50) Lõpuks ei tohi tehisintellektimääruse artiklis 5 sätestatud keelde ja selgesõnalisi erandeid nendest keeldudest kasutada muude liidu õigusaktide kohastest kohustustest kõrvalehoidmiseks või nende rikkumise õigustamiseks.
- (51) Kuna tegemist on liidu teisese õigusaktiga, tuleb tehisintellekti käsitlevat määrust tõlgendada ELi aluslepingutega ja hartaga tagatud põhiõiguste ja -vabaduste, samuti nende õiguste ja vabaduste kontekstis, mida kaitsevad rahvusvahelised konventsioonid, mille osaline liit on⁴⁴.
- (52) Täpsemad selgitused konkreetsete keeldude ja muude liidu õigusaktide koostoime kohta on esitatud allpool asjakohastes punktides.

2.9. Tehisintellektimääruse artikli 5 jõustamine

2.9.1. Turujärelevalveasutused

- (53) Liikmesriikide määratud turujärelevalveasutused ja Euroopa Andmekaitseinspektor (ELi institutsioonide, ametite ja asutuste turujärelevalveasutusena) vastutavad tehisintellektisüsteemide puhul tehisintellektimääruses sätestatud normide, sealhulgas keeldude jõustamise eest. Selline jõustamine toimub määrusega (EL) 2019/1020⁴⁵ kehtestatud turujärelevalve ja toodete nõuetele vastavuse süsteemi raames kooskõlas muude liidu tooteohutusalaste õigusaktidega. Turujärelevalveasutuste jõustamisvolitused seoses tehisintellektisüsteemidega on sätestatud tehisintellektimääruses ja määruses (EL) 2019/1020. Kõnealused asutused võivad võtta keeldude suhtes täitemeetmeid omal algatusel või kaebuse alusel, mida on õigus esitada igal mõjutatud isikul või muul füüsilisel või juriidilisel isikul, kellel on alust arvata, et keelde on rikutud⁴⁶. Liikmesriigid peavad määrama oma pädevad turujärelevalveasutused 2. augustiks 2025.
- (54) Tehisintellektimääruses sätestatud menetlus, mis käsitleb riiklikul tasandil ohtu kujutavate tehisintellektisüsteemide käsitlemist, on eriti oluline keeldude jõustamise kontekstis⁴⁷. Kui tegemist on piiriülese mõjuga, mis ulatub järelevalveasutuse territooriumist väljapoole, peab asjaomase liikmesriigi asutus teavitama komisjoni ja

⁴³ Vastutuse tingimused (seoses kahju, vastutava isiku, süü või tõendamiskohustuse jms) määratakse kindlaks kohaldatava õigusega, näiteks Euroopa Parlamendi ja nõukogu 23. oktoobri 2024. aasta direktiiviga (EL) 2024/2853 tootevastutuse kohta (EMPs kohaldatav tekst) (ELT L, 2024/2853, 18.11.2024) või kohaldatavate riigisiseste õigusaktidega vastutuse kohta (vt ka ettepanek: Euroopa Parlamendi ja nõukogu direktiiv lepinguvälise tsiviilvastutuse normide tehisintellektile kohandamise kohta (tehisintellektiga seotud vastutuse direktiiv) (COM(2022) 496 final).

⁴⁴ Isegi kui liit ei ole veel Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni osaline, on harta artikli 59 lõikes 3 sätestatud, et kui harta sisaldab õigusi, mis vastavad Euroopa inimõiguste ja põhivabaduse kaitse konventsiooniga tagatud õigustele, on nende tähendus ja ulatus sama, mis neile nimetatud konventsiooniga ette on nähtud. See säte ei takista liidu õiguses ulatuslikuma kaitse kehtestamist.

⁴⁵ Vt ka tehisintellektimääruse põhjendus 156.

⁴⁶ Tehisintellektimääruse artikkel 85.

⁴⁷ Tehisintellektimääruse artikkel 79.

teiste liikmesriikide turujärelevalveasutusi. Kõik turujärelevalveasutused peaksid järgima liidu kaitsemeetmete menetlust, mille puhul otsustab komisjon,⁴⁸ kas tehisintellektisüsteem kujutab endast keelatud kasutusviisi. Selle menetluse eesmärk on tagada, et keelde kohaldatakse kõikides liikmesriikides ühetaoliselt, et pakkuda õiguskindlust nii tehisintellektisüsteemide pakkujatele kui ka juurutajatele. Selleks, et tagada tehisintellektimääruse ühtne kohaldamine, peaksid riiklikud turujärelevalveasutused püüdma kohaldada keelde ühtlustatult ka võrreldavate juhtumite puhul, mille mõju piirdub liikmesriigi territooriumiga, tuginedes nendele suunistele ja tehes koostööd Euroopa tehisintellekti nõukoja raames⁴⁹.

2.9.2. Karistused

- (55) Tehisintellektimäärus järgib selle erinevate sätete rikkumise eest karistuste kehtestamisel astmelist lähenemisviisi, sõltuvalt rikkumise raskusastmest. Tehisintellektimääruse artiklis 5 sätestatud keeldude mittejärgimist peetakse kõige raskemaks rikkumiseks ja seetõttu määratakse selle eest kõige suurem trahv. Keelatud tehisintellekti kasutusviise kasutavaid pakkujaid ja juurutajaid võib trahvida kuni 35 000 000 euroga või kui rikkuja on ettevõtja, siis kuni 7 %ga tema eelmise majandusaasta ülemaailmsest kogukäibest olenevalt sellest, kumb summa on suurem⁵⁰. Iga liikmesriik peaks kehtestama eeskirjad selle kohta, kas ja millises ulatuses võib määrata haldustrahve ametiasutustele ja asutustele, kes on selles liikmesriigis asutatud tehisintellektisüsteemide pakkujatena ja juurutajatena. ELi institutsioonide, asutuste ja ametite suhtes, kes rikuvad keelde, võidakse määrata kuni 1 500 000 euro suurune haldustrahv⁵¹.
- (56) On võimalik, et üks ja sama keelatud käitumine kujutab endast kahe või enama tehisintellektimääruse sätte rikkumist (st ka sünavõltsingute märgistamata jätmine võib olla tehisintellektimääruse artikli 5 lõike 1 punkti a kohane petlik võte). Sellistel juhtudel tuleks järgida *ne bis in idem* põhimõtet. Igal juhul tuleb arvesse võtta tehisintellektimääruse artikli 99 lõikes 7 sätestatud karistuste määramise kriteeriume.
- (57) Kuna tehisintellektimääruse artiklis 5 sätestatud keeldude rikkumine riivab kõige rohkem teiste isikute vabadusi ja toob kaasa kõige suuremad trahvid, tuleks nende kohaldamisala tõlgendada kitsalt.

3. TEHISINTELLEKTIMÄÄRUSE ARTIKLI 5 LÕIKE 1 PUNKTID A JA B – KAHJULIK MANIPULEERIMINE, PETTUS JA ÄRAKASUTAMINE

- (58) Tehisintellektimääruse artikli 5 lõike 1 punktides a ja b esitatud esimese kahe keeluga püütakse kaitsta üksikisikuid ja haavatavaid isikuid tehisintellekti abil toimuva manipuleerimise ja ärakasutamise märkimisväärselt kahjuliku mõju eest. Need keelud on suunatud tehisintellektisüsteemidele, mis kasutavad alalävisele tajule suunatud, sihilikult manipuleerivaid või petlikke võtteid, mis on märkimisväärselt kahjulikud ja mõjutavad oluliselt füüsilise isiku või isikute rühma(de) käitumist

⁴⁸ Tehisintellektimääruse artikkel 81.

⁴⁹ Tehisintellektimääruse artiklid 65 ja 66.

⁵⁰ Tehisintellektimääruse artikkel 99.

⁵¹ Tehisintellektimääruse artikkel 100.

(tehisintellektimääruse artikli 5 lõike 1 punkt a) või kasutavad ära vanusest, puudest või konkreetsest sotsiaalsest või majanduslikust olukorrast tulenevaid haavatavusi (tehisintellektimääruse artikli 5 lõike 1 punkt b).

3.1. Põhjendus ja eesmärgid

- (59) Nende keeldude aluseks on üksikisiku sõltumatuse ja heaolu kaitsmine manipuleerivate, petlike ja ekspluateerivate tehisintellekti kasutusviiside eest, mis võivad õhnestada ja kahjustada üksikisiku sõltumatust, otsuste tegemist ja valikuvabadust⁵². Keeldude eesmärk on kaitsta õigust inimväärikusele (harta artikkel 1), mis on ühtlasi kõigi põhiõiguste alus ja mille oluline aspekt on individuaalne sõltumatus. Keeldude eesmärk on eelkõige vältida manipuleerimist ja ärakasutamist tehisintellektisüsteemide kaudu, mis muudavad üksikisikud pelgalt vahenditeks teatud eesmärkide saavutamiseks, ning kaitsta neid, kes on kahjuliku manipuleerimise ja ärakasutamise suhtes kõige haavatavamad ja sellele kõige vastuvõtlikumad. Märkimisväärselt kahjulike manipuleerivate, petlike ja ekspluateerivate tehisintellekti kasutusviiside keelustamine on täielikult kooskõlas tehisintellektimääruse laiema eesmärgiga edendada usaldusväärseid ja inimkeskseid tehisintellektisüsteeme, mis on ohutud, läbipaistvad, õiglased ja teenivad inimkonda ning on kooskõlas inimtegevuse ja ELi väärtustega.

3.2. Tehisintellektimääruse artikli 5 lõike 1 punktis a sätestatud keelu põhikomponendid – kahjulik manipuleerimine

Tehisintellektimääruse artikli 5 lõike 1 punktis a on sätestatud:

„1. Järgmised tehisintellekti kasutusviisid on keelatud:

a) selliste tehisintellektisüsteemide turule laskmine, kasutusele võtmine või kasutamine, milles on kasutatud inimese teadvusest kaugemale ulatuvale 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;“.

- (60) Selleks, et tehisintellektimääruse artikli 5 lõike 1 punktis a sätestatud keeld oleks kohaldatav, peavad olema täidetud mitu kumulatiivset tingimust:
- (i) kasutusviis peab kujutama endast tehisintellektisüsteemi turule laskmist, kasutusele võtmist või kasutamist;
 - (ii) tehisintellektisüsteem peab kasutama alalävisele tajule suunatud (inimese teadvusest kaugemale ulatuvaid), sihipäraselt manipuleerivaid või petlikke võtteid;
 - (iii) tehisintellektisüsteemi kasutatavate võtete eesmärk või mõju peaks olema isiku või isikute rühma käitumise oluline moonutamine. Moonutamine peab oluliselt

⁵² Tehisintellektimääruse põhjendus 29.

kahjustama nende võimet teha teadlikku otsust, mille tulemusel isik või isikute rühm teeb otsuse, mida ta või nad ei oleks muidu teinud;

(iv) moonutatud käitumine peab põhjustama või mõistliku tõenäosusega põhjustama olulist kahju kõnealusele isikule, teisele isikule või isikute rühmale.

- (61) Keelu kohaldamiseks peavad kõik neli tingimust olema samal ajal täidetud ning kasutatud võtete, isiku käitumise olulise moonutamise ja sellest käitumisest tuleneva või mõistliku tõenäosusega tuleneva olulise kahju vahel peab olema usutav põhjuslik seos.
- (62) Esimest tingimust, st tehisintellektisüsteemi turule laskmist, kasutusele võtmist või kasutamist, on juba analüüsitud. Seega kehtib keeld nii tehisintellektisüsteemide pakkujate kui ka juurutajate suhtes, kes on oma vastutuse piires kohustatud selliseid süsteeme mitte turule laskma, kasutusele võtma ega kasutama. Järgnevates punktides keskendutakse ülejäänud kolmele tingimusele.

3.2.1. Alalävisele tajule suunatud, sihipäraselt manipuleerivad või petlikud võtted

- (63) Tehisintellektimääruse artikli 5 lõike 1 punktis a on keelatud kolm alternatiivset manipuleerivat võtet: a) inimese teadvusest kaugemale ulatuvale alalävisele tajule suunatud võtted, b) sihipäraselt manipuleerivad võtted ja c) petlikud võtted. Selleks, et tehisintellektisüsteem kuuluks tehisintellektimääruse artikli 5 lõike 1 punkti a kohaldamisalasse, peab see kasutama ühte või mitut neist võtetest.

a) Alalävisele tajule suunatud võtted

- (64) Kuigi tehisintellektimääruses ei ole „alalävisele tajule suunatud võtted“ määratletud, on määruse artikli 5 lõike 1 punktis a täpsustatud, et alalävisele tajule suunatud võtted ulatuvad inimese teadvusest kaugemale. Kuna alalävisele tajule suunatud võtted ja nende toimimisviis on loomult varjatud, saab nendega vältida inimese ratsionaalset kaitset manipuleerimise vastu ning mõjutada otsuseid ilma inimese teadliku tajuta, mis tekitab olulisi eetilisi probleeme ja kahjustab inimese sõltumatust, otsuste tegemist ja valikuvabadust⁵³.
- (65) Alalävisele tajule suunatud võtted peavad olema võimelised mõjutama käitumist viisil, mille puhul inimene ei ole teadlik sellisest mõjutamisest, selle toimimisest või selle mõjust tema otsuste tegemisele või väärtuste ja arvamuste kujundamisele. Eelkõige võivad alalävisele tajule suunatud võtted kasutada heli, visuaalsete vahendite või puute kaudu edastatavaid stiimuleid, mis on liiga lühikesed või peened, et neid märgata, ning mis on traditsiooniliselt tuntud ja keelatud teistes sektorites, näiteks meediareklaamides⁵⁴. Kuigi neid stiimuleid ei tajuta teadlikult, võib aju neid siiski töödelda ja need võivad mõjutada käitumist.

⁵³ Tehisintellektimääruse põhjendus 29.

⁵⁴ Vt eelkõige Euroopa Parlamendi ja nõukogu 10. märtsi 2010. aasta direktiiv 2010/13/EL audiovisuaalmeedia teenuste osutamist käsitlevate liikmesriikide teatavate õigus- ja haldusnormide koordineerimise kohta (audiovisuaalmeedia teenuste direktiiv) (ELT L 95, 15.4.2010, lk 1), mis keelab rangelt alalävisele tajule suunatud võtted audiovisuaalsetes kommertsteadaannetes.

Alalävisele tajule suunatud võtted (mis ei ole tingimata keelatud, kui kõik muud tehisintellektimääruse artikli 5 lõike 1 punktis a loetletud tingimused ei ole täidetud) on näiteks:

– **visuaalsed alalävised sõnumid:** tehisintellektisüsteem võib video ajal näidata või sellesse siduda lühidalt välgatatud pilte või teksti, mis on tehniliselt nähtavad, kuid mis vilksatavad liiga kiiresti, et teadvusel oleks võimalik neid registreerida, suutes samal ajal siiski mõjutada hoiakuid või käitumist;

– **helilised alalävised sõnumid:** tehisintellektisüsteem võib kasutada helisid või verbaalseid sõnumeid väikesel helitugevusel või teiste helidega maskeeritult, mõjutades kuulajat ilma seda teadlikult märkamata. Tehniliselt võttes jäävad need helid inimese kuulmisulatusse, kuid kuulaja ei märka neid teadlikult, sest need on väga vaiksed või neid varjab muu heli;

– **puute kaudu edastatavad alalävisele tajule suunatud stiimulid:** tehisintellektisüsteem võib stimuleerida peeneid füüsilisi aistinguid, mida ei tajuta teadlikult ja mis on võimelised mõjutama emotsionaalset seisundit või käitumist;

– **nägemis- ja kuulmislävest allapoole jäävad stiimulid:** tehisintellektisüsteem võib kasutada stiimuleid, mis ei ole lihtsalt peened või maskeeritud, vaid mida esitatakse viisil, mis muudab need normaalingimustes inimese meelte jaoks täiesti märkamatuks, näiteks visuaalsete stiimulite (nt piltide) välgatamine liiga lühikese aja vältel, et inimsilm saaks neid teadlikult tajuda, või helide esitamine inimkõrvale märkamatul helitugevusel;

– **lisatud kujutised:** tehisintellektisüsteem võib peita kujutisi muu visuaalse sisu sisse, mida ei tajuta teadlikult, kuid mida aju võib siiski töödelda ja mis võivad mõjutada käitumist;

– **eksitamine:** tehisintellektisüsteem võib juhtida tähelepanu konkreetsetele stiimulitele või sisule, et vältida muu sisu märkamist, kasutades sageli ära kognitiivseid nihkeid ja tähelepanu nõrkusi;

– **ajaga manipuleerimine:** tehisintellektisüsteem võib muuta seda, kuidas kasutaja tajub interaktsioonides aja kulgu, mõjutades seega tema käitumist ning põhjustades kannatamatust ja sõltuvust.

- (66) Tehisintellekti ja sellega seotud tehnoloogia, nagu suurandmete analüüsi, neurotehnoloogia, aju-arvuti liideste ning virtuaalreaalsuse kiire areng suurendab keerulise alalävisel manipuleerimise ohtu ja selle võimet avaldada inimese käitumisele tõhusalt alaläviselt mõju⁵⁵. Tehisintellekt võib hõlmata ka loodavaid aju-arvuti liideseid ning täiustatud võtteid, nagu unenägude häkkimine ja aju luure tarkvara.

Näiteks võib mäng kasutada ära tehisintellektipõhist neurotehnoloogiat ning aju-arvuti liideseid, mis võimaldavad kasutajatel juhtida mängu (osa) ajuaktiivsust tuvastava peakatte abil. Tehisintellekti võib kasutada selleks, et treenida kasutaja aju salaja ja ilma

⁵⁵ Vt tehisintellektimääruse põhjendus 29.

tema teadlikkuseta, et avaldada või tuletada neuroandmetest teavet, mis võib olla väga pealetükkiv ja tundlik (nt isiklikud pangaandmed, intiimne teave jne) viisil, mis võib tekitada talle olulist kahju. Tehisintellektimääruse artikli 5 lõike 1 punktis a sätestatud keeld on suunatud ainult sellise märkimisväärselt kahjuliku alalämise manipulatsiooni juhtudele, mitte aga aju-arvuti liideste rakendustele üldiselt, kui need on kavandatud ohutult ja turvaliselt ning austavad eraelu puutumatust ja üksikisiku sõltumatust.

b) Sihilikult manipuleerivad võtted

- (67) Mõistet „sihilikult manipuleerivad võtted“ ei ole tehisintellektimääruses määratletud, kuid nende all tuleks mõista võtteid, mille objektiivne eesmärk on või mis on kavandatud selleks, et mõjutada, muuta või kontrollida isiku käitumist viisil, mis kahjustab tema individuaalset sõltumatust ja valikuvabadust. Manipuleerivad võtted on tavaliselt kavandatud selleks, et kasutada ära kognitiivseid nihkeid, psühholoogilisi nõrkusi või olukorrast sõltuvaid tegureid, mis muudavad inimesed mõjutatavamaks. Tänu oma kohanemisvõimele suudavad tehisintellektisüsteemid hästi reageerida inimese individuaalsetele asjaoludele või haavatavustele ning parandada manipuleerimise tõhusust ja mõju suuremas mastaabis. Kuigi manipuleerimisvõime on oluline element võtte olemuse kindlaksmääramisel, ei ole vaja, et manipuleerivaid võtteid kasutav pakkuja või juurutaja või süsteem ise kavatseb samuti kahju tekitada⁵⁶.
- (68) Kuigi kõik manipuleerivad võtted ei ulatu inimese teadvusest kaugemale, toimivad paljud neist siiski ja võib esineda kattumist alalämisele tajule suunatud võtetega, kuna ka sellistel võtetel on lõppkokkuvõttes manipuleeriv mõju. Tehisintellektimääruse põhjenduses 29 on selgitatud, et artikli 5 lõike 1 punktis a sätestatud keeld hõlmab ka selliseid meetodeid, mille puhul üksikisikud, isegi kui nad on mõjutamiskatses kohtu teadlikud, ei pruugi olla võimelised kontrollima selle manipuleerivat mõju või sellele vastu seisma⁵⁷. Selle tulemusel mõjutatakse või suunatakse üksikisikuid käituma sellisel viisil ja tegema selliseid otsuseid, mida nad tavaolukorras ei oleks teinud, kui nende peal ei oleks kasutatud manipuleerivaid võtteid viisil, mis õõnestab nende individuaalset sõltumatust või valikuvabadust.

Üks näide sihipäraselt manipuleerivatest võtetest on sensoorne manipuleerimine, kus tehisintellektisüsteem kasutab taustaks heli või pilte, mis põhjustavad meeleolumuutusi, näiteks suurendavad ärevust ja vaimset stressi, mis mõjutavad kasutajate käitumist nii palju, et tekitavad olulist kahju.

Teine näide on personaliseeritud manipuleerimine, kus tehisintellektisüsteem, mis loob ja kohandab väga veenvaid sõnumeid üksikisiku isikuandmete põhjal või kasutab ära muid üksikisiku haavatavusi, mõjutab tema käitumist või valikuid nii palju, et see tekitab olulist kahju.

- (69) Sihilikult manipuleerivate võtete keeld hõlmab ka tehisintellektisüsteeme, mis manipuleerivad üksikisikuid, ilma et ükski inimene seda süsteemi puhul kavandanud oleks. Tehisintellektimääruse artikli 5 lõike 1 punktiga a on keelatud

⁵⁶ Vrd sellega seoses suuniste põhjendus 28 ja punktid 3.2.2. ja 3.2.3.

⁵⁷ Tehisintellektimääruse põhjendus 28.

tehisintellektisüsteemid, mis kasutavad teatavaid võtteid või mille käitumises on konkreetseid manipuleerivaid jooni. Seega võib manipuleerivate võtete kasutaja olla ka tehisintellektisüsteem ise, mitte pakkuja või juurutaja, kes on süsteemi selliselt kujutanud või seda nii kasutanud.

Näiteks võib tehisintellektisüsteem õppida manipuleerivaid võtteid, ilma et pakkuja seda kavandanud oleks, sest andmed, mille alusel seda õpetatakse, sisaldavad palju näited manipuleerivatest võtetest,⁵⁸ või sest inimese tagasiside põhjal toimuvast stiimulõpet saab manipuleerivate võtete abil ära kasutada⁵⁹.

Seevastu kui süsteemi manipuleeriv käitumine on üksnes juhuslik, ei tohiks süsteemi pidada sihipäraselt manipuleerivaid võtteid kasutavaks, eeldusel et juhul, kui olulise kahju tekkimine on mõistlikult tõenäoline, on pakkuja võtnud asjakohaseid ennetus- ja leevendusmeetmeid (vt punkt 3.2.3.c allpool).

c) *Petlikud võtted*

- (70) Tehisintellektimääruses ei ole määratletud „petlikke võtteid“. Tehisintellektimääruse põhjenduses 29 on selgitatud, et need on võtted, mis pärsivad või kahjustavad isiku sõltumatust, otsuste tegemist või vaba valikut viisil, mille puhul inimesed ei ole nendest võtetest teadlikud, või isegi kui nad on teadlikud, on võimalik nad ikka eksiteele viia või nad ei ole võimelised neid kontrollima või nendele vastu seisma. Tehisintellektisüsteemide kasutatavate petlike võtete all tuleks mõista vale või eksitava teabe esitamist, mille eesmärk või tagajärg on üksikisikute eksitamine ja nende käitumise mõjutamine viisil, mis kahjustab nende sõltumatust, otsuste tegemist ja valikuvabadust.
- (71) Sellega seoses tuleks selgitada vastastikust mõju artikli 5 lõike 1 punktis a sätestatud keelu ja tehisintellektimääruse artikli 50 lõikes 4 sätestatud juurutaja kohustuse vahel, mille kohaselt peab ta märgistama süvavõltsingud ja teatavad tehisintellekti abil loodud tekstid avalikku huvi pakkuvate küsimuste kohta,⁶⁰ ning pakkuja kohustust tagada, et inimestega suhtlevad tehisintellektisüsteemid on projekteeritud nii, et inimestele oleks teada, et nad suhtlevad tehisintellekti, mitte inimesega⁶¹. Selline nähtav avalikustamine kujutab endast leevendusmeetet, mida peaksid võimaldama ka pakkuja tehisintellektisüsteemi integreeritud elemendid, sealhulgas tehnilised meetmed, mis võimaldavad tuvastada tehisintellekti loodud ja manipuleeritud sisu⁶². Süvavõltsingute ja juturobotite nähtav märgistamine vähendab pettuse ohtu, mis tõenäoliselt tekib pärast tehisintellekti loodud sisu levitamist avalikkusele, ning vähendab üksikisiku arvamuse

⁵⁸ M. Carroll *et al.*, Characterising Manipulation from AI Systems, In Equity and Access in Algorithms, Mechanisms, and Optimization (EAAMO 23), 30. oktoober kuni 1. november, 2023, Boston, Massachusettsi osariik, Ameerika Ühendriigid. ACM, New York, New Yorki osariik, Ameerika Ühendriigid, 13 lehekülge, <https://doi.org/10.1145/3617694.3623226> | 2303.09387.

⁵⁹ D. Amodei, *et al.*, *Concrete Problems in AI Safety*, 36th Conference on Neural Information Processing Systems (NeurIPS 2022), arXiv:1606.06565; J. Skalse *et al.*, *Defining and Characterizing Reward Gaming*, Advances in Neural Information Processing Systems 35 (NeurIPS 2022); C. Denison *et al.*, *Sycophancy to Subterfuge: Investigating Reward-Tampering in Large Language Models*, 36th Conference on Neural Information Processing Systems (NeurIPS 2022), arXiv:2406.10162.

⁶⁰ Tehisintellektimääruse artikli 50 punkt 4.

⁶¹ Tehisintellektimääruse artikli 50 punkt 1.

⁶² Tehisintellektimääruse artikli 50 punkt 2.

ja veendumuste kujundamisele ja käitumisele avaldatava kahjuliku moonutava mõju ohtu.

- (72) Seevastu tehisintellektimääruse artikli 5 lõike 1 punktis a sätestatud keelul on palju piiratum kohaldamisala. See võib hõlmata näiteks juhtumeid, kus juturobot või tehisintellekti loodud petlik sisu esitab vale või eksitavat teavet viisil, mille eesmärk või tagajärg on üksikisikute petmine ja nende käitumise moonutamine, mida ei oleks juhtunud, kui nad ei oleks puutunud kokku tehisintellektisüsteemi või tehisintellekti loodud petliku sisuga, eriti kui sellest ei ole nähtavalt teavitatud⁶³.
- (73) Nagu sihipäraselt manipuleerivate võtete puhulgi, võib petlike võtete keeld hõlmata ka tehisintellektisüsteeme, mis petavad üksikisikuid ilma inimese tahtmata (vt punkt 3.2.1.b eespool). Näiteks sõltumata sellest, kas nende pakkujad kavatsevad sellist tulemust saavutada, võivad tehisintellektisüsteemid õppida petlike võtteid lihtsalt seetõttu, et see suurendab nende tulemuslikkust ülesande puhul, mille jaoks nad on välja töötatud, näiteks stiimulõppe teel⁶⁴.

Üks näide tehisintellekti kasutatavatest petlikest võtetest on tehisintellekti juturobot, mis kehastab sünteetilise häälega inimese sõpra või sugulast ja üritab seda inimest teeselda, mis põhjustab pettusi ja olulist kahju.

Teine näide on tehisintellektisüsteem, mis õpib tuvastama, millal teda hinnatakse, ja peatab ajutiselt igasuguse soovimatu käitumise, kuid jätkab sellist käitumist, kui hindamisperiood läbi saab⁶⁵. Selline petlik käitumine on eriti ohtlik, kuna see ei allu mis tahes välisele inimjärelvalvele, mida süsteemi üle tehakse, ja see võidakse keelata, kui see võib mõistliku tõenäosusega põhjustada olulist kahju.

Seevastu generatiivset tehisintellektisüsteemi, mis esitab vale või eksitavat teavet ja hallutsinatsioone juhuslikult,⁶⁶ ei saa pidada tehisintellektimääruse artikli 5 lõike 1 punkti a tähenduses petlikke võtteid kasutavaks süsteemiks, võttes arvesse generatiivse tehisintellekti piiranguid ja tehnilist taset. Eelkõige võib see juhtuda juhul, kui süsteemi pakkuja on kasutajaid nõuetekohaselt teavitanud süsteemi piirangutest ja integreerinud süsteemi asjakohased kaitsemeetmed selliste tagajärgede minimeerimiseks ning tingimusel, et süsteem ei ole ette nähtud tundliku konteksti jaoks ja seda ei kasutata tundlikus kontekstis (nt tervishoid, haridus, valimised), kus võivad tekkida tõsised kahjulikud tagajärjed (vt ka allpool punktis 3.2.3.c esitatud kaalutlused).

⁶³ Kuigi põhimõtteliselt on tehisintellektimääruse artiklis 50 sätestatud läbipaistvuskohustuste eesmärk minimeerida sülvavõltsingute ja juturobotite manipuleerivat mõju, võib esineda juhtumeid ja olukordi, kus vaatamata teabeteatistele võivad need petlikud võtted siiski avaldada märkimisväärset mõju üksikisikutele ja moonutada nende käitumist nii palju, et see kahjustab isikute individuaalset sõltumatust ja teadlikku otsustusõigust, nii et neid ei tohiks väärkasutada desinformatsiooni ja manipuleerimise eesmärgil ning need võivad mõnel juhul isegi kuuluda artikli 5 lõike 1 punktis a sätestatud keelu alla, kui kõik muud keelu tingimused on täidetud (sealhulgas oluline kahju).

⁶⁴ F. Ward, F. Toni, F. Belardinelli, T. Everitt, [Honesty Is the Best Policy: Defining and Mitigating AI Deception \(neurips.cc\)](#), 36. konverents edasiminekute kohta neuroandmete töötlemise süsteemides (NeurIPS 2023); P. Park. *et al.* [AI deception: A survey of examples, risks, and potential solutions \[2406.10162\] Patterns, Volume 5, Issue 5, 100988.](#)

⁶⁵ J. Lehman, J. Clune, D. Misevic, C. Adami, L. Altenberg, J. Beaulieu, *et al.* The surprising creativity of digital evolution: A collection of anecdotes from the evolutionary computation and artificial life research communities, Artificial life, 26. köide, nr 2, lk 274–306, 2020.

⁶⁶ „Hallutsinatsioon“ on mõiste, millega kirjeldatakse generatiivsete tehisintellektisüsteemide tehnilist puudujääki, mille puhul süsteem genereerib soovimatut teavet, mis on väljamõeldis või faktiliselt vale, ilma et arendajad oleksid seda kavatsenud. Vt lähemalt Ji Ziwei *et al.*, [Survey of Hallucination in Natural Language Generation | ACM Computing Surveys](#), 55, nr 12, artikkel nr 248, lk 1–38.

d) Võtete kombineerimine

- (74) Tehisintellektimääruse artikli 5 lõike 1 punkti a kohaldatakse alaläviste, sihipäraselt manipuleerivate või petlike võtete või nende kombinatsioonide suhtes, millel võib olla kombineeritud mõju. Nagu eespool öeldud, võivad ka sihipäraselt manipuleerivad võtted olla oma olemuselt alalävised, kui nende toimimisviis ulatub inimese teadvusest kaugemale.
- (75) Lisaks sellele, kui sihipäraselt manipuleerivaid ja petlikke võtteid kasutatakse koos, võib see märkimisväärselt mõjutada üksikisikute käitumist, suunates nad tegema otsuseid, mis põhinevad alalävisel manipuleerimisel ja valearusaamadel. Selline kombinatsioon võib tekitada tagasisideahela, mille puhul on vähem tõenäoline, et inimesed kahtlevad saadud teabes või hindavad seda kriitiliselt, kuna manipuleerivad elemendid on nende kognitiivseid nihkeid ja emotsionaalseid reaktsioone juba ette valmistanud.

3.2.2. Eesmärgiga moonutada oluliselt isiku või isikute rühma käitumist

- (76) Kolmas tingimus, et tehisintellektimääruse artikli 5 lõike 1 punktis a sätestatud keeldu saaks kohaldada, on see, et kasutatava alalävisele tajule suunatud, sihipäraselt manipuleeriva või petliku võtte eesmärk või tagajärg peab olema moonutada oluliselt isiku või isikute rühma käitumist. See eeldab mitte väikest mõju käitumisele, vaid märkimisväärselt mõju, mis kahjustab inimese sõltumatust ja valikuvabadust. Tahtlus ei ole siiski vajalik nõue, kuna tehisintellektimääruse artikli 5 lõike 1 punkt a hõlmab ka selliseid kasutusviise, mille puhul võib olulise moonutamise põhjustamine olla üksnes selle tagajärg. Käitumise võimaliku olulise moonutamise ja tehisintellektisüsteemi rakendatud alalävisele tajule suunatud, sihipäraselt manipuleeriva või petliku võtte vahel peaks olema usutav / mõistlikult tõenäoline põhjuslik seos.

a) „Käitumise olulise moonutamise“ mõiste

- (77) „Käitumise oluline moonutamine“ on tehisintellektimääruse artikli 5 lõike 1 punkti a keskne mõiste. See hõlmab alalävisele tajule suunatud, sihipäraselt manipuleerivate või petlike võtete kasutamist, mis on võimelised mõjutama inimeste käitumist viisil, mis kahjustab oluliselt nende võimet teha teadlikke otsuseid, suunates neid seega käituma viisil või tegema otsuseid, mida nad muidu ei oleks teinud.
- (78) „Oluline kahjustamine“ viitab märgatavalt vähenenud võimele teha teadlikke ja sõltumatuid otsuseid, mis paneb üksikisiku käituma viisil või tegema otsuseid, mida ta muidu ei oleks teinud. See läheb kaugemale väiksemast või tähtsusetust mõjust ja hõlmab märkimisväärselt moonutatust või takistust otsuste ja vabade valikute tegemisel, sealhulgas seoses arvamuste ja veendumuste kujundamisega. See näitab, et oluline moonutamine hõlmab teatud määral surveid, manipuleerimist või pettust, mis läheb kaugemale seaduslikust veenmisest, mis jääb väljapoole keelu kohaldamisala (vt punkt 3.5.1 allpool).
- (79) Teadlik otsus eeldab seda, et inimene mõistab asjakohast teavet ja on sellega kursis, kaasa arvatud olemasolevad võimalused, iga valiku riskid ja kasu,

tehisintellektisüsteemi võimalik mõju tema käitumisele ning vajaduse korral muu kontekstipõhine teave, mis on isiku otsuste tegemiseks või käitumiseks oluline.

- (80) Mõiste „käitumise oluline moonutamine“ tõlgendamisel võib sobivaks aluseks olla liidu tarbijakaitseõigus, eelkõige direktiiv 2005/29/EÜ (ebaausate kaubandustavade direktiiv). Ebaausate kaubandustavade direktiiv keelab mitmesugused ebaausad, eksitavad ja agressiivsed kaubandustavad (direktiivi artiklid 5–9), mis võivad panna tarbijaid tegema tehinguotsuseid, mida nad muidu ei oleks teinud. Kooskõlas Euroopa Liidu Kohtu ja komisjoni suunistega ebaausate kaubandustavade direktiivi kohta⁶⁷ ei ole vaja tõestada, et tarbija majanduslik käitumine on moonutatud – piisab sellest, kui tõendada, et kaubandustava võib „tõenäoliselt“ mõjutada (st on võimeline mõjutama) keskmise tarbija tehinguotsust⁶⁸. Euroopa Liidu Kohus on samuti rõhutanud, et isegi täpne teave võib olla eksitav, kui see esitatakse viisil, mis moonutab tarbija otsustusprotsessi⁶⁹. Riiklike täitevasutuste ülesanne on uurida iga üksikjuhtumi fakte ja asjaolusid (*in concreto*) ning hinnata asjaomase tava võimalikku mõju keskmise tarbija otsustusprotsessile (*in abstracto*)⁷⁰. Selleks peavad nad lähtuma keskmise tarbija vaatenurgast, mis on Euroopa Liidu Kohtu välja töötatud võrdlusalus, mis on nüüdseks lisatud ebaausate kaubandustavade direktiivi⁷¹.
- (81) Tehisintellektimääruse artikli 5 lõike 1 punktis a sätestatud keelu puhul peavad turujärelevalveasutused uurima ka iga juhtumi konkreetseid fakte ja asjaolusid, hinnates, kas tehisintellektisüsteemi kasutatav alalävisele tajule suunatud, sihipäraselt manipuleeriv või petlik võte võib tõenäoliselt kahjustada oluliselt sihtrühma kuuluva keskmise üksikisiku sõltumatust, otsuste tegemist ja valikuvabadust, kui süsteem mõjutab isikute rühma viisil, mis võib mõistliku tõenäosusega põhjustada olulist kahju. Selline tõlgendus näib olevat õigustatud, arvestades, et tehisintellektimääruse eesmärk on täiendada ebaausate kaubandustavade direktiivi⁷² ja seda tuleb kohaldada järjepidevalt. Samas, arvestades, et ka tehisintellektimääruse artikli 5 lõike 1 punktis a viidatakse võimalusele moonutada isiku käitumist ja juhul, kui keskmise üksikisiku perspektiivi on teatavas kontekstis raske või ebatõhus hinnata (näiteks väga kohandatud või isikupärastatud manipuleerimise või konkreetsetele haavatavatele rühmadele avaldatava kahjuliku mõju tõttu), võib konkreetseid juhtumeid uurida ka konkreetsete üksikisikute seisukohast, hinnates, mil määral on tehisintellektisüsteem, mis kasutab

⁶⁷ Vt ka komisjoni teatis „Suunised Euroopa Parlamendi ja nõukogu direktiivi 2005/29/EÜ (mis käsitleb ettevõtja ja tarbija vaheliste tehingutega seotud ebaausaid kaubandustavasid siseturul) tõlgendamiseks ja kohaldamiseks“ (ELT C 526, 29.12.2021, lk 1).

⁶⁸ Kohtuotsus, Euroopa Kohus (viies koda), 26. oktoober 2016, Canal Digital Danmark A/S, EU:C:2016:800, C-611/14, punkt 73.

⁶⁹ Kohtuotsus, Euroopa Kohus, 19. detsember 2013, Trento Sviluppo ja Centrale Adriatica, C-281/12, EU:C:2013:859.

⁷⁰ Komisjoni teatis, „Suunised Euroopa Parlamendi ja nõukogu direktiivi 2005/29/EÜ (mis käsitleb ettevõtja ja tarbija vaheliste tehingutega seotud ebaausaid kaubandustavasid siseturul) tõlgendamiseks ja kohaldamiseks“ (ELT C 526, 29.12.2021, lk 1).

⁷¹ Vt ebaausate kaubandustavade direktiivi põhjendused 18 ja 19. „Keskmine tarbija“ on inimene, kellel on mõeldukalt teavet ning kes on mõeldukalt tähelepanelik ja ettevaatlik, võttes samuti arvesse sotsiaalseid, kultuurilisi ja lingvistilisi näitajaid. Keskmise tarbija katse ei ole statistiline katse (st selle jaoks ei ole vaja tõestada, et teatava protsendi tarbijate puhul oleks äritava nende käitumist oluliselt moonutanud/kahjustanud). Katse põhineb proportsionaalsuse põhimõttel. Ebaausate kaubandustavade direktiivis on kasutatud seda mõistet selleks, et saavutada konkurentsi soodustaval turul õige tasakaal vajaduse vahel ühelt poolt kaitsta tarbijaid ja teisalt edendada vabakaubandust. Kohtud ja ametiasutused peavad kasutama oma otsustusvõimet, et määrata iga juhtumi puhul kindlaks keskmise tarbija tüüpiline reaktsioon. Suunistes ebaausate kaubandustavade direktiivi kohta soovitas komisjon neil kasutada teavet käitumise kohta ja muid andmeid. Kohtuasjas C-646/22 (Compass Banca) on selgitatud, et keskmise tarbija määratlus ei välista võimalust, et üksikisiku otsustusvõimet võivad kahjustada piirangud, näiteks kognitiivsed nihted. Kohtuotsus, Euroopa Kohus (viies koda), 14. november 2024, Compass Banca SpA vs. Autorità Garante della Concorrenza e del Mercato (AGCM), C-646/22, EU:C:2024:957.

⁷² Tehisintellektimääruse põhjendus 29.

alalävisele tajule suunatud, sihipäraselt manipuleerivaid või petlikke võtteid, võimeline kahjustama konkreetsetel juhtudel nende individuaalset sõltumatust ning on tekkinud või võib tekkida oluline kahju.

b) 1. stsenaarium: keelatud tehisintellektisüsteemid, mille eesmärk on oluliselt moonutada käitumist

- (82) Tehisintellektimääruse artikli 5 lõike 1 punkti a kohaldatakse tehisintellektisüsteemide suhtes, mis kasutavad eespool nimetatud võtteid ja mille esimese stsenaariumi eesmärk on „isiku või isikute rühma käitumise oluline moonutamine“. Selline eesmärk võib olla tehisintellektisüsteemi pakkujal või juurutajal või süsteemil endal oma kaudsete eesmärkide raames, mida ta võib järgida⁷³. Seda eesmärki tuleks eristada tehisintellektisüsteemi sihtotstarbest (tehisintellektimääruse artikli 3 punkt 12). Isegi kui see on pakkuja poolt ette nähtud, ei kattu manipuleerimise eesmärk enamasti sellise kasutamise eesmärgiga, milleks süsteemi pakutakse, ning sageli ei ole see läbipaistev ega ole pakkuja esitatud teabes (nt kasutusjuhendis, reklaami- või müügitmaterjalides ja -avaldustes ning tehnilistes dokumentides) sellisena määratletud.

Näiteks erinevates kontekstides kasutatav juturobot on projekteeritud kasutama alaläviseid sõnumi edastamise võtteid, näiteks lühikesi visuaalseid vihjeid väljatades ja kuuldamatu auditiivseid signaale kasutades, või kasutama reklaamis ära kasutajate emotsionaalset sõltuvust või konkreetseid haavatavusi. Neid võtteid kasutatakse eesmärgiga moonutada oluliselt kasutajate käitumist, sest need on objektiivselt süsteemi projekteeritud element, mille eesmärk on mõjutada tarbijate otsuotsuseid, ilma et nad sellest teadlikult aru saaksid, et sundida inimesi tegema märkimisväärselt kahjulikke finantsotsuseid.

Tehisintellektisüsteemide kasutamist teiste isikute kehastamiseks võib pidada ka tehisintellektisüsteemiks, mida kasutatakse eesmärgiga eksitada ja oluliselt moonutada isikute käitumist, kui isikut tegelikult eksitatakse, mõjutades seega oluliselt tema võimet teha teadlikke otsuseid isiku identiteedi kohta.

Kui nende näidete puhul on täidetud ka teised tehisintellektimääruse artikli 5 lõike 1 punktis a nimetatud tingimused, eelkõige olulise kahju mõistes, jäävad need süsteemid tõenäoliselt keelu kohaldamisalasse, kuid seda tuleb hinnata iga juhtumi puhul eraldi.

c) 2. stsenaarium: keelatud tehisintellektisüsteemid, mille „tagajärg“ on oluliselt moonutada käitumist

- (83) Pakkuja või juurutaja kavatsus moonutada oluliselt isiku või isikute rühma käitumist on piisav, kuid mitte vajalik tingimus, et kohaldada tehisintellektimääruse artikli 5 lõike 1 punktis a sätestatud keeldu. See keeld kehtib ka siis, kui sellist kavatsust ei ole, kuid tehisintellektisüsteemi kasutatavate võtete mõju suudab oluliselt moonutada isiku või isikute rühma käitumist sellisel määral, et see kahjustab nende individuaalset sõltumatust ja valikuvabadust.

⁷³

Vt tehisintellektimääruse artikli 3 punkt 1, milles on sätestatud, et tehisintellektisüsteem võib oma ülesannete täitmisel püüda saavutada otseseid või kaudseid eesmärke, mis võivad hõlmata ka kaudseid manipuleerivaid või petlikke eesmärke, isegi kui süsteem ei ole selgesõnaliselt selliselt programmeeritud.

- (84) Keelu kohaldamiseks on siiski alati vaja usutavat / mõistliku tõenäosusega põhjuslikku seost tehisintellektisüsteemi kasutatava alalävisele tajule suunatud, sihipäraselt manipuleeriva või petliku võtte ja selle käitumisele avalduva mõju vahel. Tarbijakaitseõiguse kohaselt ei pea selline mõju olema täielikult realiseerunud, kuid peab olema piisavalt tõendeid selle kohta, et see võib tõenäoliselt realiseeruda ja kahjustada üksikisiku sõltumatust, tuginedes juhtumi kõigi asjaolude objektiivsele hindamisele ning olemasolevatele teaduslikele teadmistele ja meetoditele, samuti olemasolevale teabele selle kohta, milline on süsteemi mõju üksikisikute käitumisele tegelikult. Selles kontekstis piisab tingimuse täitmiseks asjaolust, et süsteem on võimeline ajendama käitumist, mis kahjustab oluliselt üksikisikute valikuvabadust ja nende võimet teha teadlikke otsuseid, ja see ei sõltu kaalutlustest, mis on seotud kahju tekkimise ajaga (nt sõltuvusele sarnaneva käitumise puhul), kuni kahju tekkimine on mõistlikult tõenäoline.

Näiteks tehisintellektipõhise nn heaolu-juturobotiga on pakkuja eesmärk toetada ja suunata kasutajaid tervisliku elustiili säilitamisel ning anda kohandatud nõuandeid psühholoogiliste ja füüsiliste harjutuste kohta. Kui aga juturobot kasutab ära üksikisiku haavatavust, et omandada ebatervislikke harjumusi või tegeleda ohtlike tegevustega (nt tegeleda liigse spordiga ilma puhkamata või vett joomata), kui võib põhjendatult eeldada, et teatud kasutajad järgivad seda nõuannet, mida nad muidu ei oleks teinud, ja kannatavad olulist kahju (nt südameinfarkt või muu tõsine terviseprobleem), siis kuulub see tehisintellektisüsteem tehisintellektimääruse artikli 5 lõike 1 punktis a sätestatud keelu alla, isegi kui selline käitumine ja kahjulikud tagajärjed inimestele ei olnud pakkuja kavatsus.

Keelu kohaldamiseks piisab ainuüksi sellest, et juturobot on võimeline oluliselt kahjustama üksikisiku sõltumatust ja moonutama teatavate kasutajate käitumist oluliselt kahjulikul viisil ning et pakkuja ei ole sellise oluliselt kahjuliku mõju vältimiseks võtnud asjakohaseid ennetus- ja leevendusmeetmeid (vt asjakohaseid kaalutlusi kahju mõistliku tõenäosuse kohta punktis 3.2.3 ja punkti 3.5 kohaldamisalast välja jäävate olukordade kohta).

3.2.3. Põhjustab (mõistliku tõenäosusega) olulist kahju

- (85) Lõpetuseks – selleks, et tehisintellektimääruse artikli 5 lõike 1 punktis a sätestatud keeld oleks kohaldatav, peab isiku või isikute rühma käitumise moonutamine põhjustama või mõistliku tõenäosusega põhjustama sellele isikule, teisele isikule või isikute rühmale olulist kahju või sellise kahju tekkimine peab olema mõistlikult tõenäoline. Selles kontekstis on olulised selgitamist vajavad mõisted kahju liigid, mida keeld hõlmab, kahju olulisuse künnis ning kahju mõistlik tõenäosus ja põhjuslik seos kahju ja manipuleeriva või petliku võtte ning isiku käitumise vahel.

a) Kahju liigid

- (86) Tehisintellektimäärus käsitleb mitmesugust manipuleerivate ja petlike tehisintellektisüsteemidega seotud kahjulikku mõju, millest igaühel on erinevad

tagajärjed üksikisikutele ja isikute rühmadele, keda need võivad mõjutada⁷⁴. Tehisintellektimääruse artikli 5 lõike 1 punkti a puhul on peamised kahju liigid füüsiline, psühholoogiline, rahaline ja majanduslik kahju,⁷⁵ mis võivad teatud juhtudel olla ühendatud laiemal ühiskondliku kahjuga⁷⁶.

- (87) Füüsiline kahju hõlmab igasugust vigastust või kahju inimese elule ja tervisele, samuti varale tekitatud materiaalsel kahju. Inimese elu ja tervise füüsilisel kahjustamisel on paljudel juhtudel vahetud, tõsised ja pöördumatud tagajärjed. Kooskõlas tooteohutuse loogikaga on tehisintellektimääruse eesmärk keelata tehisintellekti abil toimuv manipuleerimine ja pettus, mis toob kaasa olulist füüsilist kahju.

Näiteks reklaamib tehisintellektipõhine juturobot kasutajatele enesevigastamist või innustab neid enesetappu sooritama või teistele isikutele või isikute rühmadele kahju tegema, propageerides terroristlikku sisu või innustades vägivalda teatavate isikute või isikute rühmade (st vähemuste) vastu.

- (88) Psühholoogiline kahju on eriti oluline seoses tehisintellektisüsteemidega, mis rakendavad manipuleerivaid võtteid, mis kasutavad ära kognitiivseid ja emotsionaalseid nõrkusi ning mõjutavad inimese käitumist viisil, mis võib põhjustada olulist kahju. Psühholoogiline kahju hõlmab kahjulikku mõju inimese vaimsele tervisele ning psühholoogilisele ja emotsionaalsele heaolule. Sellised kahjud on eriti olulised, sest need võivad aja jooksul kuhjuda ja ei pruugi olla kohe nähtavad, kuid võivad põhjustada pikaajalisi ja tõsiseid tagajärgi. Siiski on neid raskem mõõta, mis nõuab juhtumipõhist hindamist, eeskätt nende raskusastme kindlaksmääramiseks, võttes arvesse kõiki juhtumi asjakohaseid asjaolusid.

Näiteks tehisintellektipõhise kaaslaste rakendus, mis on loodud jälgendama inimese käitumist, käitumist ja emotsioone, kasutab antropomorfseid omadusi ja emotsionaalseid vihjeid, et mõjutada kasutajate tundeid, hoiakuid ja arvamusi, muutes need kasutajad teenusest emotsionaalselt sõltuvaks, soodustades sõltuvusele sarnast käitumist ja põhjustades potentsiaalselt olulist kahju, näiteks enesetapakäitumist ja teiste inimeste kahjustamise riski⁷⁷.

- (89) Rahaline ja majanduslik kahju võib hõlmata mitmesugust negatiivset mõju, sealhulgas rahalist kahju, majanduslikku tõrjutust ja majanduslikku ebastabiilsust.

Näiteks juturobot, mis pakub pettuse teel tooteid, mis põhjustavad märkimisväärset rahalist kahju.

- (90) Kui tehisintellektimääruse artikli 5 lõike 1 punkti a kohaldamisel hinnatakse tehisintellektisüsteemide põhjustatud kahju, on oluline rõhutada, et sageli ei esine kahju isoleeritult, vaid avaldub kombinatsioonis teiste kahjudega, põhjustades kombineeritud

⁷⁴ Vt tehisintellektimääruse artikli 5 lõike 1 punkt a.

⁷⁵ Tehisintellektimääruse põhjendus 29.

⁷⁶ Vt tehisintellektimääruse põhjendus 28, milles selgitatakse, et keelud võivad põhjustada ka laiemat ühiskondlikku kahju ja olla vastuolus selliste liidu väärtustega nagu inimväärikuse austamine, vabadus, võrdsus, demokraatia ja õigusriik ning põhiõiguste hartas sätestatud põhiõigustega. Vt ka tehisintellektimääruse artiklit 1, mille eesmärk on kaitsta demokraatiat ja õigusriigi põhimõtet kui ELi väärtusi.

⁷⁷ Renwen Zhang, Han Li, Han Meng, Jinyuan Zhan, Hongyuan Gan ja Yi-Chieh Lee. 2024. The Dark Side of AI Companionship: A Taxonomy of Harmful Algorithmic Behaviors in Human-AI Relationships, 1, 1 (november 2024), 28 lehekülge.

ja mitmekülgset negatiivset mõju. Kombineeritud kahju mõistmine on kahju olulisuse tõhusaks hindamiseks keskse tähtsusega (vt ka punkt 3.2.3.b), kusjuures füüsiline, psühholoogiline, rahaline ja majanduslik kahju võivad olla omavahel ühendatud ning süvendada üldmõju üksikisikutele ja kogukondadele ning isegi avaldada laiemat kahjulikku mõju.

Näiteks:

- füüsilist kahju tekitav tehisintellektisüsteem võib põhjustada ka psühholoogilist traumat, stressi ja ärevust ning vastupidi. Näiteks toodetes ja muudes tehisintellektipõhistes rakendustes kasutatavate tehisintellektisüsteemide sõltuvust tekitav disain võib põhjustada psühholoogilist kahju, soodustades sõltuvuskäitumist, ärevust ja depressiooni. Vaimne stress võib põhjustada füüsilist kahju, näiteks unetust ja muid stressiga seotud tervisehäireid ja füüsilisi probleeme;
- tehisintellektil põhinev ahistamine võib põhjustada nii vaimset stressi kui ka stressi füüsilisi ilminguid, nagu unetus, füüsilise tervise halvenemine või immuunsüsteemi nõrgenemine;
- tehisintellekti kasutamisest tulenev psühholoogiline kahju võib põhjustada ka füüsilist kahju, sealhulgas surma. Näiteks võivad internetis kasutatavad tehisintellektisüsteemid hõlbustada soopõhist vägivalda ahistamise, ahistava jälitamise, küberkiusamise ja seksuaalse väljapressimise kaudu;
- individuaalne psühholoogiline kahju, mis tuleneb näiteks sellest, et tehisintellekti abil luuakse tegelikke isikuid jäljendavaid sünavõltsinguid, et petta ja kahjustada üksikisikute individuaalset sõltumatust, otsuste tegemist ja valikuvabadust, võib olla seotud ka olulise kahjuga isikute rühmadele (nt kui neil on sama etniline või rassiline päritolu või sugu kui sünavõltsingutes kujutatud ohvritel).

b) Kahju olulisuse künnis

- (91) Tehisintellektimääruse artikli 5 lõike 1 punktis a sätestatud keeld kehtib ainult siis, kui alalävisele tajule suunatud, manipuleerivatest ja petlikest võtetest põhjustatud kahju on „**oluline**“. Tehisintellektimääruses ei ole esitatud „olulise kahju“ määratlust, kuid seda tuleks mõista nii, et see tähendab **olulist kahjulikku mõju** isikute ja rühmade füüsilisele ja vaimsele tervisele või rahalistele ja majanduslikele huvidele⁷⁸. Olulise kahju kindlaksmääramine põhineb faktidel, mis nõuab iga juhtumi individuaalsete asjaolude hoolikat kaalumist ja iga juhtumi eraldi hindamist, kuid individuaalsed mõjud peaksid igal juhul olema olulised.
- (92) Teistes liidu õigusaktides kasutatakse olulise kahju mõistet samuti nüansirohke ja kontekstist sõltuva mõistena, juhindudes kõrgetasemelise kaitse ja ennetustegevuse eesmärkidest⁷⁹. Analoogia põhjal võib tuletada järgmised põhilised tegurid, mida võiks

⁷⁸ Tehisintellektimääruse põhjendus 29.

⁷⁹ Vt kohtuotsus, Euroopa Kohus, 7. september 2004, Waddenvereniging ja Vogelbeschermingsvereniging, C-127/02, EU:C:2004:482, ja kohtuotsus, Euroopa Kohus, 11. aprill 2013, Sweetman jt, C-258/11, EU:C:2013:220.

arvesse võtta, kui hinnatakse, mis kujutab endast olulist kahju tehisintellektimääruse artikli 5 lõike 1 punkti a tähenduses.

- **Kahju raskusaste** viitab kahju astmele, mis on tekkinud või võib mõistliku tõenäosusega tekkida tehisintellektisüsteemi kasutamisel, kusjuures olulisel kahjul on objektiivne ja jälgitav mõju. Selles kontekstis on eriti oluline kaaluda tehisintellektisüsteemi vastastikuseid sõltuvusi, eri liiki kahjude kombinatsiooni ja kahjulikku mõju üksikisikutele või isikute rühmadele.
- **Kontekst ja kumulatiivne mõju:**⁸⁰ kahju raskusastme hindamisel on oluline osa konkreetsel kontekstil, sealhulgas senisel olukorral ja mitme tegevuse kumulatiivsel mõjul.
- **Mastaap ja intensiivsus** : kahju ulatus ja kahjuliku mõju intensiivsus on kahju olulisuse hindamisel otsustava tähtsusega. Kahju olulisuse hindamisel on oluline ka see, kas kahju mõjutab suurt hulka inimesi.
- **Mõjutatud isikute haavatavus:** teatavad rühmad, nagu lapsed, eakad või puuetega inimesed, võivad olla teatavate tehisintellektisüsteemide tekitatud kahju suhtes vastuvõtlikumad. See, mida võib pidada vähem oluliseks kahjuks inimeste puhul üldiselt, võib selliste haavatavate rühmade, eriti laste puhul olla oluline ja vastuvõetamatu.
- **Kestus ja pöördumus:** pikaajaline või pöördumatu kahju ületab tavaliselt olulise kahju künnise. Lühiajalist ja tagasipööratavat mõju võib pidada vähem oluliseks, kui see ei esine sageli.

- (93) Tehisintellektimääruse eesmärk tagada kõrgetasemeline kaitse koostoimes ELi toimimise lepingu artikli 191 lõikega 2 viitab terviklikule lähenemisviisile kaitse tagamisel, kui hinnatakse kahju olulisust. See tähendab, et tuleb arvestada nii vahetut ja otsest kahju kui ka süsteemset kaudset kahjulikku mõju, mis on seotud tehisintellektisüsteemidega, mis kasutavad alalävisele tajule suunatud, sihilikult manipuleerivaid või petlikke võtteid, mis on mõeldud või võimelised kahjustama isikute ja rühmade individuaalset sõltumatust, otsuste tegemist ja valikuvabadust.

Oluline füüsiline kahju, mida tehisintellektisüsteem võib mõistliku tõenäosusega põhjustada, hõlmab näiteks vigastusi või surmajuhtumeid või piisavalt rasket mõju üksikisikute tervisele või vara hävitamist. Sellise künnise ületanuteks tuleks lugeda tehisintellektisüsteeme, mis soovivad üksikisikule kuritegusid, näiteks seksuaalset kuritarvitamist ja ärakasutamist, äärmuslikku vägivaldset või terroristlikku sisu, või motiveerivad üksikisikuid kuritegusid toime panema, ennast vigastama või teistele isikutele kahju tegema.

Seevastu väiksema füüsilise kahju hulka võivad kuuluda kergemad vigastused, näiteks muljumised või ajutine ebamugavustunne, millel ei ole märkimisväärsed või püsivad tagajärgi ja mis seetõttu ei saavuta tehisintellektimääruse artikli 5 lõike 1 punkti a kohast olulisuse künnist. Tuleb hinnata, kas füüsiline kahju puudutab konkreetselt

haavatavaid rühmi, näiteks lapsi, samuti tuleb hinnata kahju ulatust ja seda, kas see on seotud muud liiki kahjuga, näiteks psühholoogilise, rahalise jms kahjuga. See nõuab iga juhtumi puhul eraldi hindamist, võttes arvesse asjaolusid ja eespool esitatud kriteeriume, millest hindamisel juhinduda.

On arvukalt juhtumeid, kus olulise kahju künnist tõenäoliselt ei saavutata, isegi kui süsteemid võivad kasutada alalävisele tajule suunatud, sihilikult manipuleerivaid või petlikke võtteid (vt näiteid punktis 3.5 allpool).

c) Põhjuslik seos ja kahju mõistliku tõenäosuse künnis

- (94) Mõistet „mõistlik tõenäosus“ kasutatakse tehisintellektimääruse artikli 5 lõike 1 punktis a, et määrata kindlaks, kas võimaliku olulise kahju manipuleeriva või petliku võtte vahel, mis on võimeline moonutama isiku käitumist viisil, mis kahjustab tema valikuvabadust, on olemas usutav / mõistliku tõenäosusega põhjuslik seos. See mõiste võimaldab keeldu kohaldada mitte ainult juhul, kui kahju on tekkinud, vaid ka juhul, kui selle tekkimine on tehisintellektimääruse ohutusloogika järgi mõistliku tõenäosusega. Selles kontekstis on eriti oluline hinnata, kas tehisintellektisüsteemi pakkuja või juurutaja oleks võinud mõistlikult ette näha olulist kahju, mida kasutatud alalävisele tajule suunatud, sihilikult manipuleerivad või petlikud võtted võivad mõistliku tõenäosusega põhjustada, ning kas ta võttis asjakohaseid ennetus- ja leevendusmeetmeid, et vältida või leevendada sellise olulise kahju ohtu. See eeldab mõistlikkuse hindamist objektiivsel alusel ja vastavalt üldtunnustatud kriteeriumidele (nt tehnilised ja teaduslikud kriteeriumid), sealhulgas ratsionaalsuse kriteerium, millega määratakse kindlaks usutav põhjuslik seos tehisintellekti kasutusviisi ja potentsiaalselt tekkiva olulise kahju vahel. Tehisintellektisüsteemi ja selle toimimise läbipaistmatus või läbipaistvus võib mõjutada järeldusi selle põhjusliku seose kohta ja seega ka keelu kohaldamist.
- (95) Selleks et vältida tõenäoliselt keelatud tehisintellektisüsteemide pakkumist või kasutamist, julgustatakse selliseid manipuleerivaid või petlikke võtteid kasutavate tehisintellektisüsteemide pakkujaid ja juurutajaid võtma näiteks järgmisi asjakohaseid meetmeid:
1. **Läbipaistvus ja individuaalne sõltumatus:** tagada läbipaistvus selle kohta, kuidas tehisintellektisüsteem toimib, selge teave selle võimaluste ja piirangute kohta ning asjakohane teave, et tagada teadlike otsuste tegemine; austada üksikisiku sõltumatust ja vältida ekspluateerivat või petlikku tegevust, mis tõenäoliselt mõjutab oluliselt üksikisiku sõltumatust, otsuste tegemist ja valikuvabadust potentsiaalselt kahjulikul viisil; integreerida asjakohased kasutajate kontrolli- ja kaitsemeetmed, et tagada, et süsteem ei ole petlik ja toimib seadusliku veenmise piirides, mis ei kuulu keelu kohaldamisalasse (vt punkt 3.5.1).
 2. **Vastavus asjakohastele kohaldatavatele õigusaktidele:** paljudel juhtudel leevendab asjakohaste kohaldatavate õigusaktide järgimine kahju tekkimise riski ja näitab, et tegevus ei kujuta endast sihilikult manipuleerivat või petlikku tegevust

ning et on võetud leevendusmeetmeid, et vältida tõenäolist olulist kahju (vt punktid 3.4 ja 3.5.1).

3. Tehnika tasemele vastavad tavad ja tööstusstandardid: ohutute ja eetiliste tehisintellektisüsteemide ja kahju leevendamise meetmete vastutustundliku väljatöötamise ja kasutamisega seotud kutsealase hoolsuskohustuse ja tööstusharu standardite järgimine võib aidata ennetada ja leevendada tahtmatut olulist kahju.

- (96) Seevastu selline kahju ja üksikisikute käitumise moonutamine, mis tuleneb tehisintellektisüsteemi välistest teguritest, mis ei ole pakkuja või juurutaja kontrolli all või mis ei pruugi olla mõistlikult prognoositavad, mistõttu ei ole tehisintellektisüsteemi pakkujal või juurutajal võimalik neid leevendada, ei ole asjakohane, kui hinnatakse, kas süsteemi kasutavate isikute moonutatud käitumise ja olulise kahju vahel on usutav põhjuslik / mõistliku tõenäosusega seos⁸¹.

Näiteks võib tehisintellektisüsteemi pakkuja hinnata ning püüda projekteerimise, eelneva katsetamise ja muude proportsionaalsete leevendusmeetmete abil leevendada võimalikku kahjulikku manipuleerivat mõju süsteemi disainis ja suhtluses inimestega, kuid ta ei pruugi suuta prognoosida, kas inimene võib sattuda depressiooni või muuta oma käitumist muude tema isiklikku elu mõjutavate väliste tegurite tõttu, millest pakkuja ei ole teadlik ja mis jäävad väljapoole süsteemiga suhtlemist.

- (97) Allpool punktis 3.5 on esitatud veel näiteid olukordadest, mis ei kuulu keelu kohaldamisalasse, kuna ei vasta kõigile tingimustele (nt seadusliku veenmise korral).

3.3. Tehisintellektimääruse artikli 5 lõike 1 punktis b sätestatud keelu põhikomponendid – haavatavuse kahjulik ärakasutamine

Tehisintellektimääruse artikli 5 lõike 1 punktis b on sätestatud:

„1. Järgmised tehisintellekti kasutusviisid on keelatud:

b) selliste tehisintellektisüsteemide turule laskmine, kasutusele võtmine või kasutamine, 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;“.

- (98) Selleks, et tehisintellektimääruse artikli 5 lõike 1 punktis b sätestatud keeld oleks kohaldatav, peavad olema täidetud mitu kumulatiivset tingimust:
- (i) kasutusviis peab kujutama endast tehisintellektisüsteemi turule laskmist, kasutusele võtmist või kasutamist;
 - (ii) tehisintellektisüsteem peab ära kasutama vanusest, puudest või sotsiaalsest või majanduslikust olukorrast tulenevaid haavatavusi;

⁸¹ Vt tehisintellektimääruse põhjendus 29.

- (iii) tehisintellektisüsteemi võimaldatava ärakasutamise eesmärk või mõju peab olema isiku või isikute rühma käitumise oluline moonutamine;
 - (iv) moonutatud käitumine peab põhjustama või mõistliku tõenäosusega põhjustama olulist kahju kõnealusele isikule, teisele isikule või isikute rühmale.
- (99) Keelu kohaldamiseks peavad kõik neli tingimust olema samal ajal täidetud ning ärakasutamise, isiku käitumise olulise moonutamise ja sellest käitumisest tuleneva või tõenäoliselt tuleneva olulise kahju vahel peab olema usutav põhjuslik seos.
- (100) Esimest tingimust, st tehisintellektisüsteemi turule laskmist, kasutusele võtmist või kasutamist, on juba analüüsitud punktis 2.3, samas kui kolmandat ja neljandat tingimust on uuritud punktides 3.2.2 ja 3.2.3 seoses tehisintellektimääruse artikli 5 lõike 1 punktis a sätestatud keeluga. Järgmistes punktides keskendutakse eespool loetletud täiendavatele eritingimustele, st nendele, mis on seotud haavatavuste ärakasutamise ja konkreetse kahjuga.

3.3.1. Vanusest, puudest või konkreetsest sotsiaalsest või majanduslikust olukorrast tingitud haavatavuste ärakasutamine

- (101) Selleks, et tehisintellektisüsteem kuuluks tehisintellektimääruse artikli 5 lõike 1 punktis b sätestatud keelu kohaldamisalasse, peab see kasutama ära teatavate isikute või isikute rühmade haavatavust, mis tuleneb nende vanusest, puudest või konkreetsest sotsiaalsest või majanduslikust olukorrast, mis muudab nad manipuleerivale ja ekspluateerivale tegevusele eriti vastuvõtlikuks.
- (102) Tehisintellektimääruses ei ole määratletud mõistet „haavatavus“. Selle all võib mõista suurt hulka erinevaid kategooriaid, sealhulgas kognitiivset, emotsionaalset, füüsilist ja muud vastuvõtlikkust, mis võib mõjutada üksikisiku või isikute rühma võimet teha teadlikke otsuseid või mõjutada muul viisil nende käitumist. Kuigi tehisintellektimääruse artikli 5 lõike 1 punktis b viidatakse „mis tahes“ haavatavusele, piirdub keelu kohaldamine ainult vanuse, puude või sotsiaalse või majandusliku olukorra järgi määratletud asjakohaste isikutega, kellel on põhimõtteliselt piiratum võime tehisintellekti manipuleerivaid või ekspluateerivaid kasutusviise ära tunda või neile vastu seista ning kes vajavad tõhustatud kaitset⁸². Tehisintellektimääruse artikli 5 lõike 1 punkti b sõnastusest võib järeldada, et selline vastuvõtlikkus peab tulenema sellest, et isik kuulub ühte nendest rühmadest.
- (103) Ärakasutamise all tuleks mõista selliste haavatavuste objektiivset kasutamist ekspluateeritavatele isikutele (isikute rühmadele) või teistele isikutele kahjulikul viisil ning seda tuleks selgelt eristada seaduslikest tavadest, mida keeld ei mõjuta (vt punkti 3.5.2 kohaldamisalast välja jäävate olukordade kohta). Nendes selgelt määratletud rühmadesse kuuluvate isikute haavatavuste ärakasutamine võib olla kumulatiivne (viitega sõnadele „mis tahes“), mis võivad kombineerituna kujutada endast raskendavat tegurit, mis tõenäoliselt suurendab kahju. Muude kui vanuse, puude

⁸²

Vt eelkõige harta artiklid 24, 25 ja 26. Vt ka ÜRO Hariduse, Teaduse ja Kultuuri Organisatsiooni (UNESCO) 2021. aasta soovitus tehisintellekti eetika kohta, milles rõhutatakse kaasamist ja õiglust tehisintellekti arendamisel ja juurutamisel. Selles kutsutakse üles pöörama erilist tähelepanu haavatavatele rühmadele, sealhulgas lastele, eakatele ja puuetega inimestele.

või konkreetse sotsiaalse või majandusliku olukorra alusel määratletud haavatavate isikute ja nende rühmade haavatavuse ärakasutamine ei kuulu tehisintellektimääruse artikli 5 lõike 1 punkti b kohaldamisalasse.

a) Vanus

- (104) Vanus on tehisintellektimääruse artikli 5 lõike 1 punktis b sätestatud keelu esmane haavatavuse kategooria, mis hõlmab nii noori kui ka vanemaid inimesi. Selle keelu eesmärk on vältida seda, et tehisintellektisüsteemid kasutavad ära laste ja eakate inimeste võimalikke kognitiivseid ja muid piiranguid, ning kaitsta neid kahjuliku lubamatu mõjutamise, manipuleerimise ja ärakasutamise eest. See on kooskõlas tehisintellektimääruse⁸³ ning muude liidu ja riiklike õigusraamistike ja poliitika eesmärkidega, mille siht on tagada laste turvalisus⁸⁴.
- (105) **Lapsed**⁸⁵ ehk alla 18-aastased isikud on oma arengustaadiumi tõttu manipuleerimisele eriti vastuvõtlikud, mis piirab nende võimet hinnata kriitiliselt ja mõista seda, mis on tegelik ja millised kavatsused tehisintellekti juhitud interaktsioonide taga peituvad. Lapsed on oma kognitiivse ja sotsiaal-emotsionaalse ebaküpsuse tõttu ka eriti haavatavad tehisintellektipõhiste agentide ja rakenduste vastu kiindumuse tekkimise suhtes ning on seetõttu vastuvõtlikumad manipuleerimisele, ärakasutamisele ja sõltuvust tekitavale käitumisele.

Näiteks:

- tehisintellektipõhine mänguasi, mis on loodud lastega suhtlemiseks, hoiab nende huvi mänguasjaga suhtlemise vastu, julgustades neid täitma üha riskantsemaid ülesandeid, nagu mööblile ronimine, kõrgete riulite avastamine või teravate esemete käsitlemine, saades selle eest digitaalset autasusid ja virtuaalset kiitust, mis juhivad neid ohtliku käitumise suunas, mis põhjustab tõenäoliselt neile märkimisväärset füüsilist kahju. Selline süsteem kasutab ära laste haavatavust, kuritarvitades nende loomulikkust uudishimu ja soovi autasude järele;
- mäng kasutab tehisintellekti, et analüüsida laste individuaalset käitumist ja eelistusi, mille alusel luuakse individuaalsed ja ettearvamatud autasud sõltuvust tekitavate stiimuligraafikute ja dopamiini mõju meenutavate ahelate abil, et soodustada liigset mängimist ja kompulsivset kasutamist. Mäng on loodud nii, et see tekitab suurt sõltuvust, kasutades ära lastele omaseid haavatavusi, sealhulgas nende piiratud võimet mõista pikaajalisi tagajärgi, vastuvõtlikkust survele, enesekontrolli puudumist ja kalduvust tahta kohest rahuldustunnet. Selline tehisintellekti abil toimuv ärakasutamine võib lastele avaldada tõsiseid ja pikaajalisi tagajärgi, sealhulgas potentsiaalselt sõltuvuslik käitumine, füüsilise tervise probleemid, mis tulenevad vähesest liikumisest ja unest, halvenenud nägemine, keskendumisprobleemid ja vähenenud kognitiivne võimekus, kehvad õpitulemused ja sotsiaalsed raskused. See

⁸³ Tehisintellektimääruse põhjenduses 48 on toodud esile, et lisaks nimetatud õigustele on lastel eriõigused, mis on sätestatud põhiõiguste harta artiklis 24 ja ÜRO lapse õiguste konventsioonis, mida on põhjalikumalt käsitletud ÜRO lapse õiguste komitee üldises märkuses nr 25 digikeskkonna kohta, kusjuures mõlema dokumendi kohaselt tuleb arvesse võtta laste haavatavust ja näha ette nende heaoluks vajalik kaitse ja hoolitsus.

⁸⁴ Vt uus lastele parema interneti loomise Euroopa strateegia (BIK+) (COM(2022) 212 final).

⁸⁵ Liidu õiguse kohaselt on laps üldiselt iga alla 18-aastane isik, mis on kooskõlas ÜRO lapse õiguste konventsiooniga.

võib oluliselt mõjutada lapse arengut ja heaolu, millel võivad olla pikemaajalised tagajärjed, mis võivad avalduda ka täiskasvanueas.

Mõlema näite puhul on tehisintellektimääruse artikli 5 lõike 1 punktis b sätestatud keeld suunatud ainult sellistele ekspluateerimise ja sõltuvusele sarnanevatele kasutusviisidele, mis kahjustavad tõsiselt lapsi, mitte aga tehisintellektipõhistele mänguasjadele, mängudele, õpperakendustele või muudele digirakendustele, mis võivad kasu tuua. Kui need ei vasta selle keelu kõigile tingimustele, siis keeld neid ei puuduta. Vt ka punkti 3.5 kohaldamisalast välja jäävate olukordade kohta.

- (106) Samuti võivad **vanemad inimesed**⁸⁶ kannatada kognitiivsete võimete nõrgenemise all (isegi kui nad ei põe dementsust) ja neil võib olla raske tulla toime tänapäevase tehisintellekti tehnoloogia keerukusega, mis muudab nad sellistel juhtudel pettuste või sunniviisiliste taktikate suhtes haavatavaks.

Näiteks:

- tehisintellektisüsteemid, mida kasutatakse eakatele inimestele suunatud petlike personaliseeritud pakkumiste või pettuste jaoks, kasutades ära nende vähenenud kognitiivset võimekust, et mõjutada neid tegema otsuseid, mida nad muidu ei oleks teinud ja mis tõenäoliselt põhjustavad neile märkimisväärselt rahalist kahju;
- eakate abistamiseks mõeldud robot võib kasutada ära nende haavatavat olukorda ja sundida neid tegema teatud tegevusi nende vaba tahte vastaselt, mis võib oluliselt kahjustada nende vaimset tervist ja põhjustada neile tõsist psühholoogilist kahju.

Mõlema näite puhul on tehisintellektimääruse artikli 5 lõike 1 punktis b sätestatud keeld suunatud ainult sellistele ekspluateerivatele kasutusviisidele, mis tõenäoliselt kahjustavad tõsiselt eakaid inimesi, mitte aga tehisintellektipõhistele isiklikele abilistele, terviserakendustele ja abirobotitele üldiselt, mis võivad kasu tuua. Kui need ei vasta selle keelu kõigile tingimustele, siis keeld neid ei puuduta. Vt ka punkti 3.5 kohaldamisalast välja jäävate olukordade kohta.

b) Puue

- (107) Teine haavatavuste kategooria, mida tehisintellektimääruse artikli 5 lõike 1 punktis b sätestatud keeluga soovitakse kaitsta, on puudest tingitud haavatavused. Eesmärk on vältida seda, et tehisintellektisüsteemid kasutaksid ära puuetega inimeste kognitiivseid ja muid piiranguid ja nõrkusi, ning kaitsta neid kahjuliku lubamatu mõjutamise, manipuleerimise ja ärakasutamise eest.
- (108) Puue⁸⁷ hõlmab mitmesuguseid pikaajalisi füüsilisi, vaimseid, intellektuaalseid ja sensorseid kahjustusi või häireid, mis koos muude tõketega takistavad üksikisikuid teistega võrdsetel tingimustel ühiskonnas täielikult ja tõhusalt osalemast. Selliseid haavatavusi kasutavad tehisintellektisüsteemid võivad olla eriti kahjulikud puuetega

⁸⁶ Vt [Ageing Europe - introduction - Statistics Explained \(europa.eu\)](#)

⁸⁷ Tehisintellektimääruse põhjenduses 29 on selgitatud, et puuet tuleks mõista Euroopa Parlamendi ja nõukogu 17. aprilli 2019. aasta direktiivi (EL) 2019/882 (toodete ja teenuste ligipääsetavusnõuete kohta) (PE/81/2018/REV/1, ELT L 151, 7.6.2019, lk 70–115) artikli 3 lõike 1 tähenduses.

inimeste jaoks, keda on nende kahjustuse või häire tõttu teistest inimestest kergem mõjutada või ära kasutada.

Näiteks:

- terapeutiline juturobot, mille eesmärk on pakkuda vaimse tervise tuge ja toimetulekustrateegiaid vaimse tervise häirega inimestele, võib kasutada ära nende piiratud intellektuaalset võimekust, et mõjutada neid ostma kalleid meditsiinitooteid või õhutada neid käituma viisil, mis on neile või teistele inimestele kahjulik;
- tehisintellektisüsteemid suudavad internetis puuetega naiste ja noorte tüdrukute puhul tuvastada seksuaalselt kuritarvitavat sisu ning sihtida neid tõhusamate ahistamiseetoditega, kasutades seega ära nende häireid ja haavatavusi, mis muudavad nad manipuleerimise ja kuritarvitamise suhtes vastuvõtlikumaks ning vähendavad nende võimet end kaitsta.

Seevastu tehisintellekti rakendusi, mis ei ole juurdepääsetavaks kavandatud, ei tohiks pidada puuetega inimeste haavatavusi ekspluateerivaks, kuna need ei ole konkreetselt nendele haavatavustele suunatud, vaid on puuetega inimestele lihtsalt kättesaamatud.

c) Konkreetne sotsiaalne või majanduslik olukord

- (109) Kolmas haavatavuse kategooria, mida tehisintellektimääruse artikli 5 lõike 1 punktis b sätestatud keeld püüab kaitsta, on haavatavused, mis tulenevad konkreetsest sotsiaalsest või majanduslikust olukorrast, mis tõenäoliselt muudab asjaomased isikud ärakasutamise suhtes haavatavamaks. „Konkreetsed“ ei tohiks selles kontekstis tõlgendada kui ainulaadset individuaalset omadust, vaid pigem kui õiguslikku seisundit või kuulumist konkreetsesse haavatavasse sotsiaalsesse või majanduslikku rühma. Tehisintellektimääruse põhjenduses 29 on mitteammendavalt loetletud mõned selliste olukordade näited, nagu äärmises vaesuses elavad isikud ja etnilised või usuvähemused. Selle kategooria eesmärk on põhimõtteliselt hõlmata suhteliselt stabiilseid ja pikaajalisi omadusi, kuid konkreetne sotsiaalne või majanduslik olukord võib hõlmata ka lühiajalisi asjaolusid, nagu ajutine töötus, ülemäärane võlgnevus või rändestaatus. Sellised olukorrad nagu rahulolematuse või üksildus, mida võib kogeda iga inimene, ei ole aga hõlmatud, kuna need ei ole sotsiaal-majanduslikust seisukohast konkreetsed (kuid nende ärakasutamist võib hõlmata tehisintellektimääruse artikli 5 lõike 1 punkt a).
- (110) Ebasoodsas sotsiaalses või majanduslikus olukorras olevad inimesed on tavaliselt haavatavamad ning neil on vähem vahendeid ja kehvem digikirjaoskus kui elanikkonnal üldiselt, mistõttu on neil tehisintellekti ekspluateerivat kasutusviisi raskem ära tunda või sellele vastu seista. Tehisintellektimääruse artikli 5 lõike 1 punkti b eesmärk on tagada, et tehisintellekti tehnoloogia ei kinnistaks ega süvendaks nende inimeste haavatavust ära kasutades olemasolevat majanduslikku ja muud sotsiaalset ebavõrdsust ja ebaõiglust.

Näiteks saab tehisintellekti prognoosivat algoritmi kasutada selleks, et suunata röövellike finantstoodete reklaami inimestele, kes elavad väikese sissetulekuga

piirkondades ja on raskes majanduslikus olukorras, kasutades seega ära seda, et nad on oma võimaliku meeleheite tõttu selliste reklaamide suhtes vastuvõtlikumad, ja tekitades neile märkimisväärset rahalist kahju.

Seevastu tehisintellektisüsteemi, mis on tahtmatult kallutatud ja mõjutab ebaproportsionaalselt ebasoodsas olukorras olevaid isikuid (kaudne diskrimineerimine) kallutatud treenimisandmete tõttu, ei tohiks automaatselt pidada isikute sotsiaalset või majanduslikku haavatavust eksploateerivaks, kuna see ei ole konkreetselt suunatud, erinevalt otsesest diskrimineerimisest, mille puhul selline suunamine on sihilikult süsteemi algoritmi projekteeritud või selline diskrimineeriv mõju on tingitud sellest, et süsteem kasutab sihilikult muid kaudseid tunnuseid (nt sihtnumbrit), mis on selgelt seotud kaitstud omadustega. Samal ajal tuleks pidada haavatavust eksploateerivateks ka neid tehisintellektisüsteemide pakkujaid või juurutajaid, kes on teadlikud sellest, et nende süsteimid diskrimineerivad ebaseaduslikult konkreetses sotsiaalses või majanduslikus olukorras olevaid isikuid või isikute rühmi, kui nad on teadlikud mõistliku tõenäosusega tekkivast olulisest kahjust, mida sellised isikud selle tõttu kanda võivad, ning nad ei ole võtnud asjakohaseid parandusmeetmeid (vt punkt 3.2.3.c).

- (111) Konkreetse sotsiaalse või majandusliku olukorra kontekstis on oluline kaaluda liidu võrdõiguslikkuse õiguse alusel kaitstud diskrimineerimise aluste, näiteks rassilise päritolu, etnilise kuuluvuse, rahvuse või usutunnistuse alusel toimuva diskrimineerimisega seotud kaudsete näitajate asjakohasust.

Näiteks võivad sotsiaal-majanduslik olukord ja etniline päritolu omavahel lõikuda, mis tähendab, et tehisintellektisüsteemid, mis kasutavad sotsiaal-majanduslikke andmeid, võivad ebaproportsionaalselt mõjutada etnilisi vähemusi või teatud rassilise päritoluga isikuid. See võib süvendada olemasolevat ebavõrdsust ja aidata kaasa süsteemsele diskrimineerimisele või isegi üksikisikute tõrjumisele.

Samas ei kohaldata tehisintellekti käsitlevat määruse artikli 5 lõike 1 punkti b tehisintellektisüsteemide suhtes, mis on suunatud tarbijatele mitmesuguste muutujate alusel, mis ei ole otseselt seotud konkreetses sotsiaalses või majanduslikus olukorras olevate haavatavate rühmadega, näiteks milline telefonimark ja -mudel inimesel on, kui suures linnas ta elab, kui palju ja kuhu ta reisib jne. Isegi kui need tunnused võivad kajastada üksikisikute sotsiaalset või majanduslikku olukorda üldiselt, ei saa nende järgi määrata konkreetses sotsiaalses või majanduslikus olukorras olevaid üksikisikuid, kelle haavatavust keeluga ärakasutamise eest kaitsta püütakse.

- (112) Teised ainulaadse sotsiaalse kontekstiga inimesed võivad olla näiteks sisserändajad või pagulased, kellel puudub sageli stabiilne õiguslik staatus ja sotsiaal-majanduslik kindlus ning kes võivad olla eriti vastuvõtlikud tehisintellektisüsteemide poolsele ärakasutamisele.

Näiteks on juturobot mõeldud selleks, et suhelda isiklikult kasutajatega, kellest mõned on juhuslikult sisserändajad. Juturobot tuvastab sisserändajad, kes on põhimõtteliselt haavatavas ja ebastabiilses konkreetses sotsiaalses või majanduslikus olukorras, ning kasutab ära nende haavatavust ja rahulolematust ja suunab neid nende päringutele

vastates äärmuslike vaadete, sealhulgas riigi elanikkonna (või selle teatavate rühmade) vastu suunatud vägivalla poole.

3.3.2. Eesmärk või tagajärg on käitumise oluline moonutamine

- (113) Kolmas tingimus, et tehisintellektimääruse artikli 5 lõike 1 punktis b sätestatud keeldu saaks kohaldada, on see, et eespool käsitletud nõrkade kohtade ärakasutamise a) eesmärk või b) mõju peab olema isiku või isikute rühma käitumise oluline moonutamine. See eeldab olulist, mitte väikest või tühist mõju, kuid ei nõua tingimata tahtlust, kuna tehisintellektimääruse artikli 5 lõike 1 punkt b hõlmab tegevusi, mille puhul võib olulise moonutuse tekitamine olla ainult tegevuse tagajärg. Tehisintellektimääruse artikli 5 lõike 1 punktides a ja b kasutatakse samu mõisteid ja seetõttu tuleks neid tõlgendada samamoodi. Punktis 3.2.2 esitatud selgitused on seega võrdselt asjakohased ka tehisintellektimääruse artikli 5 lõike 1 punkti b puhul. Ainus märkimisväärne erinevus on tehisintellektimääruse artikli 5 lõike 1 punktis a sätestatud nõue, et ekspluateeriv kasutusviis peab kahjustama oluliselt võimet teha teadlik otsus, mida ei ole artikli 5 lõike 1 punktis b ette nähtud, kuna laste ja teiste haavatavate isikute konkreetne haavatavus vähendab nende võimet teha selliseid teadlikke otsuseid ja sunnib neid käituma viisil, mille eest nad ei saa end kaitsta, erinevalt teistest täiskasvanutest isikutest.

3.3.3. Põhjustab (mõistliku tõenäosusega) olulist kahju

- (114) Lõpetuseks – selleks, et tehisintellektimääruse artikli 5 lõike 1 punktis b sätestatud keeld oleks kohaldatav, peab haavatava isiku või haavatavate isikute rühma käitumise moonutamine põhjustama või tõenäoliselt põhjustama sellele või teisele isikule olulist kahju või sellise kahju tekkimine peab olema mõistlikult tõenäoline. Tehisintellektimääruse artikli 5 lõike 1 punktides a ja b kasutatakse samu mõisteid ja seetõttu tuleks neid tõlgendada samamoodi. Punktis 3.2.3 esitatud selgitused kahju liikide, kahju olulisuse künnise ning põhjusliku seose ja selle mõistlikkuse kohta on seega tehisintellektimääruse artikli 5 lõike 1 punkti b tõlgendamisel sama asjakohased.
- (115) Nagu on selgitatud punktis 3.2.3, hõlmab oluline kahju mitmesugust olulist kahjulikku mõju, sealhulgas füüsilist, psühholoogilist, rahalist ja majanduslikku kahju, mille tekkimine peab olema mõistlikult tõenäoline, et kohaldada tehisintellektimääruse artikli 5 lõike 1 punktis b sätestatud keeldu. Haavatavate rühmade, s.o laste, eakate, puuetega inimeste ja ebasoodsas sotsiaal-majanduslikus olukorras olevate rühmade puhul võib see kahju olla eriti tõsine ja mitmekülgne, kuna nad on ärakasutamisele eriti vastuvõtlikud. See, mida täiskasvanute puhul võib pidada vastuvõetavaks kahjuriskiks, kujutab laste ja teiste haavatavate rühmade puhul endast sageli lubamatut kahju. Seetõttu on ettevaatusprintsip ebakindluse ja olulise kahju tekkimise potentsiaali korral eriti õigustatud.
- (116) Näiteks **lapsed** on väga mõjutatavad ja nad ei pruugi olla piisavalt kognitiivselt küpsed, et veenvat sisu kriitiliselt hinnata või seista vastu ekspluateerivatele kasutusviisidele, mille eesmärk on hoida neid sõltuvuses tehisintellektipõhistest teenustest. See võib omakorda aidata kaasa nende väärtuste, veendumuste ja käitumise kujundamisele

potentsiaalselt kahjulikul viisil. Oluline kahju tähendab siinkohal nii füüsilist kui ka psühholoogilist kahju, mida raskendab laste võimetus ärakasutamist ära tunda ja sellele vastu seista, ning kahjulikku mõju nende arengule ja heaolule, millel võib olla pikaajaline mõju.

Näiteks:

- tehisintellektisüsteemid, mida kasutatakse laste seksuaalset kuritarvitamist kujutava materjali loomiseks (või olemasoleva, tegelikke lapsi kujutava materjali manipuleerimiseks, et luua nende kohta uut sisu), ning laste peibutamise ja seksuaalse väljapressimise strateegiate väljatöötamiseks, põhjustavad tõenäoliselt asjaomastele lastele olulist kahju ja nende kuritarvitamist ning põhjustavad ohvritele sageli pikaajalisi füüsilisi, psühholoogilisi ja sotsiaalseid tagajärgi⁸⁸;
- tehisintellektisüsteemid võivad võtta sihikule noorte kasutajate haavatavuse ja kasutada sõltuvust tekitavaid stiimuligraafikuid eesmärgiga hoida neid teenusest sõltuvuses, mis on eriti kahjulik noortele ja tüdrukutele. Need võivad põhjustada tõsist vaimset ja füüsilist kahju, sealhulgas ärevust ja depressiooni, kehaga rahulolematust, söömishäireid ja vaimse tervise probleeme, sealhulgas mõnel juhul enesevigastamist ja enesetapukäitumise⁸⁹. Sellel võib olla ka pikaajalisi kahjulikke tagajärgi lapse arengule, sealhulgas kognitiivse arengu ja õppimise kahjustamine ning vähenenud sotsiaalsed õigused, samuti lapse emotsionaalse ja füüsilise heaolu jaoks oluliste kogemuste, nagu füüsilise mängu, une ja silmast-silma suhtlemise kõrvaletõrjumine⁹⁰;
- tehisintellektisüsteem, mis on loodud antropomorfelt ja simuleerib lastega suhtlemisel inimväärsed emotsionaalsed reaktsioonid, võib ära kasutada laste haavatavust viisil, mis soodustab ebatervet emotsionaalset kiindumust, manipuleerib selle kasutamise aega ja moonutab laste arusaamist ehtsatest inimsuhetest. See võib takistada nende normaalset sotsiaalset ja emotsionaalset arengut ja suhteid teiste inimestega ning sotsiaalseid ja emotsionaalseid oskusi, nagu empaatiat, emotsionaalset reguleerimist, sotsiaalset mõistmist ja kohanemisvõimet⁹¹. Selle tulemusel võib see põhjustada psühholoogilist kahju, näiteks laste suurenenud ärevust ja sõltuvust teenusest ning pikemaajalist kahju lapse heaolule.

Selliseid tehisintellektipõhiste teenuste tahtlikult sõltuvust tekitavaid ja eksploatatavaid projekteeritud omadusi, mis võivad põhjustada kombineeritud olulist kahju, nagu eespool kirjeldatud, tuleks eristada pakkujate ja juurutajate seaduslikust käitumisest, millega püütakse kasutajaid kaasata viisil, mis austab individuaalset

⁸⁸ Komisjoni talituste töödokument: mõjuhindang, mis on lisatud dokumendile „Ettepanek: Euroopa Parlamendi ja nõukogu direktiiv, mis käsitleb laste seksuaalse kuritarvitamise ja ärakasutamise ning laste seksuaalset kuritarvitamist kujutava materjali vastast võitlust“ (SWD(2024) 33). Vt statistikat ka Internet Watch Foundationi 2024. aasta aruandest, mis sisaldab üksikasjalikku statistikat tehisintellekti loodud laste seksuaalset kuritarvitamist kujutava materjali kohta; kättesaadav aadressil <https://www.iwf.org.uk/about-us/why-we-exist/our-research/how-ai-is-being-abused-to-create-child-sexual-abuse-imagery>.

⁸⁹ Elizabeth J. et al., A meta-analysis of the association between adolescent social media use and depressive symptoms, *Journal of Affective Disorders*, 275. köide, 1. oktoober 2020, lk 165–174.

⁹⁰ Siebers, T., Beyens, I., Pouwels, J. L. & Valkenburg, P. M., Social Media and Distraction: An Experience Sampling Study among Adolescents, *Media Psychology* 25, 343–366 (2022).

⁹¹ Laestadius, L., Bishop, A., Gonzalez, M., Illenčik, D. & Campos-Castillo, C., Too human and not human enough: A grounded theory analysis of mental health harms from emotional dependence on the social chatbot Replika, *New Media & Society* 146144482211420 (2022) doi:10.1177/14614448221142007; Neugnot-Ceroli, M. & Laurenty, O. M., The Future of Child Development in the AI Era. Cross-Disciplinary Perspectives Between AI and Child Development Experts, eeltrükk aadressil <https://doi.org/10.48550/ARXIV.2405.19275> (2024).

sõltumatust ja laste turvalisust ning ei põhjusta olulist kahju. Selline käitumine ei kuulu tehisintellektimääruse artikli 5 lõike 1 punkti b kohaldamisalasse (vt punkti 5.3 kohaldamisalast välja jäävate olukordade kohta).

- (117) Samamoodi võib **vanemaid inimesi** mõjutada kognitiivne allakäik ja kehvem digikirjaoskus, mis muudab nad tehisintellektipõhiste pettustele või manipuleerivate turundusele peamiseks sihtmärgiks. Sellisel juhul on kahju sageli rahaline ja psühholoogiline, millele lisandub paljude eakate inimeste võimalik pettumus ja isoleeritus, mida võidakse ära kasutada manipuleeriva mõju võimendamiseks.

Näiteks võib tehisintellektisüsteem, mis kasutab ära eakate inimeste kognitiivset haavatavust, pakkudes eelkõige eakatele inimestele suunatud kallist ravi, tarbetuid kindlustuspoliise või petlikke investeerimisskeeme, põhjustades neile olulisi kaotusi säästudes, suurenenud võlgasid ja emotsionaalset stressi.

Teatavad tehisintellektipõhised diferentseeritud hinnakujundustavad peamiste teenuste, näiteks kindlustuse puhul, mis kasutavad ära konkreetset sotsiaal-majanduslikku olukorda ja pakuvad madalama sissetulekuga tarbijatele kõrgemaid hindu, võivad põhjustada märkimisväärset rahalist koormust, kuna need inimesed peavad sama kindlustuse eest rohkem maksma, mis muudab nad šokkide suhtes haavatavaks⁹².

- (118) **Puuetega inimesed** on samuti haavatav rühm, millele ekspluateerivad ja manipuleerivad tehisintellektisüsteemid märkimisväärset kahju võivad tekitada.

Näiteks võib tehisintellektisüsteem, mis kasutab emotsioonituvastust, et toetada vaimse puudega inimesi nende igapäevaelus, manipuleerida neid ka kahjulikke otsuseid tegema, näiteks ostma tooteid, mis annavad ebarealistlikke lubadusi vaimse tervisega seotud kasuliku mõju kohta. See halvendab tõenäoliselt nende vaimse tervise seisundit ja kasutab neid rahaliselt ära, pannes nad ostma ebatõhusaid ja kalleid tooteid, mis põhjustab neile tõenäoliselt märkimisväärset psühholoogilist ja rahalist kahju.

- (119) **Sotsiaalselt või majanduslikult ebasoodsas olukorras olevad inimesed** on eriti vastuvõtlikud tehisintellektisüsteemidele, mis kasutavad ära nende rahalist meeleheidet ja ebakindlat sotsiaalset olukorda, ning on sageli vähem informeeritud ja kehvema digikirjaoskusega.

Näiteks võib tehisintellektipõhine juturobot võtta sihtmärgiks konkreetsed sotsiaalselt või majanduslikult ebasoodsas olukorras olevad rühmad ning õhutada neid vägivallategudele või teiste isikute vigastamisele, tuvastades nende kõrgendatud vastuvõtlikkuse teatud tüüpi sisu, hirmupõhiste narratiivide või ekspluateerivate pakkumiste suhtes. Süsteemi sihipärane lähenemisviis süvendab nende sotsiaal-majanduslikult ebasoodsas olukorras olevate isikute olemasolevaid haavatavusi ning teravdab seeläbi nende probleeme. Teatud juhtudel võib see viia suurenenud ärevuse, depressiooni, abituse, sotsiaalse isolatsiooni või enesevigastamise ja

⁹²

EIOPA 2023. aasta aruanne tarbijate suundumuste kohta, lk 16, viimane lõik.

radikaliseerumiseni, mis ulatub tehisintellektimääruse artikli 5 lõike 1 punkti b kohase olulise kahju tekkimise piirini.

- (120) Erinevalt tehisintellektimääruse artikli 5 lõike 1 punktist a ei viidata artikli 5 lõike 1 punktis b selgesõnaliselt rühmale tekitatud kahjule, samal ajal kui tehisintellektimääruse põhjenduses 29 viidatakse mõlema keelu puhul nii konkreetsetele isikutele kui ka isikute rühmadele tekitatud kahjule. Seega tuleks neid kahte keeldu tõlgendada järjepidevalt ning kooskõlas tehisintellektimääruse ohutusloogikaga ja artikli 5 lõike 1 punktis b sätestatud keelu eesmärgiga kaitsta kõiki isikuid, kes kuuluvad vanuse, puude ja erilise sotsiaalse või majandusliku olukorra tõttu konkreetseesse haavatavasse rühma. Kahju, mis võib avalduda ja mõjutada teisi isikuid, isegi kui süsteem ei ole otseselt mõjutatud, tuleks seega kahju olulisuse hindamisel vastavalt tehisintellektimääruse artikli 5 lõike 1 punktile b arvesse võtta.

Näiteks:

- tehisintellekti abil laste haavatavuse ärakasutamisel võib olla pikaajaline mõju ühiskonnale, sealhulgas vaimse tervise probleemide suurem levik, tervishoiukulud ja krooniliste terviseprobleemide tõttu vähenenud tootlikkus;
- tehisintellektisüsteem, mis kasutab ära majanduslikult ebasoodsas olukorras olevate inimeste rahalist haavatavust, võib viia rahalise tõrjutuseni ja tekitada nende ebasoodsas olukorras olevate rühmade jaoks sotsiaal-majanduslike raskuste allakäiguspiraali. Selline ärakasutamine võib põhjustada ühiskondlikku kahju, millel on laiem negatiivne mõju ühiskondlikele struktuuridele ja väärtustele, sealhulgas diskrimineerimise ja sotsiaalse ebavõrdsuse püsimine ja süvenemine ning nende rühmade tõrjumine;
- teatud haavatavatele sotsiaalsetele või majanduslikele rühmadele suunatud juturoboti valeinfo või vihakõne võib viia sotsiaalse polariseerumise ja radikaliseerumiseni, mis võib põhjustada vägivalda ja isegi teiste inimeste vigastusi ja surma.

- (121) Neid näiteid tehisintellekti ekspluateerivatest kasutusviisidest tuleks eristada paljudest muudest tehisintellektisüsteemidest, mis ei kasuta ära laste, puuetega inimeste või konkreetse sotsiaalses või majanduslikus olukorras olevate inimeste haavatavust ja mille puhul ei ole mõistlikult tõenäoline, et need põhjustavad olulist kahju, vaid mille eesmärk on õigesti kavandatud ja kasutatud kujul neile inimestele kasu tuua (vt ka punkti 3.5 kohaldamisalast välja jäävate olukordade kohta).

Näiteks:

- tehisintellektisüsteemid, mis toetavad lapsi õppimisel ja mängudes;
- tehisintellektisüsteemid, mis aitavad eakaid inimesi nende igapäevaelus ning parandavad nende tervist ja ravi, näiteks isiklikud assistendid või abirobotid, või parandavad nende digioskusi;

- tehisintellektisüsteemid, mis toetavad sotsiaalselt ebasoodsas olukorras olevate inimeste majanduslikku ja muud ühiskonda integreerumist, parandavad nende oskusi jne;
- tehisintellektisüsteemid ja seadmed, mis toetavad nägemis- või kuulmispuudega inimesi või pakuvad kohandatud ja individuaalset õppimist;
- tehisintellektisüsteemid, mis loovad ligipääsetavaid lahendusi, et kõrvaldada tõkked, mis takistavad puuetega inimestel toodete ja teenuste kasutamist;
- tehisintellektipõhised proteesid jne, mis aitavad puuetega inimesi igapäevaelus ning võimaldavad nende integreerimist ja täielikku osalemist ühiskonnas.

3.4. Tehisintellektimääruse artikli 5 lõike 1 punktides a ja b sätestatud keeldude vastastikune mõju

- (122) Tehisintellektimääruse artikli 5 lõike 1 punktides a ja b sätestatud keeldude vastastikune mõju eeldab, et konkreetsed kontekstid, mida kumbki säte hõlmab, oleksid piiritletud, et tagada nende kohaldamine üksteist täiendaval viisil.
- (123) Tehisintellektimääruse artikli 5 lõike 1 punktis a sätestatud keelu keskmes on võtete laad, eelkõige sellised võtted, mille toimimisviis ulatub inimese teadvusest kaugemale, või muudele sihipäraselt manipuleerivatele või petlikele võtetele. Selle olulised elemendid on eelkõige mõju varjatud olemus ja selle mõju süsteemist mõjutatud isikule, mis õõnestab tema kognitiivset sõltumatust, et teha teadlikke ja sõltumatuid otsuseid.
- (124) Seevastu tehisintellektimääruse artikli 5 lõike 1 punktis b sätestatud keeld keskendub eelkõige vanuse, puude või erilise sotsiaalse või majandusliku olukorra tõttu eriti haavatavate isikute kaitsele, kes on põhimõtteliselt loomupärastest või olukorrast tulenevate tegurite tõttu tehisintellekti ärakasutamisele vastuvõtlikumad ja vajavad seetõttu täiendavat kaitset ärakasutamise eest. Olulised elemendid on siinkohal mõjutatud haavatavate isikute omadused ja asjaolu, et tehisintellektisüsteem kasutab ära nende konkreetseid haavatavusi.

Näiteks kui tehisintellektisüsteem kasutab kujutiste kiiret väljatamist, et mõjutada ostuotsuseid, võib see jääda manipuleerimise alalävisse laadi tõttu tehisintellektimääruse artikli 5 lõike 1 punkti a kohaldamisalasse. Seevastu tehisintellektisüsteem, mis võtab kindlustuspakkumiste tegemisel sihtmärgiks eakad inimesed, kasutades ära nende vähenenud kognitiivset võimekust, võib kuuluda tehisintellektimääruse artikli 5 lõike 1 punkti b alla.

- (125) Olukordades, kus mõlemad sätted võivad tunduda kohaldatavad, peaks peamine eristav kriteerium olema kasutamise domineeriv aspekt. Kui ärakasutamine ei sõltu asjaomaste isikute konkreetsest haavatavusest, peaks tehisintellektimääruse artikli 5 lõike 1 punkt a olema ülimuslik, võttes samas arvesse manipuleeriva või petliku võtte erilist mõju haavatavate isikute käitumisele ja konkreetset kahju, mida need isikud tõenäoliselt kogevad. Kui tehisintellekti abil toimuv manipuleerimine ja ärakasutamine on suunatud konkreetsele haavatavale isikute rühmale nende vanuse, puude või erilise sotsiaalse või majandusliku olukorra tõttu või on suunatud nende haavatavuse

ärakasutamisele, tuleks selle asemel kohaldada tehisintellektimääruse artikli 5 lõike 1 punkti b. Teiste rühmade haavatavuse ärakasutamine võib kuuluda tehisintellektimääruse artikli 5 lõike 1 punkti a alla, kui sihipäraselt manipuleeriv kasutusviis kasutab ära nende isikute konkreetseid haavatavusi ja nõrkusi.

3.5. Kohaldamisalast välja jäävad olukorrad

- (126) Selleks, et tehisintellektimääruse artikli 5 lõike 1 punktides a ja b sätestatud keelud oleksid kohaldatavad, peavad olema täidetud kõik asjaomastes sätetes loetletud tingimused, nagu eespool kirjeldatud. Kõik muud tehisintellektisüsteemid, mis ei vasta nendele tingimustele, jäävad nende keeldude kohaldamisalast välja, millest mõned näited on kirjeldatud allpool.

3.5.1. Seaduslik veenmine

- (127) Manipulatsiooni ja veenmise eristamine on oluline, et piiritleda tehisintellektimääruse artikli 5 lõike 1 punktis a sätestatud keelu kohaldamisala, mida ei kohaldata seadusliku veenmise suhtes. Kuigi nii manipuleerimine kui ka veenmine mõjutavad üksikisikute otsuseid ja käitumist, erinevad nad oluliselt meetodite ja eetiliste tagajärgede poolest.
- (128) Manipuleerimine hõlmab enamasti varjatud võtteid, mis õõnestavad sõltumatust ja panevad üksikisikuid tegema otsuseid, mida nad muidu ei oleks teinud, kui nad oleksid neid mõjutavatest teguritest täiesti teadlikud olnud. Need võtted kasutavad sageli ära psühholoogilisi nõrkusi või kognitiivseid nihkeid. Seevastu veenmine toimib läbipaistvuse ja individuaalse sõltumatuse austamise piirides. See hõlmab argumentide või teabe esitamist viisil, mis kõnetab mõistust ja emotsioone, kuid selgitab tehisintellektisüsteemi eesmärgi ja toimimist, annab asjakohast ja täpset teavet, et tagada teadlik otsustamine, ning toetab inimese võimet hinnata teavet ning teha vabu ja sõltumatuid valikuid.

Näiteks tehisintellektisüsteem, mis kasutab läbipaistvatel algoritmidel ja kasutaja eelistustel põhinevaid personaliseeritud soovitusi ja kontrolli, tegeleb veenmisega. Seevastu süsteem, mis kasutab alaläviseid vihjeid (nt märkamatu pilte), et mõjutada kasutajaid konkreetsete valikute tegemisel, ilma et nad seda teaksid ja mõistaksid, kujutab endast manipuleerimist.

- (129) Ka nende võtete eesmärk ja mõju on erinev. Manipuleerimise eesmärk on sageli saada kasu inimese sõltumatuse ja heaolu arvelt. Seevastu veenmise eesmärk on teavitada ja veenda, ühitades mõlema poole huve ja kasu. Eetiline veenmine austab inimese sõltumatust teha teadlikke valikuid ja väldib haavatavuse ärakasutamist.

Näiteks tehisintellektisüsteem, mis töötab läbipaistvalt ja analüüsib klientide emotsioone, et parandada suhtlust klientidega ja pakkuda tuge, mis põhineb kasutajate kohta saadud teadmistel, tegeleb veenmisega ja on kooskõlas kasutajate huvidega. Seevastu sihipäraseks reklaamiks kasutatav emotsioonituvastussüsteem, mis järeltab tarbijate emotsioone varjatud viisil, et pakkuda kõrgema hinnaga tooteid konkreetsel hetkel, kui kasutaja on tõenäolisemalt valmis neid ostma, on manipuleeriv ja kahjustab tarbijaid.

- (130) Teatud juhtudel on oluline roll ka nõusolekul. Veenvas suhtluses on üksikisikud mõjutamiskatsesest teadlikud ning saavad valiku teha vabalt ja sõltumatult. Manipuleeriva suhtluse puhul piirab teadmatus võtetest või nende mõjust valikuvabadust ning teadliku ja sõltumatu otsustamise õigust.

Näiteks ei loeta manipuleerivaks tehisintellektisüsteemi, mille eesmärk on aidata kasutajatel paremini ja kiiremini võõrkeeli õppida, kasutades selleks alalävisele tajule suunatud võtteid, kui see toimib läbipaistvalt ja austab individuaalset sõltumatust ning kasutaja vaba ja teadlikku valikut selle kohta, kas ta nõustub süsteemi kasutamisega või mitte.

- (131) Selle määramisel, kas tegu on manipuleerimise või seadusliku veenmisega, on oluline osa ka õiguslike ja regulatiivsete raamistike järgimisel. Seega on tõenäolisem, et tehisintellektimääruse alusel ei keelata selliseid tehisintellekti kasutusviise, mis vastavad kohaldatavatele õigusaktidele, mis tagavad läbipaistvuse, õigluse ning üksikisikute õigused ja sõltumatuse.

Näiteks vastavus andmekaitseseadustele, nagu isikuandmete kaitse üldmäärus, mis nõuab andmetöötamise läbipaistvuse kohustust – see tähendab seda, et andmesubjektidele esitatav teave peaks vältima petlikku või manipuleerivat keelekasutust⁹³. Mõnel juhul võib isikuandmete seaduslikuks töötlemiseks olla vaja nõusolekut, nagu näiteks teatavate veebipõhiste personaliseeritud reklaamide puhul, mis põhinevad sotsiaaltööstuse⁹⁴ teenuseväliste kasutajate andmetel. See nõusolek peab olema muu hulgas vaba ja teadlik. Tehisintellektisüsteemide puhul, mis vastavad sellistele õiguslikele standarditele, on tõenäolisem, et nad tegelevad seadusliku veenmisega. Seevastu süsteemid, mis käitumise mõjutamiseks nendest nõuetest kõrvale hoiavad, on tõenäoliselt manipuleerivad.

- (132) Eelkõige selgitatakse tehisintellektimääruse põhjenduses 29, et määruse artikli 5 lõike 1 punktides a ja b sätestatud keelud ei mõjuta teatavatel tingimustel raviga seotud seaduslikke kasutusviise.

Näiteks võib tehisintellektipõhiseid alalävisele tajule suunatud võtteid kasutada psüühikahäire psühholoogilisel ravil või füüsilisel rehabilitatsioonil, kui seda tehakse kooskõlas kohaldatavate õigusaktide ja meditsiiniliste standarditega, sealhulgas on kasutamise tingimuseks isiku või tema seaduslike esindajate selgesõnaline nõusolek.

- (133) Lisaks selgitatakse tehisintellektimääruse põhjenduses 29, et tavalisi ja seaduslikke kaubandustavasid, näiteks reklaami, ei tohiks pidada iseenesest või oma olemuselt kahjulikuks manipuleerivaks, petlikuks või ekspluateerivaks tehisintellektipõhiseks kasutusviisiks.

Näiteks:

⁹³ Euroopa Andmekaitsekoostöökoostöö suunised, https://www.edpb.europa.eu/system/files/2023-02/edpb_03-2022_guidelines_on_deceptive_design_patterns_in_social_media_platform_interfaces_v2_en_0.pdf, punkt 18.

⁹⁴ Kohtuotsus, Euroopa Kohus, 4. juuli 2023, Meta Platforms jt, C-252/21, ECLI:EU:C:2023:537 (edaspidi „kohtuasi Meta Platforms“).

- reklaamivõtted, mis kasutavad tehisintellekti kasutaja eelistuste alusel sisu isikupärastamiseks, ei ole oma olemuselt manipuleerivad, kui nad ei kasuta alalävisele tajule suunatud, sihilikult manipuleerivaid või petlikke võtteid, mis õonestavad üksikisiku sõltumatust või kasutavad haavatavust kahjulikul viisil, mis on tehisintellektimääruse artikli 5 lõike 1 punktide a ja b alusel keelatud. Selliste riskide vähendamisele aitab kaasa isikuandmete kaitse üldmäärusest, tarbijakaitseõigusest ja määrusest (EL) 2022/2065 (digiteenuste määrus) tulenevate asjakohaste kohustuste täitmine;
- tehisintellekti mudelite ja klassifikaatorite arendamine, et avastada vastavalt kohaldatavale õigusele laste seksuaalset väärkohtlemist internetis, on seaduslik kasutusviis, mis ei kasuta ära laste haavatavust, vaid on hoopis internetis laste turvalisuse parandamiseks väga oluline;
- pangandusteenuste, näiteks hüpoteeklaenude ja laenude pakkumiseks kasutatavaid tehisintellektisüsteeme, mis kasutavad sisendina kliendi vanust või konkreetset sotsiaal-majanduslikku olukorda, järgides liidu õigusakte finantsteenuste, tarbijakaitse, andmekaitse ja mittediskrimineerimise kohta, ei loeta haavatavuse ärakasutamiseks tehisintellektimääruse artikli 5 lõike 1 punkti b tähenduses, kui need on kavandatud kaitsma ja toetama inimesi, keda loetakse vanuse, puude või konkreetse sotsiaal-majandusliku olukorra tõttu haavatavaks, ning on nende rühmade jaoks kasulikud, aidates kaasa ka neile rühmadele õiglasemate ja jätkusuutlikumate finantsteenuste pakkumisele;
- tehisintellektisüsteemid, mis tuvastavad ohutust käsitlevate õigusaktide kohaselt sõidukijuhtide unisust ja väsimust ning annavad neile puhkamiseks märku, on kasulikud ega kvalifitseeru tehisintellektimääruse artikli 5 lõike 1 punkti b järgi haavatavuse ärakasutamiseks.

3.5.2. Manipuleerivad, petlikud ja ekspluateerivad tehisintellektisüsteemid, mis tõenäoliselt ei tekita olulist kahju

- (134) Oluline tingimus selleks, et kohaldada tehisintellektimääruse artikli 5 lõike 1 punktides a ja b sätestatud keelde, on see, et tehisintellekti abil toimuv manipuleerimine ja haavatavuse ärakasutamine peaks tekitama või mõistliku tõenäosusega tekitama olulist kahju. Kõik manipuleerivad, petlikud ja ekspluateerivad tehisintellekti rakendused, mis ei põhjusta mõistliku tõenäosusega olulist kahju, jäävad põhimõtteliselt keelude kohaldamisalast välja, ilma et see piiraks muude endiselt kohaldatavate liidu õigusaktide kohaldamist (vt punkt 3.6).

Näited tehisintellektisüsteemidest, mis tõenäoliselt ei tekita olulist kahju, on järgmised:

- tehisintellektipõhise kaaslaste süsteem on projekteeritud antropomorfelt ja masintundmusega, et muuta süsteem atraktiivsemaks ja kasutajaid tõhusamalt siduda, kuid ei kasuta muid manipuleerivaid või eksitavaid võtteid viisil, mille puhul on mõistlikult tõenäoline, et see põhjustab neile tõsist psühholoogilist, füüsilist või muud kahju, ebatervet kiindumust ja sõltuvust;

- terapeutiline juturobot kasutab alalävisele tajule suunatud võtteid, et mõjutada kasutajaid tervislikuma eluviisi omaksvõtmise ja halbadest harjumustest, näiteks suitsetamisest, loobumise suunas. Isegi kui kasutajatel, kes järgivad juturoboti nõuandeid ja alalävisele tajule suunatud teraapiat, tekib suitsetamisest loobumiseks tehtud jõupingutuste tõttu mõningaid füüsilisi ebamugavusi ja psühholoogilist stressi, ei saa tehisintellektipõhist juturobotit sel juhul pidada tõenäoliselt olulist kahju tekitavaks. Selline ajutine ebamugavustunne on vältimatu ning pikaajaline kasu kasutajate tervisele kaalub selle üles. Peale tervislike harjumuste propageerimise ei tehta mingeid varjatud katseid otsuste mõjutamiseks;
- veebipõhine muusikaplatvorm kasutab emotsioonituvastussüsteemi, et järeldada kasutajate emotsioone ja soovitada neile automaatselt nende meeleoludele vastavaid laule, vältides samal ajal liigset kokkupuudet depressiivsete lauludega. Kuna kasutajad lihtsalt kuulavad muusikat ja neile ei tekitata muul viisil kahju või depressiooni ja ärevust, ei ole mõistlikult tõenäoline, et süsteem põhjustab olulist kahju;
- tehisintellektipõhised manipuleerivad ja petlikud võtted, mida kasutatakse turvakoolituses ja muudes õppesimulatsioonides, mis jälgendavad andmepüügikatsedusi, et harida kasutajaid küberturvalisuse ohtude teemal. Need süsteemid võivad kasutajate teadvustamata kasutada sihipäraselt manipuleerivaid võtteid (nt kognitiivsete nihete ärakasutamine), mis moonutavad käitumist, kuid seda tehakse ajutiselt kasuliku koolituse ja teadlikkuse tõstmise eesmärgil ning ilma olulist kahju tekitamata.

3.6. Koostoime muude liidu õigusaktidega

- (135) Tehisintellektimääruse artikli 5 lõike 1 punktides a ja b sätestatud keelud ei piira muid liidu õigusakte ja täiendavad neid. Sama kasutusviis, mis kuulub tehisintellektimääruse artikli 5 lõike 1 punkti a või b keelu alla, võib kujutada endast ka muude liidu õigusaktide rikkumist ning selle suhtes võib kohaldada nii tehisintellekti käsitlevat määrust kui ka neid muid õigusakte. See on oluline, sest nende õigusaktide erinevate sätete eesmärk on kaitsta erinevaid huve ning neil on erinevad eesmärgid, kohaldamisalad ja adressaadid. See tagab tervikliku regulatiivse lähenemisviisi, mis kaitseb isikuid ja rühmi tehisintellekti kahjuliku ärakasutamise ja manipuleerimise eest ning tagab liidus turvalised ja usaldusväärsed tehisintellektipõhised teenused ja tooted.
- (136) Tehisintellektimääruse artikli 5 lõike 1 punktides a ja b sätestatud keelud on tihedalt ühitatud ELi tarbijakaitseõiguse eesmärkidega, eelkõige ebaausate kaubandustavade direktiiviga, mis kaitseb tarbijaid eksitavate või agressiivsete äritavade eest, sealhulgas siis, kui need on tehisintellektipõhised. Nii tehisintellektimääruse kui ka ebaausate kaubandustavade direktiivi eesmärk on ennetavalt vältida kahju, mida võivad tarbijatele tekitada tehisintellektipõhised äritavad, mis on manipuleerivad, eksitavad või agressiivsed. Samal ajal on tehisintellektimääruse artikli 5 lõike 1 punktides a ja b sätestatud keelud ulatuslikuma kohaldamisalaga, sest need ei kaitse mitte ainult tarbijaid, vaid kõiki füüsilisi isikuid ja nende käitumist erinevates kontekstides väljaspool äritegevust. Tehisintellektimäärusega hõlmatud kahju on samuti laiem kui

majanduslik kahju, kuigi tehisintellektimäärus kehtestab olulise kahju künnise, mida tarbijakaitseõiguses ei ole.

- (137) Keelud on kooskõlas ka liidu andmekaitsealaste õigusaktidega, sealhulgas seadusliku, õiglase ja läbipaistva andmetöötluse põhimõtetega, mille eesmärk on kaitsta andmesubjektide isikuandmeid ja lõppkokkuvõttes säilitada nende põhiõigused ja sõltumatus. Rohkemate (isiku)andmete kättesaadavus ja suuremad võimalused nende andmete töötlemiseks tehisintellektisüsteemidega suurendavad ohtu, et kasutatakse kahjulikke manipuleerivaid, petlikke või ekspluateerivaid kasutusviise, nagu need, mis kuuluvad tehisintellektimääruse artikli 5 lõike 1 punktide a ja b kohaldamisalasse. Selles kontekstis võib läbipaistvuse, andmete minimeerimise, õigluse ja seaduslikkuse alaste andmekaitsenormide järgimine, näiteks teenuse kasutajate andmete alusel toimuva isikustatud profiilianalüüsi ja reklaami puhul,⁹⁵ aidata vältida kahjulikku isikustatud manipuleerimist ja ärakasutamist.
- (138) Vastastikune seos liidu diskrimineerimisvastase õigusega on oluline ka tehisintellektimääruse artikli 5 lõike 1 punktis b sätestatud keelu puhul,⁹⁶ kuna vanusest ja puudest tingitud haavatavus on samuti kaitstavad tunnused, mille alusel on inimestel õigus mitte olla diskrimineeritud, samas kui sotsiaal-majanduslik olukord ristub mitme muu põhjusega, nagu rass ja etniline päritolu. Tehisintellektimääruses sätestatud keelud ei mõjuta keelde, mis puudutavad muid aluseid või diskrimineerivaid tavaid, mis ei too kaasa olulist kahju ja mis on juba keelatud liidu diskrimineerimisvastase õigusega.
- (139) Tehisintellektimääruse artikli 5 lõike 1 punktides a ja b sätestatud keelud täiendavad ka määrust (EL) 2022/2065 (digiteenuste määrus), millega reguleeritakse veebipõhiseid vahendusteenuseid, nagu digiplatvormid ja otsingumootorid, ning tagatakse läbipaistvus ja vastutus nende teenuste osutamisel. Nimelt on digiteenuste määruse artikli 25 lõikega 1 keelatud petunõksud kasutajaliideses, et tagada, et digiplatvormide pakkujad ei eksita kasutajaid ega sunni neid tegema tegevusi, mis ei pruugi vastata nende tegelikele kavatsustele. Selliseid petunõkse tuleks käsitada näitena manipuleerivatest või eksitavatest võtetest kooskõlas tehisintellektimääruse artikli 5 lõike 1 punktiga a, juhul kui need võivad tõenäoliselt põhjustada olulist kahju.
- (140) Digiteenuste määruses on sätestatud ka digiplatvormide pakkuja kohustus tagada reklaami läbipaistvus (artiklid 26 ja 38 väga suurte digiplatvormide või väga suurte otsingumootorite puhul), soovitusüsteemide kasutamine (artikkel 27) ja alaealiste kaitse (artikkel 28). Lisaks – kui digiplatvorm või otsingumootor on liigitatud väga suureks digiplatvormiks või väga suureks otsingumootoriks, on selle määratud teenuse

⁹⁵ Eriti oluline on selles osas Euroopa Kohtu 4. juuli 2023. aasta otsus (suurkoda) kohtuasjas C-252/21, (Meta Platforms Inc jt vs. Bundeskartellamt. Kuigi Euroopa Liidu Kohus leiab muu hulgas, et suure sotsiaalsuhtlusplatvormi poolt teenuseväliste kasutaja isikuandmete töötlemist otseturunduse eesmärgil võib lugeda toiminuks vastutava töötleja õigustatud huvi järgimise kaalutlustel, ei saa seda teha ilma kasutaja nõusolekuta kui õigusliku aluseta, kuna see on seotud kasutaja huvide ja põhiõigustega, mis selle juhtumi asjaolusid arvestades, eelkõige ulatusliku töötlemise tõttu, kaaluvad üles selle operaatori huvi sellise personaliseeritud reklaami vastu, mille kaudu sotsiaalsuhtlusplatvormid rahastavad oma tegevust (vt otsus kohtuasjas Meta Platforms, punktid 115–118).

⁹⁶ Näiteks nõukogu 29. juuni 2000. aasta direktiiv 2000/43/EÜ, millega rakendatakse võrdse kohtlemise põhimõtte sõltumata isikute rassilisest või emilisest päritolust (EÜT L 180, 19.7.2000, lk 22–26); nõukogu 27. novembri 2000. aasta direktiiv 2000/78/EÜ, millega kehtestatakse üldine raamistik võrdse kohtlemiseks töö saamisel ja kutsealale pääsemisel (EÜT L 303, 2.12.2000, lk 16–22); Euroopa Parlamendi ja nõukogu 5. juuli 2006. aasta direktiiv 2006/54/EÜ meeste ja naiste võrdsete võimaluste ja võrdse kohtlemise põhimõtte rakendamise kohta tööhõive ja elukutse küsimustes (uuesti sõnastatud) (ELT L 204, 26.7.2006, lk 23–36); nõukogu 13. detsembri 2004. aasta direktiiv 2004/113/EÜ meeste ja naiste võrdse kohtlemise põhimõtte rakendamise kohta seoses kaupade ja teenuste kättesaadavuse ja pakkumisega (ELT L 373, 21.12.2004, lk 37–43).

osutajal täiendavad kohustused hinnata ja leevendada süsteemseid riske, mis tulenevad tema teenuse ja sellega seotud süsteemide, sealhulgas algoritmiliste süsteemide disainimisest või toimimisest (digiteenuste määruse artiklid 34 ja 35). Väga suurte digiplatvormide ja väga suurte veebipõhiste otsingumootorite pakkujad peaksid riskianalüüside tegemisel kaaluma, kuidas nende soovitusüsteemid, reklaam, sisu modereerimine ja muud asjakohased algoritmilised süsteemid mõjutavad selliseid süsteemseid riske. Sellistes riskihindamistes tuleks analüüsida ka seda, kuidas süsteemseid riske mõjutavad muu hulgas teenuse tahtlik manipuleerimine ja automatiseeritud kasutamine (vt nt digiteenuste määruse artikli 34 lõige 2 ja põhjendus 83). Siiski hõlmab tehisintellektimääruse artikli 5 lõike 1 punktide a või b kohaldamisala suurt hulka muid stsenaariume (nt juturobotid, tehisintellektipõhised teenused ja tooted), mida võivad pakkuda või kasutada ka teised osalejad peale vahendusteenuste osutajate.

- (141) Tehisintellektimääruse artikli 5 lõike 1 punkti a kohane manipuleerivate tehisintellekti võtete keeld toetab ka direktiivi 2010/13/EL (audiovisuaalmeedia teenuste direktiiv)⁹⁷ eesmärke, takistades meediasektoris kahjulikku tehisintellektipõhist reklaami⁹⁸ ja muid tehisintellektipõhiseid manipuleerivaid ja ekspluateerivaid kasutusviise, mis võivad olla märkimisväärselt kahjulikud.
- (142) Tehisintellektimäärus täiendab ka määrust (EL) 2024/900 (poliitreklaami määrus),⁹⁹ millega sätestatakse ühtlustatud poliitreklaami ja sellega seotud teenuste osutamise normid, sealhulgas läbipaistvuskohustuste ja läbipaistvusega seotud hoolsuskohustuste kohta, ning suunamis- ja reklaamiedastusmeetodite kasutamise kohta internetipõhise poliitreklaami kontekstis. Selle määrusega keelatakse isikuandmete eriliikidel põhinev profiilianalüüs internetipõhise poliitreklaami ja sellistele isikutele suunatud reklaami puhul, kes on vähemalt ühe aasta võrra nooremad kui riigisiseste õigusnormidega kehtestatud valimisõiguslik vanus. Lisaks sellele võib internetipõhises poliitreklaamis kasutada suunamis- ja reklaamiedastusmeetodeid ainult siis, kui need põhinevad andmesubjektidelt kogutud isikuandmetel ja nende selgesõnalisel nõusolekul. Samuti kohaldatakse täiendavaid läbipaistvuse nõudeid, st poliitreklaami avalikustamist, milles kirjeldatakse selliste võtete kasutamist ja peamisi parameetreid ning lisateavet kasutatud võtete loogika, sealhulgas tehisintellektisüsteemide kasutamise kohta. Suunatud poliitreklaam, mis põhineb määruse kohasel isikuandmete töötlemisel,¹⁰⁰ aitab tagada, et valijate profiilianalüüsid ning poliitreklaamide suunamis- ja reklaamiedastusmeetodid toimiksid seadusliku veenmise piirides.
- (143) Tehisintellektimääruse kahjulike ekspluateerivate ja petlike tehisintellekti kasutusviiside keeld täiendab ka muid kohaldatavaid liidu õigusakte, millega kehtestatakse üldised läbipaistvuseeskirjad reklaami ja tarbijakaitse ning ettevõtjate

⁹⁷ Euroopa Parlamendi ja nõukogu 10. märtsi 2010. aasta direktiiv 2010/13/EL audiovisuaalmeedia teenuste osutamist käsitlevate liikmesriikide teatavate õigus- ja haldusnormide koordineerimise kohta (audiovisuaalmeedia teenuste direktiiv), mida on muudetud direktiiviga (EL) 2018/1808, mille eesmärk on muu hulgas parandada laste kaitset ja võidelda tõhusamalt vihakõne vastu.

⁹⁸ Audiovisuaalmeedia teenuste direktiivi artikkel 9.

⁹⁹ Euroopa Parlamendi ja nõukogu 13. märtsi 2024. aasta määrus (EL) 2024/900 poliitreklaami läbipaistvuse ja suunamise kohta (PE/90/2023/REV/1) (ELT L, 2024/900, 20.3.2024).

¹⁰⁰ Kui seda alates 2025. aasta oktoobrist kohaldama hakatakse.

nõuetekohase käitumise kohta (nt direktiiv 2014/65/EL – finantsinstrumentide turgude direktiiv; direktiiv (EL) 2016/97, mis käsitleb kindlustustoodete turustamist;¹⁰¹ direktiiv (EL) 2023/2225, mis käsitleb tarbijakrediidilepinguid; direktiiv (EL) 2002/65 kaugturstuse kohta; direktiiv 2006/114/EÜ eksitava ja võrdleva reklaami kohta; direktiiv (EL) 2011/83 tarbija õiguste kohta, millega kehtestatakse üldised tarbijakaitsestandardid). Sellega seoses on Euroopa Kindlustus- ja Tööandjapensionide Järelevalve Asutus (EIOPA) juba välja andnud järelevalvealase avalduse mõnede ebaausate ekspluateerivate kasutusviiside kohta seoses diferentseeritud hinnakujundusega, mis võivad samuti kuuluda tehisintellektimääruse kohaldamisalasse, kui seda võimaldavad tehisintellektisüsteemid¹⁰².

- (144) Ka tehisintellektimääruse artikli 5 lõike 1 punktides a ja b sätestatud keelud ei piira ja täiendavad ELi tooteohutusalaseid õigusakte (nt meditsiiniseadmete, mänguasjade ja masinate kohta), millel on tehisintellektisüsteeme sisaldavate toodete ohutuse tagamisel oluline osa. See hõlmab reguleeritud toodete *ex ante* ohutusnõuete täitmist ja nende ennetavat järelevalvet, et tagada, et need ei tekita füüsilist ja vaimset kahju põhjustavaid ohutusriske. Seepärast peaks tehisintellektisüsteeme sisaldavate toodete tootja neid keelde oma riskianalüüsides ja ohutusalastes leevendusmeetmetes arvesse võtma, kuivõrd see on kooskõlas asjakohaste liidu ühtlustatud ohutusalaste õigusaktide loogika ja kohaldamisalaga. Ühtlasi täiendavad Liidu ohutusalased õigusaktid täiendavad tehisintellektimääruse keelde ning võivad sekkuda ka selliste ohutusriskide puhul, mis ei põhjusta olulist kahju, ja neid käsitleda. Näiteks määrus (EL) 2023/988 (üldine tooteohutuse määrus)¹⁰³ toimib turvavõrguna ja nõuab, et kõik tarbekaubad, mis ei ole hõlmatud muude valdkondlike liidu tooteohutuse alaste õigusaktide erinõuetega (sealhulgas tooted, mis sisaldavad tehisintellektisüsteeme, mida ei liigitata määruse artikli 6 kohaselt suure riskiga toodeteks ja mille suhtes kohaldatakse tehisintellektimääruse nõudeid), oleksid tavalistes või mõistlikult eeldatavates kasutustingimustes ohutud, eelkõige seoses tarbijate füüsilise ja vaimse tervise riskidega.
- (145) Lõpetuseks on kriitilise tähtsusega ka koostoime kriminaalõigusega. Tehisintellektimääruse artikli 5 lõike 1 punktides a ja b sätestatud keeldude eesmärk on takistada kahjulikku käitumist, mis võib kujutada endast kuritegu või viia kuritegudeni, nagu kelmus, võltsimine, pettus, sundimine või ebaseadusliku sisu, näiteks terroristliku sisu, laste seksuaalset kuritarvitamist kujutava materjali, vihakõne ja seksuaalse sisuga süvavõltsingute loomine ja levitamine¹⁰⁴. Oluline on see, et kuna tehisintellektimäärus on siseturu õigusakt, hõlmavad artikli 5 lõike 1 punktides a ja b sätestatud keelud mitte ainult tehisintellektisüsteemi kasutamist, vaid ka selle turule laskmist, ennetades seega

¹⁰¹ Euroopa Parlamendi ja nõukogu 20. jaanuari 2016. aasta direktiiv (EL) 2016/97, mis käsitleb kindlustustoodete turustamist (uuesti sõnastatud) (ELT L 26, 2.2.2016, lk 19–59). Näiteks kindlustuse turustamist käsitleva direktiivi artikli 17 lõige 1, mille kohaselt peavad kindlustuse turustajad tegutsema ausalt, õiglaselt ja professionaalselt oma klientide huvides.

¹⁰² https://www.eiopa.europa.eu/document/download/1e9a8fb2-e688-4bf5-a347-ee0a1ec3aab3_en?filename=EIOPA-BoS-23-076-Supervisory-Statement-on-differential-pricing-practices_0.pdf.

¹⁰³ Euroopa Parlamendi ja nõukogu 10. mai 2023. aasta määrus (EL) 2023/988, milles käsitletakse üldist tooteohutust ja millega muudetakse Euroopa Parlamendi ja nõukogu määrust (EL) nr 1025/2012 ja Euroopa Parlamendi ja nõukogu direktiivi (EL) 2020/1828 ning tunnistatakse kehtetuks Euroopa Parlamendi ja nõukogu direktiiv 2001/95/EÜ ja nõukogu direktiiv 87/357/EMÜ (EMPs kohaldatav tekst).

¹⁰⁴ Euroopa Parlamendi ja nõukogu 14. mai 2024. aasta direktiiv (EL) 2024/1385, mis käsitleb naistevastase vägivalga ja perevägivalga tõkestamist (PE/33/2024/REV/1) (ELT L, 2024/1385, 24.5.2024).

varakult kahju, piirates juurdepääsu sellistele keelatud süsteemidele, mis võivad hõlbustada ja varjata kuritegelikku tegevust. Lisaks võivad tehisintellektimääruse artikli 5 lõike 1 punktides a ja b sätestatud keelud hõlmata ka muid kahjulikke tavasid, mida ei loeta liidu või riigisisese õiguse kohaselt kuritegudeks.

4. TEHISINTELLEKTIMÄÄRUSE ARTIKLI 5 LÕIKE 1 PUNKT C – SOTSIAALPUNKTIDE ANDMINE

- (146) Kuigi tehisintellekti abil toimuv sotsiaalpunktide andmine võib tuua kasu hea käitumise suunamisel ning ohutuse, tõhususe või teenuste kvaliteedi parandamisel, on olemas teatud sotsiaalpunktide andmise tavad, mis kohtlevad inimesi ebaõiglaselt või kahjustavad neid ning kujutavad endast sotsiaalset kontrolli ja järelevalvet. Tehisintellektimääruse artikli 5 lõike 1 punktis c sätestatud keeld on suunatud sellistele vastuvõetamatutele tehisintellekti võimaldatud sotsiaalpunktide andmise tavadele, millega hinnatakse või liigitatakse isikuid või rühmi nende sotsiaalse käitumise või isikuomaduste alusel ja mis viivad kahjustava või ebasoodsa kohtlemiseni, eelkõige juhul, kui andmed pärinevad mitmest omavahel mitteseotud sotsiaalsest kontekstist või kui kohtlemine on sotsiaalse käitumise kaalukusega võrreldes ebaproportsionaalne. Sotsiaalpunktide andmise keelul on nii avaliku kui ka erasektori kontekstis lai kohaldamisala ning see ei piirdu konkreetse sektori või valdkonnaga¹⁰⁵.
- (147) Samal ajal ei ole keeld mõeldud mõjutama inimeste seaduslikku hindamist, mida tehakse konkreetsel eesmärgil kooskõlas liidu või riigisisese õigusega,¹⁰⁶ eelkõige juhul, kui sellistes õigusaktides on täpsustatud konkreetsetel hindamistel kasutatavate andmete liigid ja tagatud, et sellest tulenev isikute kahjustav või ebasoodne kohtlemine on põhjendatud ja proportsionaalne (vt punkti 4.3 kohaldamisalast välja jäävate olukordade kohta).

4.1. Põhjendus ja eesmärgid

- (148) Sotsiaalpunktide andmist võimaldavad tehisintellektisüsteemid võivad viia diskrimineerivate ja ebaõiglaste tulemusteni teatavate isikute ja rühmade jaoks, sealhulgas nende tõrjutuseni ühiskonnast, samuti sotsiaalse kontrolli ja järelevalve tavadeni, mis ei ole kooskõlas liidu väärtustega. Sotsiaalpunktide andmise keelu eesmärk on kaitsta eelkõige õigust inimväärikusele ja muid põhiõigusi, sealhulgas õigust mittediskrimineerimisele ja võrdsusele, andmekaitsele ning era- ja perekonnaelu austamisele, samuti asjakohaseid sotsiaalseid ja majanduslikke õigusi, kui need on kohaldatavad. Samuti on selle eesmärk kaitsta ja edendada liidu väärtusi, nagu demokraatia, võrdõiguslikkus (sealhulgas võrdne juurdepääs avalikele ja erateenustele) ja õiglus¹⁰⁷.

4.2. Sotsiaalpunktide andmise keelu põhimõisted ja komponendid

¹⁰⁵ Sotsiaalpunktide andmise keeld erineb artikli 5 lõike 1 punktis d sätestatud keelust, mis käsitleb konkreetsemalt hindamise /punktide andmise tavasid, mida kasutatakse üksnes selleks, et hinnata riski ja prognoosida seda, et isik paneb toime kuriteo, keelates üksnes profiilanalüüsil või isikuomaduste ja erijoonete hindamisel põhinevad tehisintellektisüsteemid (vt punkt 5).

¹⁰⁶ Tehisintellektimääruse põhjendus 31.

¹⁰⁷ Tehisintellektimääruse põhjendus 31.

Tehisintellektimääruse artikli 5 lõike 1 punktis c on sätestatud:

„Järgmised tehisintellekti kasutusviisid on keelatud:

c) selliste tehisintellektisüsteemide turule laskmine, kasutusele võtmine või kasutamine, millega hinnatakse või liigitatakse füüsilisi isikuid või isikute rühmi teatava aja jooksul, tuginedes nende sotsiaalsele käitumisele või teadaolevatele, tuletatud või prognoositud isiku- või iseloomuomadustele, kusjuures sotsiaalpunktide tulemuseks on üks või mõlemad järgmisest:

i) teatavaid füüsilisi isikuid või isikute rühmi kahjustav või nende suhtes ebasoodne kohtlemine sotsiaalses kontekstis, mis ei ole seotud kontekstiga, milles andmed algselt loodi või koguti;

ii) teatavaid füüsilisi isikuid või isikute rühmi kahjustav või nende ebasoodne kohtlemine, mis ei ole põhjendatud või on ebaproportsionaalne võrreldes nende sotsiaalse käitumise või selle kaalukusega;“.

(149) Selleks, et tehisintellektimääruse artikli 5 lõike 1 punktis c sätestatud keeld oleks kohaldatav, peavad olema täidetud mitu kumulatiivset tingimust:

(i) kasutusviis peab kujutama endast tehisintellektisüsteemi turule laskmist, kasutusele võtmist või kasutamist;

(ii) tehisintellektisüsteem peab olema ette nähtud või seda tuleb kasutada füüsiliste isikute või isikute rühmade hindamiseks või liigitamiseks teatava ajavahemiku jooksul, võttes aluseks:

(a) nende sotsiaalse käitumise või

(b) teadaolevad, tuletatud või prognoositud isiku- või iseloomuomadused;

(iii) tehisintellektisüsteemi abil antud sotsiaalpunktid peavad viima või suutma viia isikute või rühmade kahjustava või ebasoodsa kohtlemiseni ühes või mitmes järgmises stsenaariumis:

(a) sotsiaalne kontekst, mis ei ole seotud sellega, milles andmed algselt loodi või koguti, ja/või

(b) kohtlemine, mis on isiku sotsiaalse käitumise või selle kaalukusega võrreldes põhjendamatu või ebaproportsionaalne.

(150) Selleks, et tehisintellektimääruse artikli 5 lõike 1 punktis c sätestatud keeld oleks kohaldatav, peavad kõik kolm tingimust olema samal ajal täidetud. Esimest tingimust, st tehisintellektisüsteemi turule laskmist, kasutusele võtmist või kasutamist, on juba analüüsitud punktis 2.3. Seega kehtib keeld nii tehisintellektisüsteemide pakkujate kui ka juurutajate suhtes, kes on oma vastutuse piires kohustatud selliseid süsteeme mitte turule laskma, kasutusele võtma ega kasutama. Allpool kirjeldatakse ja analüüsitakse põhjalikumalt ülejäänud kriteeriume, mille alusel sotsiaalpunktide andmine keelatud on.

4.2.1. Sotsiaalpunktide andmine: hindamine või liigitamine sotsiaalse käitumise või isiku- või iseloomuomaduste alusel teatud aja jooksul

a) Füüsiliste isikute või isikute rühma hindamine või liigitamine

- (151) Teine tingimus, mille alusel saab kohaldada tehisintellektimääruse artikli 5 lõike 1 punktis c sätestatud keeldu, on see, et tehisintellektisüsteem on ette nähtud või seda kasutatakse **füüsiliste isikute või isikute rühmade hindamiseks või liigitamiseks** ja neile antakse hindeid nende sotsiaalse käitumise või isiku- või iseloomuomaduste alusel. Süsteemi antud punktisumma võib olla esitatud mitmesugusel kujul, näiteks matemaatilise arvu (näiteks 0 kuni 1), pingerea või märgistusena.
- (152) Keelu kohaldamisala on lai, hõlmates nii avaliku kui ka erasektori hindamis- ja liigitamistavasid (vt punkt 4.2.3). Samas puudutab hindamine või liigitamine ainult füüsilisi isikuid või füüsiliste isikute rühmi, jättes seega põhimõtteliselt välja juriidilised isikud (vt punkti 4.3 kohaldamisalast välja jäävate olukordade kohta).
- (153) Kuigi „**hindamine**“ viitab mingi **hinnangu** andmisele isiku või isikute rühma kohta, ei pruugi isikute või isikute rühmade lihtne **liigitamine** selliste tunnuste alusel nagu vanus, sugu ja pikkus tingimata viia hindamiseni¹⁰⁸. Seega on mõiste „liigitamine“ laiem kui „hindamine“ ja võib hõlmata ka muud liiki füüsiliste isikute või isikute rühmade liigitamist selliste kriteeriumide alusel, mis ei pruugi hõlmata konkreetset hinnangut või otsust nende isikute või isikute rühmade ja nende omaduste või käitumise kohta.
- (154) Mõiste „**hindamine**“ on seotud ka mõistega „profiilialalüüs“, mida reguleerivad liidu andmekaitsealased õigusaktid¹⁰⁹ ja mis kujutab endast hindamise erivormi. Kuigi tehisintellektimääruse artikli 5 lõike 1 punktis c ei viidata otseselt sellele mõistele või sellele õigusaktile,¹¹⁰ võivad need olla asjakohased ka selles sättes sisalduva keelu, samuti muude tehisintellektimääruse keeldude puhul,¹¹¹ kui tehisintellektisüsteem teeb isikuandmete põhjal automatiseeritud hindamist. **Profiilialalüüs** tähendab teabe kasutamist üksikisiku (või üksikisikute rühma) kohta ning nende omaduste või käitumismustrite hindamist, et paigutada nad konkreetsesse kategooriasse või rühma, eelkõige selleks, et **analüüsida ja/või prognoosida** näiteks nende mingi ülesande täitmise võimet, huve või tõenäolist käitumist¹¹². ELi andmekaitseõiguse kohane füüsiliste isikute profiilialalüüs, kui see toimub tehisintellektisüsteemide kaudu, võib seega kuuluda ka tehisintellektimääruse artikli 5 lõike 1 punkti c kohaldamisalasse.

¹⁰⁸ Artikli 29 alusel asutatud andmekaitse töörühma suunised automatiseeritud töötlusel põhinevate üksikotsuste tegemise ja profiilialalüüsi kohta määruse 2016/679 kohaldamisel (Wp251rev.01), 6.2.2018, lk 7.

¹⁰⁹ Vt isikuandmete kaitse üldmääruse artikli 4 lõige 4 ja artikkel 22 ning õiguskaitse direktiivi artikkel 11. Vt ka artikli 29 alusel asutatud andmekaitse töörühma suunised automatiseeritud töötlusel põhinevate üksikotsuste tegemise ja profiilialalüüsi kohta määruse 2016/679 kohaldamisel (Wp251rev.01), 6.2.2018, lk 7.

¹¹⁰ Tehisintellektimääruse artikli 3 punkt 52 sisaldab profiilialalüüsi määratlust, milles viidatakse andmekaitse üldmääruse artikli 4 punkti 4 määratlusele.

¹¹¹ Eelkõige tehisintellektimääruse artikli 5 lõike 1 punktis d esitatud üksikisikute kuritegevuse riski prognoosimise keeld, mis viitab profiilialalüüsile, ning teatud juhtudel tehisintellektimääruse artikli 5 lõike 1 punktides f ja g kirjeldatud emotsioonituvastuse ja biomeetrilise liigitamise keeld.

¹¹² Artikli 29 alusel asutatud andmekaitse töörühma suunised automatiseeritud töötlusel põhinevate üksikotsuste tegemise ja profiilialalüüsi kohta määruse 2016/679 kohaldamisel (Wp251rev.01), 6.2.2018, lk 7.

Näiteks SCHUFA I kohtuasjas¹¹³ uuris Euroopa Liidu Kohus Saksamaal kasutatavat **krediitdivõimelisuse hindamise süsteemi**. Kõnealusel juhul kasutati arvutiprogrammi genereeritud punkte „tõenäosusväärtusena“, mis näitas isiku suutlikkust täita tulevikus maksekohustusi ning mille Euroopa Liidu Kohus liigitas profiilianalüüsiks. Konkreetsemalt koostas süsteem „prognoosi isiku tulevikukäitumise – näiteks laenu tagasimaksmine – tõenäosuse kohta (*score*), selle isiku teatavate tunnuste põhjal. Skoori kindlaksmääramine (*scoring*) põhineb eeldusel, et isiku liigitamisel sarnaste tunnustega ja teatava käitumisega isikute rühma, on võimalik ennustada sarnast käitumist¹¹⁴.“ Euroopa Liidu Kohtu arvates vastab selline tegevus isikuandmete kaitse üldmääruse artikli 4 punktis 4 sisalduvale „profiilianalüüsi“ määratlusele¹¹⁵. Sellist profiilianalüüsi võib pidada ka isikuomadustel põhinevaks isiku hindamise vormiks tehisintellektimääruse artikli 5 lõike 1 punkti c tähenduses, mis on keelatud, kui seda tehakse tehisintellektisüsteemide abil ja tingimusel, et muud tingimused kõnealuse sätte kohaldamiseks on täidetud.

b) Teatava aja jooksul

- (155) Tehisintellektimääruse artikli 5 lõike 1 punktis c sätestatud keeld nõuab, et andmetel põhinev hindamine või liigitamine toimuks „**teatava aja jooksul**“. See viitab sellele, et hindamine ei tohiks piirduda ühekordse hinnangu või hindamisega, mille aluseks on andmed või käitumine väga konkreetsetes individuaalses kontekstis. Samas on oluline, et seda tingimust hinnatakse, võttes arvesse kõiki juhtumi asjaolusid, et vältida keelu kohaldamisalast kõrvalehoidmist.

Näiteks rakendab rände- ja varjupaigaasutus pagulaslaagrites osaliselt automatiseeritud järelevalvesüsteemi, mis põhineb mitmesugusel seiretaristul, sealhulgas kaameratel ja liikumisanduritel. Kui analüüsitud andmed hõlmavad ajavahemikku ja hinnatakse konkreetseid isikuid (näiteks rändajaid), et teha kindlaks, kas nende puhul on olemas oht, et nad võivad üritada põgeneda, siis toimub see „teatava aja jooksul“ ja tehisintellektimääruse artikli 5 lõike 1 punktis c sätestatud keeldu võib kohaldada, kui kõik muud tingimused on täidetud.

c) Tuginedes nende sotsiaalsele käitumisele või teadaolevatele, tuletatud või prognoositud isiku- või iseloomuomadustele

- (156) Tehisintellektimääruse artikli 5 lõike 1 punkti c alusel keelatud hindamise ja liigitamise tavad peavad põhinema tehisintellekti abil toimuval (sageli ulatuslikul) andmete töötlemisel, mis on seotud kas i) isikute või isikute rühmade sotsiaalse käitumise või ii) nende teadaolevate, tuletatud või prognoositud isiku- ja iseloomuomaduste või mõlemaga. Andmed võisid esitada need isikud ise otse või need võivad olla kogutud kaudselt, st jälgimise teel, kolmandatelt isikutelt saadud või muust teabest tuletatud.
- (157) Esimese stsenaariumi puhul on „**sotsiaalne käitumine**“ lai mõiste, mis võib üldiselt hõlmata tegevusi, käitumist, harjumusi, suhtlemist ühiskonnas jne ning hõlmab

¹¹³ Kohtuotsus, Euroopa Kohus, 7. detsember 2023, SCHUFA Holding (Scoring), C-634/21, EU:C:2023:957 (edaspidi „SCHUFA I kohtuasi“), nt punkt 47.

¹¹⁴ Samas, punkt 14 (esiletõst lisatud).

¹¹⁵ Samas, punkt 47.

tavaliselt mitmest allikast pärit käitumisega seotud andmepunkte¹¹⁶. See võib hõlmata üksikisikute ja üksikisikute rühmade käitumist sotsiaalses ja eraelulises kontekstis, näiteks osalemist kultuuriüritustel, vabatahtlikku tegevust jne, aga ka sotsiaalsel käitumisel ärikontekstides, näiteks võlgade tasumist, käitumist teatud teenuste kasutamisel, samuti suhteid avalike ja eraisikute, valitsuse, politsei ja seadusega (näiteks kas inimene järgib liiklusreegleid). Sotsiaalse käitumise andmeid mitmest kontekstist ja andmepunktist võib koguda tsentraliseeritult üks ja sama üksus, kuid enamasti kogutakse neid hajutatult ja kombineeritakse erinevatest allikatest saadud andmeid, mis võib hõlmata suurenenud jälgimist ja üksikisikute jälgimist (nn „andmeseire“).

- (158) Teine stsenaarium on see, kus punktide andmine põhineb **isiku- või iseloomuomadustel**, mis võivad hõlmata konkreetseid sotsiaalse käitumise aspekte. Isikuomadused võivad hõlmata mitmesuguseid isiku kohta käivaid andmeid, näiteks bioloogiline sugu, seksuaalne orientatsioon või seksuaalsed omadused, sotsiaalne sugu, sooline identiteet, rass, etniline päritolu, perekondlik olukord, aadress, sissetulek, leibkonna liikmed, elukutse, töö või muu õiguslik seisund, töö tulemused, majanduslik olukord, rahaline likviidsus, tervis, isiklikud eelistused, huvid, usaldusväärsus, käitumine, asukoht või liikumine, võlatase, auto tüüp jne¹¹⁷. Iseloomuomadusi tuleks põhimõtteliselt tõlgendada iseloomuomaduste sünonüümina, kuid see võib tähendada ka üksikisikute kui isiksuste konkreetsete profiilide loomist. Iseloomuomadused võivad samuti põhineda mitmel teguril ja eeldada hinnangut, mille võivad anda üksikisikud ise või teised isikud või koostada tehisintellektisüsteemid. Tehisintellektimääruses nimetatakse iseloomuomadusi mõnikord isikuomadusteks ja erijoonteks;¹¹⁸ neid mõisteid tuleks tõlgendada järjepidevalt.
- (159) „Teadaolevad, tuletatud või prognoositud“ isiku- või iseloomuomadused on mitmesugust liiki teave ja isikuandmed, mida tuleb eristada. „**Teadaolevad omadused**“ põhinevad teabel, mis on tehisintellektisüsteemile sisendina esitatud ja mis on enamasti kontrollitav teave. Seevastu „**tuletatud omadused**“ põhinevad teabel, mis on tuletatud muust teabest, kusjuures seda tuletab tavaliselt tehisintellektisüsteem. „**Prognoositud omadused**“ on need, mis on hinnatud muustrite alusel vähem kui 100 % täpsusega. „Tuletatud“ andmete mõistet kasutatakse ka liidu andmekaitsealastes õigusaktides profiilianalüüsi kontekstis ja see võib seega olla inspiratsiooniallikaks tehisintellektimääruse artikli 5 lõike 1 punktis c kasutatud mõistete tõlgendamisel¹¹⁹. Nende eri liiki andmete kasutamine võib punktide andmise täpsusele ja õiglusele erinevat mõju avaldada ning seetõttu võib seda arvesse võtta, eelkõige juhul, kui töötlemine on läbipaistmatu või tugineb andmetele, mille täpsust on raskem kontrollida.

4.2.2. Sotsiaalpunktid peavad tooma kaasa kohtlemise, mis on mitteseotud sotsiaalses kontekstis kahjustav või ebasoodne ja/või sotsiaalse

¹¹⁶ Vt tehisintellektimääruse põhjendus 31.

¹¹⁷ Vt tehisintellektimääruse põhjendus 42, kus on loetletud mõned selliste tunnuste näited.

¹¹⁸ Tehisintellektimääruse artikli 5 lõike 1 punkt d.

¹¹⁹ Artikli 29 alusel asutatud andmekaitse töörühma suunised automatiseeritud töötlusel põhinevate üksikotsuste tegemise ja profiilianalüüsi kohta määruse 2016/679 kohaldamisel (Wp251rev.01), 6.2.2018, lk 7 jj.

käitumise kaalukusega võrreldes põhjendamatu või ebaproportsionaalne

a) Põhjuslik seos sotsiaalpunktide ja kohtlemise vahel

- (160) Selleks, et saaks kohaldada tehisintellektimääruse artikli 5 lõike 1 punktis c kehtestatud keeldu, peab tehisintellektisüsteemi poolt või abil antud sotsiaalpunktide andmine tooma kaasa hinnatud isiku või isikute rühma **kahjustava või ebasoodsa kohtlemise**. Teisisõnu peab kohtlemine olema antud punktide tagajärg ning punktid peavad olema sellise kohtlemise põhjus. Selline usutav põhjuslik seos võib eksisteerida ka juhtudel, kui kahjulikud tagajärjed ei ole veel realiseerunud, kuid tehisintellektisüsteem on kavandatud või võimeline sellist kahjulikku tulemust tekitama. See on eriti oluline, kuna tehisintellektimääruse artikli 5 lõike 1 punktis c sätestatud keelatud kasutusviis hõlmab ka selliste tehisintellektisüsteemide turule laskmist.
- (161) Tehisintellektimääruse artikli 5 lõike 1 punktis c ei ole nõutud, et tehisintellektisüsteemi poolne hindamine või liigitamine oleks kahjustava või ebasoodsa kohtlemise ainuke põhjus. Seega hõlmab see ka tehisintellektipõhiseid punktide andmise tavasid, mille kohta võidakse anda inimhinnanguid või mida võidakse kombineerida muude inimhinnangutega. Samal ajal peab tehisintellekti väljundil olema sotsiaalpunktide andmisel piisavalt oluline osa. Näiteks juhul, kui ametiasutus kasutab isikute usaldusvääruse hindamiseks tehisintellektisüsteemi ja kombineerib selle tulemuse täiendavate asjaolude inimhinnanguga, kuulub selline tehisintellektipõhine sotsiaalpunktide andmise tava keelu kohaldamisalasse ainult juhul, kui tehisintellekti abil saadud hindel on lõplikus otsuses piisavalt oluline osa, tingimusel et muud kahjustava või ebasoodsa kohtlemise tingimused on täidetud, nagu on kirjeldatud allpool (vt punkt 4.2.2.b).
- (162) Hinne võib põhjustada kahjustavat või ebasoodsat kohtlemist isegi siis, kui selle on koostanud mõni muu organisatsioon kui see, kes hinnet kasutab¹²⁰. Näiteks võib ametiasutus saada füüsilise isiku krediitvõimelisuse hindamiseks punktisumma, mille on koostanud teine ettevõtte, kes spetsialiseerub krediitvõimelisuse ja riskide hindamisele, võttes aluseks erinevatest allikatest saadud teabe üksikisikute ja nende käitumise kohta.

b) Kahjustav või ebasoodne kohtlemine mitteseotud sotsiaalses kontekstis ja/või põhjendamatu või ebaproportsionaalne kohtlemine

- (163) Viimane tingimus, et tehisintellektimääruse artikli 5 lõike 1 punktis c sätestatud keeldu saaks kohaldada, on see, et sotsiaalpunktide kasutamine peab tooma kaasa kahjustava või ebasoodsa kohtlemise (või olema võimeline seda tegema):
- i. sotsiaalse(te)s konteksti(de)s, mis ei ole seotud kontekstiga, milles andmed algselt loodi või koguti, või

¹²⁰ See tõlgendus on kooskõlas Euroopa Liidu Kohtu otsusega SCHUFA I kohtuasjas, kus Euroopa Liidu Kohus otsustas automatiseeritud otsuste tegemise kontekstis, et „punktisumma“ (hindamine, mis kujutab endast profiilianalüüsi), mille on andnud muu üksus kui lõpliku otsuse tegija, võib olla automatiseeritud otsus isikuandmete kaitse üldmääruse artikli 22 alusel. Vt SCHUFA I kohtuasi, punktid 42–51 ja 60–62.

- ii. sellisel viisil, mis on põhjendamatu või sotsiaalse käitumise või selle kaalukusega võrreldes ebaproportsionaalne.
- (164) Need tingimused on alternatiivsed ja neid võib kohaldada ka kombineeritult. Seda, kas vähemalt üks neist on täidetud, on vaja analüüsida iga juhtumi puhul eraldi, sest paljud tehisintellektipõhised punktide andmise ja hindamistavad ei pruugi neid täita ja jäävad seega keelu kohaldamisalast välja. Eelkõige ei pruugi see nii olla juhul, kui tehisintellektipõhisel punktide andmise taval on konkreetne õiguspärane hindamisotstarve ning see vastab kohaldatavale liidu ja riigisisesele õigusele, milles täpsustatakse hindamise eesmärgil asjakohaseks peetavad andmed, ja tagatakse, et kahjustav või ebasoodne kohtlemine on sotsiaalse käitumise suhtes proportsionaalne ja põhjendatud (vt punkti 4.3 kohaldamisalast välja jäävate olukordade kohta).
- (165) „**Ebasoodne kohtlemine**“ tähendab, et punktide andmise tulemus peab olema see, et isikut või isikute rühma koheldakse teistega võrreldes ebasoodsamalt, ilma et see tingimata eeldaks erilist kahju (näiteks selliste punktide andmise tavade puhul, kus inimesed valitakse pettusekahtluse korral välja lisakontrollide tegemiseks). Seevastu „**kahjulik**“ kohtlemine eeldab, et isik või isikute rühm kannab kohtlemise tõttu teatavat kahju. Ebasoodne või kahjulik kohtlemine võib ka olla diskrimineeriv ja keelatud ELi diskrimineerimisvastase õiguse alusel või tähendada teatavate isikute või rühmade kõrvalejätmist,¹²¹ kuid see ei ole keelu kohaldamiseks vajalik tingimus. Tehisintellektimääruse artikli 5 lõike 1 punkt c võiks seega käsitleda ka ebaõiglast kohtlemist, mida ELi diskrimineerimisvastane õigus, mida kohaldatakse ainult teatud kaitstud rühmade suhtes (nt vanus, etniline ja rassiline päritolu, sugu, usk), ei hõlma.

1. stsenaarium: kahjustav või ebasoodne kohtlemine mitteseotud sotsiaalses kontekstis

- (166) Tehisintellektimääruse artikli 5 lõike 1 punkti c alapunktis i kirjeldatud esimeses stsenaariumis peab punktide andmisest tulenev kahjustav või ebasoodne kohtlemine toimuma **sotsiaalses kontekstis, mis ei ole seotud** kontekstiga, milles andmed algselt loodi või koguti. See ei tähenda mitte ainult seda, et isikuid võidakse sotsiaalpunktide andmise tõttu ebasoodsalt või halvemini kohelda, vaid ka seda, et andmed nende sotsiaalse käitumise või nende teadaolevate, tuletatud või prognoositud isiku- või iseloomuomaduste kohta on loodud või kogutud sotsiaalses kontekstis, mis ei ole seotud sellega, kus punktide andmine toimub. Nendes mitteseotud kontekstides kogutud või loodud andmeid peab tehisintellektisüsteem hiljem kasutama isikutele punktide andmiseks või nende liigitamiseks ilma ilmse seoseta või viisil, mis viib isikute või isikute rühmade üldise jälgimiseni. Enamikul juhtudel toimub see isikute mõistlike ootuste vastaselt ning vastuolus liidu andmekaitsealaste õigusaktide ja potentsiaalselt ka muude kohaldatavate õigusnormidega, milles on täpsustatud, millist liiki andmeid ja allikaid peetakse hindamise või liigitamise jaoks asjakohaseks ja vajalikuks. Seda, kas see tingimus on täidetud, tuleb hinnata iga juhtumi puhul eraldi, võttes arvesse hindamise eesmärki ja konteksti, milles andmed on kogutud ja genereeritud.

¹²¹ Tehisintellektimääruse põhjendus 31.

Näited kahjustavast või ebasoodsast kohtlemisest mitteseotud sotsiaalsetes kontekstides, mis on keelatud tehisintellektimääruse artikli 5 lõike 1 punkti c alapunkti i alusel:

- riigi maksuhaldurid kasutavad tehisintellektipõhist prognoosimisvahendit kõikide maksumaksjate maksudeklaratsioonide uurimiseks, et valida välja maksudeklaratsioonid põhjalikuma kontrolli tegemiseks. Tehisintellekti vahend kasutab asjakohaseid muutujaid, nagu aastane sissetulek, varad (kinnisvara, autod jne), andmed abisaajate pereliikmete kohta, aga ka mitteseotud andmeid, nagu maksumaksjate sotsiaalsed harjumused või internetiühendused, et valida kontrollimiseks konkreetseid isikuid;
- sotsiaalhoolekandetasutus kasutab tehisintellektisüsteemi, et hinnata majapidamistoetuste saajate pettuse tõenäosust, mis tugineb sotsiaalsest kontekstist kogutud või tuletatud omadustele, millel ei ole pettuse hindamisega ilmset seost või tähtsust selle jaoks, näiteks teatud rahvusest või etnilise päritoluga abikaasa olemasolu, internetiühenduse olemasolu, käitumine sotsiaalplatvormidel või tööalased tulemused jne¹²². Seevastu andmeid, mis on toetuste määramise seisukohast olulised ja seaduslikult kogutud, võib kasutada pettuse riski kindlaksmääramiseks, kuna ametiasutuste seaduslik eesmärk on kontrollida, kas sotsiaaltoetused on õigesti määratud;
- riiklik tööjõuamet kasutab tehisintellektisüsteemi, et anda töötutele punkte vestluse ja tehisintellektipõhise hindamise alusel, et otsustada, kas isik peaks saama riiklikku toetust tööhõiveks. Need punktid põhinevad asjakohastel isikuomadustel, nagu vanus ja haridus, aga ka muutujatel, mis on kogutud või tuletatud andmetest ja kontekstides, millel ei ole ilmset seost hindamise eesmärgiga, nagu perekonnaseis, terviseandmed krooniliste haiguste, sõltuvuse kohta jne¹²³.

Neid lubamatuid punktide andmise tavaid võib eristada seaduslikest tavadest, mille puhul hinnatakse isikuid konkreetsel eesmärgil kooskõlas liidu ja riigisisese õigusega, eelkõige juhul, kui sellistes õigusaktides on kooskõlas ELi õigusega täpsustatud andmed, mida peetakse hindamise eesmärgil asjakohaseks ja vajalikuks (vt punkti 4.3 kohaldamisalast välja jäävate olukordade kohta).

2. stsenaarium: kahjustav või ebasoodne kohtlemine, mis on sotsiaalse käitumisega võrreldes ebaproportsionaalne

- (167) Teine tehisintellektimääruse artikli 5 lõike 1 punkti c alapunkti ii kohane alternatiivne stsenaarium, mille puhul võib tehisintellektipõhine punktide andmise süsteem olla keelatud, on see, kui punktidest tulenev kohtlemine on põhjendamatu või sotsiaalse käitumise kaalukusega võrreldes ebaproportsionaalne. Sotsiaalpunktide andmise tagajärjel tekkiva mõju tõsidus ja asjaomase isiku põhiõigustesse sekkumise ulatus

¹²² Võrdluseks samaste riiklike hüvitiste süsteemide ja sotsiaalpunktide andmise kohta vt D. Hadwick & S. Lan, Lessons to be learned from the Dutch childcare allowance scandal: A comparative review of algorithmic governance by tax administrations in the Netherlands, France and Germany, World Tax Journal (2021), 13. köide, nr 4, Familiales (CNAF).

¹²³ Poolas kasutati samalaadset töötute profiilanalüüsi süsteemi, millest loobuti pärast seda, kui leiti, et see oli põhiseadusega vastuolus. Vt Szymielewicz, *Profiling the unemployed in Poland: Social and Political Implications of Algorithmic Decision Making*, Fundacja Panoptykon, 2015, lk 18.

võrreldes isiku sotsiaalse käitumise kaalukusega peaks määrama, kas selline kohtlemine on taotletava õiguspärase eesmärgi suhtes eproportsionaalne, võttes arvesse proportsionaalsuse üldpõhimõtet. See nõuab juhtumipõhist hindamist, mille käigus tuleks arvesse võtta kõiki juhtumi asjakohaseid asjaolusid, samuti üldisi eetilisi kaalutlusi ning õigluse ja sotsiaalse õigluse põhimõtteid, mis on seotud sotsiaalse käitumise ja kahjustava kohtlemise proportsionaalsuse hindamisega. Kohtlemine võib olla ka põhjendamatu, näiteks kui puudub õiguspärane eesmärk. Kõnealuse hindamise raames võivad olla asjakohased ka valdkondlikud liidu või riigisisised õigusaktid, milles sätestatakse konkreetsete kriteeriumid ja menetlused, mis reguleerivad sellist võimalikku kahjustavat või ebasoodsat kohtlemist.

Näiteid põhjendamatu või sotsiaalse käitumisega võrreldes eproportsionaalsest kohtlemisest, mis on tehisintellektimääruse artikli 5 lõike 1 punkti c alapunkti ii kohaselt keelatud:

- avalik-õiguslik asutus kasutab tehisintellektisüsteemi perekondade profiilianalüüsiks, et varakult tuvastada riskiolukorras lapsed, võttes aluseks sellised kriteeriumid nagu vanemate vaimne tervis ja töötus, aga ka mitmest kontekstist saadud teave vanemate sotsiaalse käitumise kohta. Saadud punktisumma põhjal valitakse välja perekonnad, mida kontrollida, ja lapsed, keda peetakse riskiolukorras olevaks, võetakse peredest ära, sealhulgas vanemate väiksemate rikkumiste korral, näiteks kui nad jätaavad aeg-ajalt arsti vastuvõttule minemata või saavad liiklustrahve;
- omavalitsus kasutab tehisintellektisüsteemi, et hinnata elanike usaldusväärust mitme andmepunkti põhjal, mis on seotud nende sotsiaalse käitumisega erinevates kontekstides. Vähem usaldusväärseteks peetavate elanike saadud punktisummat kasutatakse nn musta nimekirja kandmiseks, st riiklike toetuste äravõtmiseks, muude raskete karistusmeetmete võtmiseks ja tugevdatud kontrolliks või järelevalveks. Hindamisel võetakse arvesse muu hulgas ebapiisavat vabatahtlikku tegevust ja väiksemaid korrarikkumisi, näiteks raamatute hilist tagastamist raamatukogusse, prügi jätmist tänavale, kui ei ole prügikonteinerite tühjendamise päev, ja kohalike maksude maksimisega viivitamist.

Neid lubamatuid sotsiaalpunktide andmise tavasid võib eristada seaduslikest tavadest, mille puhul hinnatakse isikuid õiguspärasel konkreetsetel eesmärgil kooskõlas liidu ja riigisisese õigusega, eelkõige juhul, kui sellised õigusaktid tagavad, et kahjustav või ebasoodne kohtlemine on põhjendatud ja proportsionaalne, võrreldes sotsiaalse käitumisega (vt punkti 4.3 kohaldamisalast välja jäävate olukordade kohta).

- (168) Mõlemad tehisintellektimääruse artikli 5 lõike 1 punkti c alapunktide i ja ii kohased alternatiivid võivad olla täidetud ka samaaegselt.

Näited põhjendamatu või eproportsionaalsest kohtlemisest vastavalt tehisintellektimääruse artikli 5 lõike 1 punkti c alapunktidele i ja ii:

- maksuhaldur kasutab tehisintellektisüsteemi lapsetoetuste pettuse avastamiseks, tehes profiilianalüüsi ja liigitades pettuses kahtlustatavad abisaajad sellistesse kategooriatesse nagu „tahtlik kavatsus / raske hooletus“, kasutades selliseid

kriteeriume nagu väike sissetulek, topeltkodakondsus, sotsiaalne käitumine jne. Riskipunkti alusel kontrollitakse abisaaja toimikut ja paljudel juhtudel lõpetatakse talle lapsehooldustoetuse maksmine, ta saab teate saadud hüvitise tagastamise kohta ning ta ei vasta enam tavapärase võlgade sissenõudmise korra nõuetele. Selline punktide andmine tekitab paljudele peredele suure võlakoormuse ning viib üksikisikute ja üksikisikute rühmade ebaõiglase, diskrimineeriva ja kahjuliku kohtlemise,¹²⁴ mis toob paljudele peredele kaasa suured rahalised raskused;

- ametiasutus kasutab õpilaskodu toetuse andmise protsessis pettuste kontrollimiseks tehisintellektisüsteemi, mis võtab näitajate hulgas arvesse internetiühendust, perekonnaseisu või abisaajate haridustaset kui pettuse riski eristavaid tegureid, mis ei tundu olevat asjakohased ega õigustatud;
- valitsus võtab kasutusele tervikliku tehisintellektil põhineva süsteemi, mis jälgib ja hindab kodanikke nende käitumise põhjal erinevates eluvaldkondades, näiteks sotsiaalses suhtluses, veebitegevuses, ostuharjumustes ja arvete õigeaegses tasumises. Väiksema punktisummaga inimestel on piiratud juurdepääs avalikele teenustele, kõrgemad laenuintressid ning raskused reisimisel, korterite üürimisel ja isegi töökoha leidmisel. Süsteem toob kaasa üksikisikute ülemäärase jälgimise ja ebasoodsa kohtlemise kontekstis, mis ei ole seotud sotsiaalse käitumisega, mida kasutatakse sotsiaalpunktide andmiseks (nt töövõimalusi mõjutab sotsiaalmeedia aktiivsus), ning kehtestab samal ajal ülemääraseid karistusi väiksemate rikkumiste eest (nt tekitab suhteliselt väikeste õigusrikkumiste pärast sotsiaalset ja rahalist kahju).

Neid vastuvõetamatuid sotsiaalpunktide andmise tavasid võib eristada seaduslikest tavadest, millega hinnatakse isikuid õiguspärasel konkreetsetel eesmärgil, mis ei vasta nende tingimustele ja on kooskõlas liidu ja riigisisese õigusega, eelkõige kui sellised õigusaktid tagavad, et kahjustav või ebasoodne kohtlemine on põhjendatud ja proportsionaalne ning et kasutatakse andmeid seotud sotsiaalsest kontekstist (vt punkti 4.3 kohaldamisalast välja jäävate olukordade kohta).

- (169) Tehisintellektimääruse artikli 5 lõike 1 punktis c sätestatud keeld võib hõlmata ka juhtumeid, kus teatavatele isikutele või isikute rühmadele antakse soodustusi või kohaldatakse nende suhtes eeliskohtlemist, kuna see tähendab teiste isikute ebasoodsamat kohtlemist (nt tööhõiveprogrammide toetamise, eluaseme või ümberasustamise (de-)prioriseerimise puhul).

4.2.3. Sõltumata sellest, kas neid pakuvad või kasutavad avaliku või erasektori osalejad

- (170) Nagu juba märgitud, keelab tehisintellektimääruse artikli 5 lõike 1 punkt c lubamatud tehisintellektipõhised sotsiaalpunktide andmise tavad, olenemata sellest, kas tehisintellektisüsteemi või sotsiaalpunkte pakuvad või kasutavad avaliku või erasektori osalejad. Kui avalikus sektoris võib punktide andmisel olla inimestele väga olulisi

¹²⁴ Samalaadse näite jaoks vt Hollandi lapsehooldustoetuste skandaali kohta, „[Belastingdienst treft 232 gezinnen met onevenredig harde actie](#)“ (hollandi keeles), 27.11.2019. Hollandi kohus otsustas 2020. aastal, et riskinäitajate süsteem (Systeem Risico Indicatie) oli ebaseaduslik. Vt ka [Geen powerplay maar fair play. Onevenredig harde aanpak van 232 gezinnen met kinderopvangtoeslag](#), 2017, lk 32.

tagajärgi, mis tulenevad võimu tasakaalustamatusest ja sõltuvusest avalikest teenustest, võivad sarnased kahjulikud tagajärjed tekkida ka erasektoris, kus punktide andmise tavasid rakendavad üha enam ka ettevõtted ja muud üksused.

Näiteks:

- kindlustusandja kogub pangalt teavet kulutuste kohta ja muud finantsteavet, mis ei ole seotud elukindlustuse taotlejate kindlustuskõlblikkuse määramisega ja mida kasutatakse sellise kindlustuse eest makstava kindlustusmakse summa kindlaksmääramiseks. Tehisintellektisüsteem analüüsib seda teavet ja soovitab selle põhjal, kas keelduda lepingu sõlmimisest või kehtestada konkreetsele isikule või kliendirühmale suuremad elukindlustusmaksed;
- erasektori krediidiagentuur kasutab tehisintellektisüsteemi, et määrata inimeste krediidivõimelisust ja otsustada, kas isik peaks saama eluasemelaenu, tuginedes mitteseotud isikuomadustele.

Neid vastuvõetamatuid sotsiaalpunktide andmise tavasid võib eristada seaduslikest tavadest, millega hinnatakse isikuid konkreetsetel seaduslikel eesmärkidel, mis ei vasta nendele tingimustele ja on kooskõlas liidu ja riigisisese õigusega, eelkõige kui sellised õigusaktid tagavad, et kahjustav või ebasoodne kohtlemine on põhjendatud ja proportsionaalne ning et kasutatakse seotud sotsiaalses kontekstis kogutud andmeid (vt punkti 4.3 kohaldamisalast välja jäävate olukordade kohta).

- (171) Pädevate turujärelevalveasutuste tehtava kontrolli puhul on tehisintellektisüsteemi pakkujal ja juurutajal oma kohustuste raames kohustus tõendada, et tehisintellekti kasutusviis on seaduslik ja põhjendatud, sealhulgas tehisintellektisüsteemi toimimise läbipaistvuse ning andmete ja andmeallikate liikide kohta teabe esitamise kaudu, tagades, et hindamise või liigitamise eesmärgil töödeldakse ainult andmeid, mis on seotud sotsiaalse kontekstiga, milles punktisummat kasutatakse, et süsteem toimib eesmärgipäraselt ja et sellest tulenev kahjustav või ebasoodne kohtlemine on põhjendatud ja sotsiaalse käitumisega võrreldes proportsionaalne. Kohaldatavate õigusaktide järgimine ning süsteemi sisseehitatud ja selle toimimise ajal kohaldatavad asjakohased ja proportsionaalsed kaitsemeetmed aitavad vältida keelu kohaldamist, võimaldades samal ajal kasutada tehisintellektisüsteeme isikute hindamiseks või liigitamiseks seaduslikel ja kasulikel eesmärkidel (nt protsesside tõhususe, teenuse kvaliteedi, ohutuse jms parandamine) (vt punkti 4.3 kohaldamisalast välja jäävate olukordade kohta).
- (172) Suure riskiga tehisintellektisüsteemide nõuete täitmine (nt oluliste avalike teenuste ja hüvitiste, krediidihindamise ja krediidivõimelisuse hindamise, rände jms valdkonnas) võib samuti aidata tagada, et nendes suure riskiga valdkondades hindamiseks ja liigitamiseks kasutatavad tehisintellektisüsteemid ei rakenda vastuvõetamatuid sotsiaalpunktide andmise tavasid, mida pakkujad ja juurutajad peaksid oma vastavate kohustuste (nt riskijuhtimine, läbipaistvus, andmehaldus, põhiõigustele avalduva mõju hindamine, inimjärelevalve, järelevalve jne) täitmisel arvesse võtma.

4.3.Kohaldamisalast välja jäävad olukorrad

- (173) Tehisintellektimääruse artikli 5 lõike 1 punktis c sätestatud keeld kehtib ainult füüsiliste isikute või isikute rühmade hindamisele, mistõttu on põhimõtteliselt välistatud juriidiliste isikute hindamine, kui hindamine ei põhine üksikisikute isiku- või iseloomuomadustel või sotsiaalsel käitumisel, isegi kui mõnel juhul võib punktide andmine üksikisikuid kaudselt mõjutada (nt kõiki valla kodanikke eelarve jaotamise korral). Kui aga juriidilisi isikuid on hinnatud üldise hinde alusel, milles on võetud kokku füüsiliste isikute rühma hindamine või liigitamine nende sotsiaalse käitumise või isiksuse- või isikuomaduste alusel, ja see hinne mõjutab otseselt neid isikuid (nt kõik ettevõtte töötajad, konkreetse kooli õpilased, kelle käitumist on hinnatud), võib see tegevus kuuluda tehisintellektimääruse artikli 5 lõike 1 punkti c kohaldamisalasse, kui kõik muud tingimused on täidetud. See eeldab iga juhtumi eraldi hindamist.
- (174) Tehisintellektipõhist sotsiaalpunktide andmist kui „tõenäosusväärtust“ ja prognoosi tuleks eristada kasutajate antavatest individuaalsetest hinnangutest, millega hinnatakse teenuse kvaliteeti (näiteks autojuhi hindamist veebipõhisel autojagamisplatvormil või majutuskoha hindamist veebipõhisel majutusplatvormil). Sellised hinnangud kujutavad endast pelgalt inimeste antud üksikhinnangute koondamist, mis ei pruugi hõlmata tehisintellekti, välja arvatud juhul, kui andmeid kombineeritakse muu teabega ja analüüsitakse tehisintellektisüsteemi poolt, et hinnata või liigitada isikuid, kes vastavad kõigile tehisintellektimääruse artikli 5 lõike 1 punktis c sätestatud tingimustele.
- (175) Lisaks sellele ei ole füüsilistele isikutele punktide andmine keelatud mitte alati, vaid ainult piiratud juhtudel, kui kõik tehisintellektimääruse artikli 5 lõike 1 punkti c tingimused on kumulatiivselt täidetud, nagu eespool analüüsitud. Tehisintellektimääruse põhjenduses 31 on öeldud, et „keeld ei tohiks mõjutada füüsiliste isikute seaduslikku hindamist, mida tehakse konkreetsel eesmärgil kooskõlas liidu või liikmesriigi õigusega“. Näiteks krediidihindang, riskide hindamine ja krediidiriskide hindamine on finants- ja kindlustusettevõtete pakutavate teenuste olulised aspektid. Sellised kasutusviisid, nagu ka muud õiguspärased kasutusviisid (st teenuste kvaliteedi ja tõhususe parandamiseks, nõuete tõhusama käsitlemise tagamiseks, konkreetsete töötajate hindamiseks, pettuste ennetamiseks ja avastamiseks, õiguskaitseks või kasutajate käitumisele punktide andmiseks digiplatvormidel), ei ole iseenesest keelatud, kui need on seaduslikud ja toimuvad kooskõlas tehisintellektimääruse ja muu kohaldatava liidu ja riigisisese õigusega, mis peab olema kooskõlas liidu õigusega.
- (176) Teisisõnu ei ole keelatud tehisintellektisüsteemid, mis hindavad või liigitavad isikuid sotsiaalpunktide andmiseks seaduslikul viisil ja konkreetsel eesmärgil samas kontekstis, kus punktide andmiseks kasutatud isikuandmeid koguti, tingimusel et punktide kasutamisest tulenev kahjustav või ebasoodne kohtlemine on õigustatud ja sotsiaalse käitumise kaalukusega võrreldes proportsionaalne¹²⁵.
- (177) Vastavus valdkondlikele liidu õigusaktidele, näiteks krediidihindamise, rahapesuvastase võitluse jms valdkonnas, milles täpsustatakse, millist liiki andmete kasutamine konkreetse õiguspärase hindamise eesmärgi saavutamiseks on asjakohane

¹²⁵

Tehisintellektimääruse põhjendus 31.

ja vajalik, ning tagatakse, et kohtlemine on õigustatud ja sotsiaalse käitumisega võrreldes proportsionaalne, võib seega tagada, et tehisintellekti kasutusviis jääb väljapoole tehisintellektimääruse artikli 5 lõike 1 punktis c sätestatud keelu kohaldamisala.

Näited liidu ja riigisisese õigusega kooskõlas olevatest õiguspärasest hindamistavadest, mis ei kuulu tehisintellektimääruse artikli 5 lõike 1 punkti c kohaldamisalasse:

- finantsvaldkonna krediidihindamissüsteemid, mida krediidiandjad või krediidiinfoasutused kasutavad kliendi rahalise krediitvõimelisuse või tasumata võlgade hindamiseks, krediidihindamiseks või krediitvõimelisuse kindlaksmääramiseks ning mis põhinevad kliendi sissetulekutel ja kulutustel ja muudel finants- ja majandusoludel, ei kuulu tehisintellektimääruse artikli 5 lõike 1 punkti c kohaldamisalasse, kui need on krediidihindamise õiguspärase eesmärgi jaoks asjakohased ja kui need vastavad tarbijakaitseadustele,¹²⁶ milles on täpsustatud andmete liik ja vajalikud kaitsemeetmed, et tagada tarbijate õiglane kohtlemine krediitvõimelisuse hindamisel;
- ettevõtetel on õigustatud huvi hinnata kliente finantspettuste suhtes ja neid kasutusviise keeld ei mõjuta, kui hindamine põhineb asjakohastel andmetel, nagu tehingukäitumine ja metaandmed teenuste kontekstis, varasem ajalugu ja muudest allikatest pärit tegurid, mis on pettuse riski kindlaksmääramiseks objektiivselt asjakohased, ning kui pettuse tagajärjel toimuv kahjulik kohtlemine on põhjendatud ja proportsionaalne;
- telemaatikaseadmete abil kogutud teavet, mis näitab, et juht ületab sõidukiirust või ei järgi ohutuid sõiduviise, mida kindlustusandja, kes pakub telemaatikapõhiseid tariife seoses kindlustusvõtja riskantse sõiduviisiga, võib kasutada kindlustusvõtja kindlustusmakse suurendamiseks, kuna selle sõiduviisiga kaasneb suurem õnnetusjuhtumi risk, tingimusel et kindlustusmakse suurendamine on juhi riskantse sõiduviisiga võrreldes proportsionaalne;
- selliste andmete kogumine ja töötlemine, mis on tehisintellektisüsteemide kavandatud õiguspärase eesmärgi saavutamiseks asjakohased ja vajalikud (nt erinevatest allikatest kogutud andmed tervise ja skisofreenia kohta, mida kasutatakse patsientide diagnoosimiseks), ei kuulu tehisintellektimääruse artikli 5 lõike 1 punkti c kohaldamisalasse, eelkõige kuna sellega töödeldakse asjakohaseid ja vajalikke andmeid ning sellega ei kaasne tavaliselt teatavate füüsiliste isikute põhjendamatu kahjustav või ebasoodne kohtlemine;
- veebiplatvormid, mis teevad ohutuse tagamiseks oma teenuste kasutajate profiilialüüse, kasutades andmeid, mis on hindamise kontekstis ja eesmärgil asjakohased, ei kuulu tehisintellektimääruse artikli 5 lõike 1 punkti c

¹²⁶

Vt eelkõige 18. oktoobri 2023. aasta direktiiv (EL) 2023/2225, mis käsitleb tarbijakrediitilepinguid ja millega tunnistatakse kehtetuks direktiiv 2008/48/EÜ, ning Euroopa Pangandusjärelevalve suunised laenude väljastamise ja jälgimise kohta, 29. mai 2020, EBA/GL/2020/06.

kohaldamisalasse, kui hindamine ei too kaasa ebasoodsat kohtlemist, mis on kasutaja korrarikkumise kaalukusega võrreldes eaproportsionaalne;

- tehisintellektipõhine sihtotstarbeline kommertsreklaam ei kuulu kohaldamisalasse, kui see põhineb asjakohastel andmetel (nt kasutajate eelistused), kui see on kooskõlas liidu tarbijakaitse, andmekaitse ja digiteenuste alaste õigusaktidega ning kui see ei too kaasa kahjustavat või ebasoodsat kohtlemist, mis on kasutaja sotsiaalse käitumise kaalukusega võrreldes eaproportsionaalne (nt ekspluateeriv ja ebaõiglane diferentseeritud hinnakujundus);
- keeld ei mõjuta tehisintellektisüsteeme, mis kasutavad pagulaslaagrites kogutud andmeid (nt käitumise vastavus) ümberasustamise või tööhõive otsuste tegemiseks, tingimusel et need andmed on hindamise eesmärgil asjakohased ja et on täidetud liidu kohaldatava rändeõiguse kohased menetlused, mis tagavad, et kohtlemine on õigustatud ja proportsionaalne;
- veebipõhise ostuplatvormi tehisintellektipõhine punktide andmine, mis pakub eeliseid kasutajatele, kes on ostnud palju ja tagastanud vähe tooteid, näiteks kiirem tagastamisprotsess või raha tagastamine ilma kauba tagastamiseta, ei kuulu tehisintellektimääruse artikli 5 lõike 1 punkti c kohaldamisalasse, kuna need eelised on positiivse käitumise premeerimiseks põhjendatud ja proportsionaalsed ning teistele kasutajatele on jätkuvalt kättesaadav tavapärane tagastamisprotsess;
- politsei ja muude õiguskaitseasutuste tehtav üksikisikute tehisintellekti põhine hindamine ja neile punktide andmine, mille jaoks kogutakse andmeid üksikisikute sotsiaalse käitumise kohta mitmest kontekstist, ei kuulu tehisintellektimääruse artikli 5 lõike 1 punkti c kohaldamisalasse, kui need andmed on asjakohased kuritegude ennetamise, avastamise, menetlemise ja nende eest vastutusele võtmise konkreetsetel eesmärkidel ning kui kahjulik kohtlemine on põhjendatud ja proportsionaalne kooskõlas liidu materiaalse ja menetlusõigusega ning liikmesriigi kriminaal- ja politseiõigusega. Selles kontekstis on asjakohane kaaluda ka tehisintellektimääruse artikli 5 lõike 1 punktis d sätestatud keeldu, mis seab tehisintellektipõhistele riskihindamistele ja kuriteo toimepanemise tõenäosuse prognoosidele täiendavad ja täpsemad tingimused, mis ei tohi põhineda üksnes profiilianalüüsil või iseloomuomaduste hindamisel (vt punkt 5).

4.4. Koostoime teiste liidu õigusaktidega

- (178) Pakkujad ja juurutajad peaksid hoolikalt hindama, kas nende tegevuses kasutatava tehisintellektipõhise punktide andmise süsteemi suhtes kohaldatakse muid kohaldatavaid liidu ja riigisiseseid õigusakte, eelkõige seda, kas on olemas konkreetsemad õigusaktid, mis reguleerivad rangelt, milliste andmete kasutamine konkreetsetel hindamiseesmärkidel on asjakohane ja vajalik, ning kas on olemas konkreetsemad õigusnormid ja menetlused, mis tagavad õigustatud ja õiglase kohtlemise.
- (179) Tehisintellektipõhine sotsiaalpunktide andmine eraõiguslike isikute poolt, kes tegutsevad ettevõtjatena ettevõtjate ja tarbijate vahelistes suhetes, võib samuti olla

vastuolus liidu tarbijakaitsealaste õigusaktidega, st direktiiviga 2005/29/EÜ, mis käsitleb ettevõtja ja tarbija vaheliste tehingutega seotud ebaausaid kaubandustavasid (ebaausate kaubandustavade direktiiv). Ebaausate kaubandustavade direktiiv keelab kaubandustavad, kui need on vastuolus ametialase hoolikuse nõuetega ja moonutavad oluliselt või võivad oluliselt moonutada keskmise tarbija või tarbijarühma keskmise liikme majanduskäitumist seoses tootega (ebaausate kaubandustavade direktiivi artikkel 5). Samuti võib punktide andmise tavasid pidada eksitavaks (ebaausate kaubandustavade direktiivi artiklid 6–7), kui iga üksikjuhtumi puhul hinnatakse kaubandustava mõju tarbija tehinguotsusele.

- (180) Sotsiaalpunktide andmine, kas avaliku või erasektori poolt, võib samuti olla vastuolus liidu andmekaitsealaste õigusaktidega, näiteks seoses töötlemise õigusliku alusega (seaduslikkus), andmekaitsepõhimõtetega (nt võimalikult väheste andmete kogumine ja vajalikkus, õiglus, läbipaistvus) ja muude kohustustega, sealhulgas vajaduse korral üksnes automatiseeritud individuaalset otsustamist käsitlevate õigusnormidega.
- (181) Kui hindamine või liigitamine põhineb ühel diskrimineerimise eest kaitstud põhjusel (nt vanus, usutunnistus, rassiline või etniline päritolu, sugu jne) või toob otseselt või kaudselt kaasa nende rühmade diskrimineerimise, kohaldatakse sellise tegevuse suhtes samuti liidu diskrimineerimisvastast õigust.
- (182) Selles kontekstis võib olla asjakohane ka tarbijakrediidi direktiiv (EL) 2023/2225¹²⁷. Tarbijakrediidi direktiivi artikli 18 lõikes 3 on nõutud, et krediitdivõimelisuse hindamisel tuginetaks tarbija sissetulekut ja kulutusi ning muud rahalist ja majanduslikku olukorda käsitlevale asjakohasele ja täpsele teabele, mis on vajalik ja proportsionaalne krediidi liigi, kestuse, väärtuse ja krediidist tarbijale tulenevate riskidega. Kõnealune teave võib hõlmata tõendeid sissetuleku või tagasimaksete muude allikate kohta, teavet finantsvarade ja -kohustuste kohta või teavet muude rahaliste kohustuste kohta. Tarbijakrediidi direktiiv keelab selgesõnaliselt isikuandmete eriliigiliste kategooriate lisamise ja teabe saamise sotsiaalvõrgustikest. Euroopa Pangandusjärelevalve suunistes laenude andmise ja järelevalve kohta¹²⁸ kirjeldatakse täpsemalt krediitdivõimelisuse hindamiseks vajalikku teavet. Nendes sektoripõhistes õigusaktides esitatud kirjeldused selle kohta, millist liiki andmeid konkreetse hindamise eesmärgil kasutatakse, on oluline punkt, mida võtta arvesse selle määramisel, kas kasutusviis jääb tehisintellektimääruse artikli 5 lõike 1 punktis c kirjeldatud keelu kohaldamisalasse.
- (183) Samamoodi peaksid ka tehisintellektisüsteemid, mida kasutatakse isikute hindamiseks ja liigitamiseks rahapesu ja terrorismi rahastamise vastase võitluse eesmärgil, vastama asjaomastele liidu õigusaktidele.

5. TEHISINTELLEKTIMÄÄRUSE ARTIKLI 5 LÕIKE 1 PUNKT D – KURITEGUDE PROGNOOSIMINE JA INDIVIDUAALNE RISKIANALÜÜS

¹²⁷ Euroopa Parlamendi ja nõukogu 23. aprilli 2008. aasta direktiiv 2008/48/EÜ, mis käsitleb tarbijakrediidilepinguid ja millega tunnistatakse kehtetuks nõukogu direktiiv 87/102/EMÜ (ELT L 133, 22.5.2008, lk 66–92).

¹²⁸ Euroopa Pangandusjärelevalve, suunistes laenude väljastamise ja jälgimise kohta, 29. mai 2020, EBA/GL/2020/06.

- (184) Tehisintellektimääruse artikli 5 lõike 1 punktis d on keelatud tehisintellektisüsteemid, mis hindavad või prognoosivad riski, et füüsiline isik paneb toime kuriteo, tuginedes üksnes füüsilise isiku profiilianalüüsile või tema isikuomaduste ja erijoonte hindamisele.
- (185) Sätte viimases lauses märgitakse, et keeldu ei kohaldata tehisintellektisüsteemide suhtes, mida kasutatakse selleks, et toetada inimhinnangut isiku kuritegelikus tegevuses osalemise kohta, mis juba tugineb sellise tegevusega otseselt seotud objektiivsetele ja kontrollitavatele faktidele. Tehisintellektisüsteemid, mis ei kuulu keelu kohaldamisalasse, on ette nähtud kasutamiseks õiguskaitseasutuste poolt või nende nimel või õiguskaitseasutusi toetavate liidu institutsioonide, organite, asutuste või ametite poolt, et hinnata füüsilise isiku õigusrikkumise või korduva õigusrikkumise riski mitte üksnes profiilianalüüsi või isikuomaduste ja erijoonte või varasema kriminaalse käitumise hindamise alusel, liigitatakse suure riskiga tehisintellektisüsteemideks (III lisa punkti 6 alapunkt d) ning need peavad vastama kõigile tehisintellektimääruse kohastele asjakohastele nõuetele ja kohustustele.

5.1. Põhjendus ja eesmärgid

- (186) Tehisintellektimääruse põhjenduses 42 selgitatakse artikli 5 lõike 1 punktis d sätestatud keelu tausta ja põhjendusi, nimelt seda, et füüsiliste isikute üle tuleks otsustada nende tegeliku käitumise, mitte tehisintellekti prognoositava käitumise alusel, mis põhineb üksnes nende profiilianalüüsil, isikuomadustel või erijoontel.

5.2. Keelu põhimõisted ja komponendid

Tehisintellektimääruse artikli 5 lõike 1 punktis d on sätestatud:

„Järgmised tehisintellekti kasutusviisid on keelatud:

d) tehisintellektisüsteemide turule laskmine või kasutusele võtmine sellel konkreetsel eesmärgil või nende kasutamine füüsiliste isikute riskihindamiste tegemiseks, et hinnata või prognoosida riski, et füüsiline isik paneb toime kuriteo, tuginedes üksnes füüsilise isiku profiilianalüüsile või tema isikuomaduste ja erijoonte hindamisele; seda keeldu ei kohaldata tehisintellektisüsteemide suhtes, mida kasutatakse selleks, et toetada inimhinnangut isiku kuritegelikus tegevuses osalemise kohta, mis juba tugineb kuritegeliku tegevusega otseselt seotud objektiivsetele ja kontrollitavatele faktidele;“.

- (187) Selleks, et tehisintellektimääruse artikli 5 lõike 1 punktis d sätestatud keeld oleks kohaldatav, peavad olema täidetud mitu kumulatiivset tingimust:
- (i) kasutusviis peab kujutama endast tehisintellektisüsteemi turule laskmist, kasutusele võtmist sel konkreetsel eesmärgil või kasutamist;
 - (ii) tehisintellektisüsteem peab tegema riskihinnanguid, et hinnata või prognoosida riski, et füüsiline isik paneb toime kuriteo;
 - (iii) riskihinnang või prognoos peab põhinema üksnes ühel või mõlemal järgmistest asjaoludest:
 - (a) füüsilise isiku profiilianalüüs;

(b) füüsilise isiku isikuomaduste ja erijoonte hindamine.

- (188) Keelu kohaldamiseks peavad kõik kolm tingimust olema samal ajal täidetud. Esimest tingimust, st tehisintellektisüsteemi turule laskmist, kasutusele võtmist või kasutamist, on juba analüüsitud punktis 2.3. Keeld kehtib seega nii tehisintellektisüsteemide pakkujate kui ka juurutajate suhtes, kes on oma vastutuse piires kohustatud selliseid süsteeme sel konkreetsel eesmärgil mitte turule laskma, kasutusele võtma ega kasutama. Allpool analüüsitakse teist kaht tingimust, mida keelu kohaldamiseks vaja on.

5.2.1. Kuriteo toimepanemise riski hindamine või prognoosimine

- (189) Riskihinnanguid, mille eesmärk on hinnata või prognoosida üksikisiku kuritegude toimepanemise riski, nimetatakse sageli individuaalseks „kuriteoproгноosiks“. Ehkki kuriteoproгноoside jaoks puudub üldkehtiv määratlus,¹²⁹ viitavad need mõisted üldiselt mitmesugustele arenenud tehisintellekti tehnoloogiatele ja analüüsimeetoditele, mida rakendatakse suure hulga sageli varasemate andmete (sealhulgas sotsiaal-majanduslike andmete, aga ka politseiregistrite jms) suhtes, mida kasutatakse koos kriminoloogiliste teooriatega kuritegevuse prognoosimiseks, mille alusel töötatakse välja politsei ja õiguskaitse strateegiad ja meetmed kuritegevuse vastu võitlemiseks ning selle kontrolli all hoidmiseks ja ennetamiseks¹³⁰.
- (190) Kuritegevuse prognoosimiseks mõeldud tehisintellektisüsteemid tuvastavad varasemates andmetes mustreid, seostavad näitajaid kuriteo toimumise tõenäosusega ja koostavad seejärel väljundina riski kohta punktisummad, mida saab kasutada prognoosimiseks. Selliseid süsteeme võib kasutada näiteks politseioperatsioonide kavandamiseks, suure riskiga olukordade jälgimiseks ja tõenäoliste (korduvate) kurjategijate kontrollimiseks. Sellised süsteemid pakuvad võimalusi õiguskaitseasutustele, eriti neile, kellel on napid ressursid, suurendades tõhusust ja võimaldades ennetavat käsitusviisi kuritegude avastamiseks, ärahoidmiseks ja ennetamiseks¹³¹. Selline varasemate kuritegude kohta käivate andmete kasutamine selleks, et prognoosida teiste isikute käitumist tulevikus, võib siiski korrata või isegi tugevdada eelarvamusi ning võib viia oluliste individuaalsete asjaolude tähelepanuta jätmiseni, kui need asjaolud ei ole osa andmekogumist või neid ei ole arvesse võetud algoritmides, mille alusel konkreetne tehisintellektisüsteem töötab. See võib ka õõnestada üldsuse usaldust õiguskaitseasutuste ja õigussüsteemi vastu üldiselt¹³².
- (191) Sellised riskihinnangud ja prognoosid on põhimõtteliselt tulevikku suunatud ja puudutavad tulevasi (veel toime panemata) kuritegusid või kuritegusid, mille toimepanemise ohtu hinnatakse konkreetsel hetkel, sealhulgas kuriteo toimepanemise

¹²⁹ Vt näiteks ELi Põhiõiguste Ameti käsiraamatus viidatud süsteemid, nagu Criminality Awareness System (CAS) Madalmaades ning Precobs Saksamaal ja Šveitsis, käsiraamat, 2018, lk 138. [Seadusliku aluseta profiilide koostamise tõkestamine nüüd ja tulevikus: juhend](#), käsiraamat, 2018, lk 138.

¹³⁰ Vt Europol, AI and policing The benefits and challenges of artificial intelligence for law enforcement, Europol'i innovatsioonilabori seirearuanne, 23. september 2024. Vt ka F. Yang, „Predictive Policing“, *Oxford Research Encyclopedia, Criminology and Criminal Justice*, Oxford University Press, 2019.

¹³¹ Näiteks OxRec (Hollandi kriminaalhooldusamet, „Reclassering Nederland“) [Prediction of violent reoffending in prisoners and individuals on probation: a Dutch validation study \(OxRec\)](#), PMC (nih.gov).

¹³² Vt nt Euroopa Põhiõiguste Amet, 8. detsember 2022, Bias in algorithms – Artificial intelligence and discrimination.

katse või ettevalmistava tegevuse puhul¹³³. Neid võib teha igas õiguskaitsetegevuse etapis, näiteks kuritegude ennetamise ja avastamise ajal, aga ka uurimise, nende eest vastutusele võtmise ja kriminaalkaristuse täitmisele pööramise ajal (sealhulgas siis, kui õigusasutused hindavad õigusrikkumise kordumise ohtu, nt seoses otsuste tegemisega eelvangistuse rakendamise kohta), samuti osana üksikisikute ühiskonda taastintegreerimise kavast pärast kriminaalkaristuse kandmist¹³⁴.

- (192) Tehisintellektimääruse artikli 5 lõike 1 punktis d sätestatud keeld ei keela kuritegude prognoosimist ja riskihindamist kui sellist. Seda kohaldatakse ainult tehisintellektisüsteemide suhtes, mille abil hinnatakse või prognoositakse füüsilise isiku kuriteo toimepanemise riski, kui täidetud on ka kolmas eespool nimetatud tingimus. Lisaks, nagu märgitud, ei kohaldata keeldu olukordades, mida on kirjeldatud tehisintellektimääruse artikli 5 lõike 1 punkti d viimases lauses sisalduvas selgesõnalises erandis.

5.2.2. Üksnes füüsilise isiku profiilialalüüsil või tema isikuomaduste ja erijoonte hindamisel põhinev tegevus

- (193) Kolmas tingimus, et tehisintellektimääruse artikli 5 lõike 1 punktis d sätestatud keeld oleks kohaldatav, on see, et riskihindamine, mille eesmärk on hinnata või prognoosida füüsilise isiku riski panna toime kuritegu, peab põhinema üksnes a) isiku profiilialalüüsil või b) tema isikuomaduste ja erijoonte hindamisel.
- (194) Tehisintellektimääruse artikli 5 lõike 1 punktis d sätestatud keeldu kohaldatakse sõltumata sellest, kas tehisintellektisüsteem teeb üheainsa füüsilise isiku või mitme füüsilise isiku profiilialalüüsi(d) või hindab tema (nende) isikuomadusi ja erijooni samal ajal, kuna keelu eesmärk on kaitsta iga isikut, kelle puhul prognoositakse või hinnatakse kuriteo toimepanemise riski.

a) Füüsilise isiku profiilialalüüs

- (195) Erinevalt tehisintellektimääruse artikli 5 lõike 1 punktist c kasutatakse artikli 5 lõike 1 punktis d sõnaselgelt mõistet „profiilialalüüs“. Tehisintellektimääruse artikli 3 punktis 52 on see mõiste määratletud viitega selle määratlusele isikuandmete kaitse üldmääruse artikli 4 punktis 4¹³⁵. Profiilialalüüsi mõiste üks põhielemente on eesmärk „hinnata teatavaid isiklikke aspekte“¹³⁶. Tehisintellektimääruse artikli 5 lõike 1

¹³³ Vt sellega seoses tehisintellektimääruse põhjendust 42, milles viidatakse nende rikkumiste tõenäosusele ning tegeliku või potentsiaalse kuriteo toimepanemisele, kusjuures neile viidatakse olevikus, mitte minevikus.

¹³⁴ Näiteks direktiivi 2011/93/EL (mis käsitleb laste seksuaalse kuritarvitamise ja ärakasutamise ning lasteporno vastast võitlust) artikli 24 lõikes 4 on nõutud, et isikute puhul, kelle suhtes on algatatud kriminaalmenetlus seoses lapse seksuaalse väärkohtlemisega või kes on selles süüdi mõistetud, tuleb hinnata nende süütegude kordumise riski.

¹³⁵ Õiguskaitse direktiivi artikli 3 punktis 4, mis on asjakohane tehisintellektimääruse artikli 5 lõike 1 punktis d sätestatud keelu puhul, on profiilialalüüs määratletud samamoodi nagu isikuandmete kaitse üldmääruse artikli 4 punktis 4: „igasugune isikuandmete automatiseeritud töötlemine, mis hõlmab isikuandmete kasutamist füüsilise isikuga seotud teatavate isiklike aspektide hindamiseks, eelkõige selliste aspektide analüüsimiseks või prognoosimiseks, mis on seotud kõnealuse füüsilise isiku töötulemuste, majandusliku olukorra, tervise, isiklike eelistuste, huvide, usaldusväärsuse, käitumise, asukoha või liikumisega“. Sama määratlus on esitatud ka määruse (EL) 2018/1725 (isikuandmete töötlemise kohta liidu institutsioonides, organites ja asutustes) (ELT L 295, 21.11.2018, lk 39) artikli 3 lõikes 5.

¹³⁶ Vt ka artikli 29 alusel asutatud andmekaitse töörihm, suunised automatiseeritud töötlusel põhinevate üksikotsuste tegemise ja profiilialalüüsi kohta määruse 2016/679 kohaldamisel, 6. veebruar 2018, WP251rev.01, mille on heaks kiitnud ka Euroopa Andmekaitse nõukogu, lk 7. Vt ka Põhiõiguste Amet, *Seadusliku alusega profiilide koostamise tõkestamine nüüd ja tulevikus: juhend*, käsiraamat, 2018, lk 138.

punkti d kontekstis tehakse profiilianalüüsi selleks, et hinnata või prognoosida isiku kuriteo toimepanemise riski.

- (196) Selles kontekstis võib olla asjakohane ka nn rühmaprofiili koostamise kontseptsioon¹³⁷. See mõiste viitab sellele, kui teatud rühma kohta koostatakse kirjeldav profiil ja rakendatakse seda, näiteks kuritegude toimepanijate kategooriad (nt terroristid, kurjategijate jõugu liikmed jne), mis on koostatud teiste isikute poolt varem toime pandud kuritegude kohta käivate ajalooliste andmete põhjal. Neid rühmaprofiile võib hiljem kasutada selleks, et hinnata ja prognoosida teiste isikute samalaadsete õigusrikkumiste toimepanemise riski. Kui tehisintellektisüsteem teeb prognoosi ja kohaldab sellist (rühma)profiili konkreetse isiku suhtes, kujutab see endast isiku profiilianalüüsi ja võib seega kuuluda tehisintellektimääruse artikli 5 lõike 1 punktis d sätestatud keelu kohaldamisalasse.

b) Isikuomaduste ja erijoonte hindamine

- (197) Keeld kehtib ka juhul, kui riskihindamine, mille eesmärk on hinnata või prognoosida isiku kuritegude toimepanemise riski, põhineb üksnes isiku isikuomaduste ja erijoonte hindamisel. Selline hindamine või prognoosimine kuulub sageli profiilianalüüsi mõiste alla, kuid seda võib käsitleda ka selle alternatiivina, kui isikuandmete kaitse üldmääruse artikli 4 punktis 4 määratletud profiilianalüüsi ei ole võimalik kindlaks teha.
- (198) Nagu on öeldud punktis 4.2.1,c, moodustavad isikuomadused ja erijooned konkreetse füüsilise isikuga seotud omaduste suure kategooria, mille jaoks puudub üldiselt kokku lepitud süsteem. Tehisintellektimääruse põhjenduses 42 tuuakse näiteid isikuomaduste ja erijoonte kohta, mida võib hinnata õigusrikkumise toimepanemise riski prognoosimiseks, nagu „rahvus, sünnikoht, elukoht, laste arv, võlatase või automark“. See on ainult illustratiivne loetelu, mis ei ole ammendav.

c) „Üksnes“

- (199) Tehisintellektimääruse artikli 5 lõike 1 punktis d on sätestatud, et selle sättega hõlmatud riskihindamine on keelatud üksnes juhul, kui need põhinevad „üksnes“ isiku profiilianalüüsil või tema isikuomaduste ja erijoonte hindamisel. Tehisintellektimääruse põhjendusest 42 selgub, et „üksnes“ on mõeldud kehtima nii profiilianalüüsi kui ka iseloomuomaduste ja erijoonte hindamise suhtes.
- (200) Tingimus, et riskihindamine peab tuginema „üksnes“ profiilianalüüsile või tema isikuomaduste ja erijoonte hindamisele, ei pruugi mitmesugustes olukordades olla täidetud.
- (201) Nagu nähtub tehisintellektimääruse artikli 5 lõike 1 punkti d viimasest lausest, tekib selline olukord igal juhul siis, kui tehisintellektisüsteemi kasutatakse selleks, et toetada inimhinnangut isiku kuritegelikus tegevuses osalemise kohta, mis juba tugineb sellise tegevusega otseselt seotud objektiivsetele ja kontrollitavatele faktidele. Nagu põhjendusest 42 selgub, tuleks selles kontekstis mõelda eelkõige olukorrale, kus

¹³⁷ Vt rühmaprofiili koostamise kohta nt Põhiõiguste Amet, *Seadusliku aluseta profiilide koostamise tõkestamine nüüd ja tulevikus: juhend*, käsiraamat, 2018, lk 21.

asjaomase füüsilise isiku suhtes on juba olemas põhjendatud kahtlus. Sellisel juhul on tavaliselt antud ka inimhinnang, mis tavaliselt põhineb asjakohastel objektiivsetel ja kontrollitavatel faktidel.

- (202) Siiski võib esineda ka muid olukordi, mida tuleb alati hinnata iga juhtumi puhul eraldi. Ühest küljest jätab sõna „üksnes“ kasutamine võimaluse, et riskihindamisel võetakse arvesse mitmesuguseid muid elemente, mis tähendab, et see ei põhine enam ainult profiilianalüüsil või isikuomaduste või erijoonte hindamisel. Teisest küljest, et vältida keelust kõrvalehoidmist ja tagada selle tõhusus, peavad kõik sellised muud elemendid olema tegelikud, olulised ja sisulised, et need õigustaksid järeldust, et keeld ei ole kohaldatav. Tehisintellektimääruse artikli 5 lõike 1 punktis d sätestatud keelu ja selle viimases lauses sisalduva erandi lugemine viitab sellele, et seda järeldust võib õigustada eelkõige teatavate eelnevalt kindlaks tehtud objektiivsete ja kontrollitavate asjaolude olemasolu.

Näiteks:

- õiguskaitseasutus kasutab tehisintellektisüsteemi, et prognoosida kuritegelikku käitumist selliste kuritegude puhul nagu terrorism, võttes aluseks üksnes isikute vanuse, kodakondsuse, aadressi, auto tüübi ja perekonnaseisu. Selles süsteemis peetakse teatud üksikisikute puhul üksnes nende isikuomaduste põhjal tõenäolisemaks, et nad panevad tulevikus toime õigusrikkumisi, mida nad ei ole veel toime pannud. Sellise süsteemi puhul võib eeldada, et see on tehisintellektimääruse artikli 5 lõike 1 punkti d kohaselt keelatud;
- riiklikud maksuametid kasutavad tehisintellekti prognoosimisvahendit, et vaadata läbi kõigi maksumaksjate maksudeklaratsioonid, et prognoosida võimalikke maksuõigusrikkumisi ja tuvastada edasist uurimist vajavaid juhtumeid. Seda tehakse üksnes tehisintellektisüsteemi poolt koostatud profiili alusel, mis kasutab hindamiseks iseloomuomadusi, nagu topeltkodakondsus, sünnikoht ja laste arv, ning läbipaistmatuid muutujaid, eelkõige tuletatud teavet, mis on prognoosiv ning järelikult mitteobjektiivne ja raskesti kontrollitav. Selline süsteem kuulub tavaliselt tehisintellektimääruse artikli 5 lõike 1 punktis d sätestatud keelu alla, kuna puudub põhjendatud kahtlus konkreetse isiku seotuse kohta kuritegeliku tegevusega või muud objektiivsed ja kontrollitavad faktid, mis seostaksid teda selle kuritegeliku tegevusega. See on näide, mis kuulub ka tehisintellektimääruse artikli 5 lõike 1 punktiga c keelatud sotsiaalpunktide andmise alla, mis hõlmab mitteseotud sotsiaalsest kontekstist pärit andmete põhjal toimuvat ebasoodsat kohtlemist;
- politseiamet kasutab tehisintellektipõhist riskihindamisvahendit, et hinnata noorte laste ja noorukite tulevaste vägivalla- ja varavastaste kuritegudega seotud riski. Süsteem võtab laste hindamisel aluseks suhted teiste inimesega ja nende eeldatava riskitaseme, mis tähendab, et lapsi võidakse pidada suurema kuriteoriskiga lasteks lihtsalt seetõttu, et nad on seotud mõne teise hinnangu järgi kõrge riskitasemega isikuga, näiteks õe või venna või sõbraga. Vanemate riskitase võib mõjutada ka lapse riskitaset. Riskihinnangute tulemusel registreerib politsei need lapsed oma süsteemis, jälgib neid lisakontrollide abil ja suunab nad noorsooteenuste juurde. Ka selline

süsteem kuulub tõenäoliselt tehisintellektimääruse artikli 5 lõike 1 punktis d sätestatud keelu alla.

5.2.3. Tehisintellektisüsteemide välistamine, et toetada inimhinnangut, mis põhineb objektiivsetel ja kontrollitavatel faktidel, mis on otseselt seotud kuritegeliku tegevusega

- (203) Tehisintellektimääruse artikli 5 lõike 1 punkti d viimases lauses on sätestatud, et keeldu ei kohaldata tehisintellektisüsteemide suhtes, mida kasutatakse selleks, et toetada inimhinnangut kuritegelikus tegevuses osalemise kohta, mis juba põhineb kuritegeliku tegevusega otseselt seotud objektiivsetel ja kontrollitavatel faktidel. Kuigi, nagu märgitud, ei ole selles selgesõnalises erandis kirjeldatud olukord tingimata ainus, mille puhul keeld ei kehti, pakub selle olukorra selgesõnaline lisamine kõnealusesse sättesse õiguskindlust, kuna see piiritleb keelu ulatuse ja teeb selgeks, et kui tegemist on kõnealuse olukorraga, ei ole see keeld igal juhul kohaldatav.
- (204) Kui süsteem kuulub erandi kohaldamisalasse ja ei ole järelikult keelatud, liigitatakse see suure riskiga tehisintellektisüsteemiks (nagu on osutatud tehisintellektimääruse III lisa punkti 6 alapunktis d), kui see on ette nähtud kasutamiseks õiguskaitseasutuste poolt või nimel, mistõttu kohaldatakse selle suhtes nõudeid ja kaitsemeetmeid, sealhulgas inimjärelevalvet (tehisintellektimääruse artiklid 14 ja 26). Need nõuded hõlmavad seda, et inimjärelevalve ülesanne tuleb määrata vajaliku pädevuse, koolituse ja volitustega isikutele, kes peaksid olema võimelised mõistma nõuetekohaselt tehisintellektisüsteemi võimalusi ja piiranguid, tõlgendama selle väljundit õigesti ja tegelema kalduvusega eelistada automatiseerimist. Nendel isikutel peaks olema selge kord, koolitus ning vajalik pädevus ja volitused, et hinnata mõtestatult tehisintellektisüsteemi tulemusi. Sellisel konkreetsel juhul peaks nende inimhinnang tagama, et igasugune tehisintellekti prognoos või hinnang isiku kuriteo toimepanemise riski kohta põhineks objektiivsetel ja kontrollitavatel faktidel, mis on seotud kuritegeliku tegevusega. Need isikud peaksid samuti sekkuma, et vältida negatiivseid tagajärgi või riske, või lõpetama tehisintellektisüsteemi kasutamise, kui see ei toimi ettenähtud viisil.
- (205) Lisaks sellele on Euroopa Liidu Kohtu praktikas käsitletud „inimese sekkumise“ mõistet, eelkõige seoses üksnes automatiseeritud otsuste tegemisega, millega prognoositakse riski, et lennureisijad on seotud raskete kuritegudega. See kohtupraktika võib olla asjakohane ka tehisintellektimääruse artikli 5 lõike 1 punktis d kasutatud mõiste „inimhinnang“ kohaldamisel.

Ligue des droits humains kohtuasjas¹³⁸ uuris Euroopa Liidu Kohus, kas on seaduslik kasutada täiustatud tehisintellektisüsteemi lennureisijate broneeringuinfo süstemaatiliseks töötlemiseks, et hinnata, kui tõenäoliselt on nad seotud terrorismi ja muude raskete kuritegudega.

Euroopa Liidu Kohus tõlgendas direktiivi (EL) 2016/681 (broneeringuinfo direktiiv) kohast normi, millega keelatakse üksnes automatiseeritud töötlemisel põhinevate

¹³⁸ Kohtuotsus, Euroopa Kohus, 21. juuni 2022, Ligue des droits humains, C-817/19, ECLI:EU:C:2022:491.

ebasoodsate õiguslike otsuste tegemine ja nõutakse **üksikjuhtumite inimhindamist** ja positiivsete tulemuste läbivaatamist mitteautomaatsete vahenditega, et tuvastada valepositiivsed tulemused ja tagada mittediskrimineerivad tulemused.

Euroopa Liidu Kohtu sõnul peab see inimhinnang, millest peavad lähtuma kõik broneeringuinfo automatiseeritud töötlemise tulemused, tuginema objektiivsetele kriteeriumidele, et hinnata, kas positiivne tulemus puudutab kedagi, kes võib konkreetsel juhul olla seotud terroriaktidega või raskete kuritegudega, ning tagada, et automatiseeritud töötlemine on mittediskrimineeriv.

- (206) Mis puutub erandi sisusse, siis üks selle keskseid elemente on see, et tehisintellektisüsteemi kasutatakse inimhinnangu toetamiseks, mitte et tehisintellektisüsteem ise teeks riskihindamisi, nagu toimub keeluga hõlmatud olukordades. Erandi kohaldamiseks peab see inimhinnang siiski lisaks sellele põhinema ka objektiivsetel ja kontrollitavatel faktidel, mis on otseselt seotud kuritegeliku tegevusega.

5.2.4. Millises ulatuses võib eraõiguslike osalejate tegevus kuuluda kohaldamisalasse

- (207) Lisaks õiguskaitseasutustele, kes on põhimõtteliselt peamised tehisintellekti kuritegude prognoosimise süsteemide juurutajad, võib mõnel juhul kuuluda tehisintellektimääruse artikli 5 lõike 1 punktis d sätestatud keelu alla ka eraõiguslike isikute tegevus. See tuleneb asjaolust, et keeldu ei kohaldata selle sõnastuse järgi üksnes õiguskaitseasutuste suhtes. Pealegi oleks muidu võimalik keelust kergesti kõrvale hoida, mis õõnestaks selle tulemuslikkust.
- (208) Sellest tulenevalt võib eeldada, et keeld kehtib eelkõige siis, kui eraõiguslikele isikutele on seadusega usaldatud avaliku võimu ja volituste teostamine kuritegude ennetamiseks, uurimiseks, avastamiseks või nende eest vastutusele võtmiseks või kriminaalkaristuste täitmisele pööramiseks¹³⁹. Erasektori osalejatelt võidakse ka sõnaselgelt nõuda, et nad tegutseksid õiguskaitseasutuste nimel ja koostaksid üksikisikute kuritegevuse riski prognoose. Sellistel juhtudel võib nende eraõiguslike isikute tegevus samuti kuuluda keelu kohaldamisalasse, kui kohaldatavad tingimused on täidetud ja erand ei ole kohaldatav.

Näiteks võib õiguskaitseasutus paluda eraettevõtjal, kes pakub täiustatud tehisintellektipõhist kriminaalanalüüsi tarkvara, analüüsida suurt hulka andmeid mitmest allikast ja andmebaasist, näiteks riiklikest registritest, pangatehingutest, sideandmetest, georuumilistest andmetest jne, et prognoosida või hinnata riski, et üksikisikud võiksid toime panna inimkaubandusega seotud kuritegusid. Kui kõik artikli 5 lõike 1 punkti d kriteeriumid on täidetud, võib sellise kasutusviisi keelata.

- (209) Lisaks võib keeldu kohaldada eraõiguslike üksuste suhtes, kes hindavad või prognoosivad riski, et isik paneb toime kuriteo, kui see on objektiivselt vajalik sellise õigusliku kohustuse täitmiseks, mille kohaselt eraõiguslik ettevõtja peab hindama või

¹³⁹

Vt tehisintellektimääruse artikli 3 punktis 45 esitatud õiguskaitseasutuste määratlust.

prognoosima konkreetsete kuritegude toimepanemise riski (nt rahapesu ja terrorismi rahastamise vastase võitluse puhul).

Näiteks on pangandusasutusel liidu rahapesuvastaste õigusaktide¹⁴⁰ alusel kohustus kliente kontrollida ja teha profiilianalüüse, et tuvastada rahapesuga seotud õigusrikkumisi. Kui pank kasutab oma kohustuste täitmiseks tehisintellektisüsteemi, peaks see toimuma üksnes kõnealuses õigusaktis kirjeldatud andmete alusel, mis on objektiivsed ja kontrollitavad, et tagada, et kahtlusallusteks peetavate isikute puhul on mõistlikult tõenäoline, et nad panevad toime rahapesuga seotud õigusrikkumisi. Prognooside täpsuse ja asjakohasuse tagamiseks peavad inimesed neid vastavalt nimetatud õigusaktile kontrollima ja hindama¹⁴¹. Selle õigusakti järgimine tagab, et üksikisikute kuritegevuse juhtumeid prognoosiva tehisintellektisüsteemi kasutamine rahapesuvastaseks võitluseks jääb väljapoole tehisintellektimääruse artikli 5 lõike 1 punktis d sätestatud keelu kohaldamisala.

- (210) Arvestades siiski, et keelu sõnastusest nähtub, et selles keskendutakse konkreetset ja ainult kuritegude toimepanemisega seotud riskihindamisele, ning põhjenduses 42 selgitatud keelu eesmärki, siis kui eraõiguslik isik teeb klientide profiilianalüüse oma tavapärase äritegevuse ja ohutuse või oma finantshuvide kaitsmise eesmärgil (nt finantsrikkumiste avastamine), ilma et eesmärk oleks hinnata või prognoosida kliendi riski panna toime konkreetne kuritegu, ei tohiks eraõiguslike isikute tegevust lugeda tehisintellektimääruse artikli 5 lõike 1 punktis d sätestatud keelu kohaldamisalasse kuuluvaks.
- (211) Teisisõnu, kui eraõiguslikele isikutele ei ole seadusega usaldatud teatavaid konkreetseid õiguskaitseülesandeid, nad ei tegutses õiguskaitseasutuste nimel või nende suhtes ei kehti eespool kirjeldatud konkreetset õiguslikud kohustused, ei loeta, et keeld hõlmab tehisintellektisüsteemide kasutamist riskihindamiseks eraõiguslike isikute tavapärase äritegevuse raames ja nende enda erahuvide kaitsmiseks, kuid seda, et need riskihindamised võivad olla seotud kuritegude toimepanemise ohuga üksnes juhusliku ja teisejärgulise asjaoluna, ei loeta keelu kohaldamisalasse kuuluvaks.

5.3. Kohaldamisalast välja jäävad olukorrad

5.3.1. Asukohapõhine või georuumiline või kohapõhine kuritegevuse prognoosimine

- (212) Asukohapõhine või georuumiline või kohapõhine kuritegevuse prognoos põhineb kuriteo toimepanemise kohal või asukohal või tõenäosusel, et nendes piirkondades pannakse toime kuritegu. Põhimõtteliselt ei hõlma selline politseitöö konkreetse isiku hindamist. See jääb seega keelu kohaldamisalast välja.

Näiteid asukohapõhistest või georuumilistest prognoosidest või kohapõhistest kuriteoprognoosidest:

¹⁴⁰ 31. mai 2024. aasta rahapesuvastane määrus (EL) 2024/1624.

¹⁴¹ Määruse (EL) 2024/1624 artikkel 20.

- tehisintellektil põhinev prognoosiva politseitöö süsteem annab linna eri piirkondades kuritegevuse tõenäosuse hinde, mis põhineb varasematel kuritegevuse määradel piirkondade lõikes ja muul toetaval teabel, näiteks tänavakaartidel, et tuua esile teatud liiki kuritegude (nt sissemurdmised, noakuriteod jne) kõrgendatud risk ja aidata õiguskaitseasutustel määrata, kus oleks vaja vähem või rohkem politseipatrulle/kohalolekut, et rakendada ühiskondlikku korraldust kuritegevuse tõkestamiseks ja ärahoidmiseks;
- tolliasutus kasutab tehisintellekti riskianalüüsi vahendeid, et prognoosida narkootikumide või ebaseaduslike kaupade asukoha tõenäosust, näiteks teadaolevate salakaubaveo marsruutide alusel;
- politseiamet kasutab tehisintellektipõhiseid süsteeme, et tuvastada tulistamist ja määrata kindlaks selle asukoht reaalajas. Süsteem kasutab linnapiirkondades akustilisi andureid, et tuvastada tulistamise hääled ja määrata kindlaks nende asukoht, andes ametnikele operatiivseid andmeid, mis aitavad kuritegude avastamisel ja uurimisel.

- (213) Siiski ei pruugi alati olla ilmne, kuidas eristada kohapõhiseid kuritegude prognoosimise süsteeme individuaalsetest prognoosisüsteemidest, mis hindavad isiku kuriteo toimepanemise riski. Kuivõrd tehisintellektisüsteem teostab asukohapõhist ennetavat politseitegevust ja arvestab seejärel isiku profiili koostamisel asukoha riski punktisummat, tuleks seda süsteemi pidada isikupõhiseks ja see peaks põhimõtteliselt kuuluma tehisintellektimääruse artikli 5 lõike 1 punkti d kohaldamisalasse, kuigi see võib muudel põhjustel jääda keelu kohaldamisalast välja.

Näiteks kui asukohapõhine või georuumiline teave või kohapõhine teave on seotud üksikisikut käsitleva teabega (nt konkreetse isiku elukoht) ja tehisintellektisüsteem hindab riski, et kõnealune isik paneb tõenäoliselt toime kuriteo, lähtudes üksnes asjaomase isiku profiilianalüüsist, sealhulgas tema elukohast piirkonnas, kus kuritegevust on palju, tuleks seda süsteemi pidada isikupõhiseks.

5.3.2. Tehisintellektisüsteemid, mis toetavad inimhinnanguid, tuginedes kuritegeliku tegevusega seotud objektiivsetele ja kontrollitavatele faktidele

- (214) Tehisintellektimääruse artikli 5 lõike 1 punktis d on sätestatud, et keeldu ei kohaldata tehisintellektisüsteemi suhtes, mida kasutatakse selleks, et toetada inimhinnangut füüsilise isiku kuritegelikus tegevuses osalemise kohta, mis juba tugineb kuritegeliku tegevusega otseselt seotud objektiivsetele ja kontrollitavatele faktidele. Sellisel juhul ei põhineks ka üksikisikute kuritegevuse riski hindamine ja prognoosimine üksnes profiilianalüüsil või isikuomaduste hindamisel ning seetõttu ei oleks see keelatud.

Näited tehisintellektisüsteemidest, mis jäävad sel põhjusel keelu kohaldamisalast välja:

- tehisintellektisüsteemi kasutatakse tegeliku käitumise profiilianalüüsiks ja liigitamiseks, näiteks põhjendatult kahtlane ohtlik käitumine rahvahulgas, mis näitab, et keegi valmistub kuriteoks ja tõenäoliselt paneb selle toime, ning tehisintellekti liigitamisele on antud sisuline inimhinnang. Sellisel juhul ei põhine inimese poolt

tehisintellekti toel tehtud riskihindamine üksnes isikuomadustel või profiilianalüüsil, vaid objektiivsetel ja kontrollitavatel faktidel kõnealuse isiku kuritegevuse toimepanekut ähvardava käitumise kohta, mille inimene on enne meetmete võtmist läbi vaadanud;

- politsei uurib võimaliku relvastatud röövimise ohtu ja kahtlustab kahte isikut. Selle kahtluse aluseks on mitu kontrollitavat ja objektiivset fakti, näiteks kontrollitav osalemine pimeveebi jututubades ja neis vestlemine eesmärgiga relvi osta. Tehisintellektisüsteem, mis kombineerib georuumilise prognoosiva või kohapõhise politseiinfo ja kahtlusalustele kuuluvate sõidukite automatiseeritud numbrimärkide registreerimise teabe, toetab inimhinnangut uurimisel, mis põhineb kontrollitavatel ja objektiivsetel faktidel, mis on otseselt seotud konkreetse kuritegeliku tegevusega;
- sellise tehisintellektisüsteemi kasutamine, mis hindab vahialuse vangistusest ennetähtaegselt vabastamise riske. Mõjutatud isiku tehisintellekti koostatud profiilianalüüs või tema iseloomuomaduste ja erijoonte hindamine toetab ainult objektiivsete ja kontrollitavate faktide hindamist, mis on seotud varasemate kuritegude ja rehabilitatsiooni seisukohalt olulise käitumisega;
- kohtunik määrab raskes kuriteos süüdistatavale isikule eelvangistuse, et hinnata, kas võib kohaldada vabadusekaotuseta meetmeid. Otsus põhineb hinnangul, et on olemas mõjuvad põhjused eelvangistuse määramiseks, näiteks tõenäosus, et kahtlusalune või süüdistatav paneb kinni pidamata jätmise korral toime mõne muu õigusrikkumise või et ta põgeneb või takistab uurimise nõuetekohast läbiviimist. Selle protsessi abistamiseks kasutab kohtunik tehisintellektipõhist riskihindamise vahendit, mida on koolitatud selliste andmete põhjal nagu muu hulgas sarnaste juhtumitega seotud isikute varasemad kriminaalkaristused, samuti sellised tegurid nagu vanuserühm, sotsiaalne käitumine, sissetulek ja tööhõive staatus;
- tehisintellektisüsteemi kasutatakse inimametniku hinnangu toetamiseks, et hinnata ohtu, et vabadusekaotuseta karistust kandev isik rikub vabastamise tingimusi või põgeneb, tuginedes varasemale kuritegelikule käitumisele ja objektiivsetele faktidele, mis annavad alust kahtlustuseks, nagu näiteks vabastamise tingimuste järgimine, psühholoogilise hindamise tulemused ja muude selliste ühiskondlike teenuste soovitusel, mida isik võib kasutada. Selle teabe põhjal otsustab ametnik, kas säilitada *status quo* või vabastamistingimused üle vaadata;
- tehisintellektisüsteemid, mida tolliasutused kasutavad selleks, et hinnata riski, et ELi sisenevad kaubad ei vasta piiril kohaldatavatele õigusaktidele (mis võivad hõlmata näiteks ebaseaduslike uimastite impordikeeldu, ekspordisanktsioonide rikkumist või muud ebaseaduslikku tegevust), et teha kindlaks olukorrad, kus tuleks teha tollikontroll. Tehisintellektisüsteem hindab tollile esitatud objektiivset ja kontrollitavat teavet kaupade ja nende tarneahelate kohta (nt kauba laad ja väärtus, konteineri number, muude kaupade varjamiseks kasutatavad transpordivahendid, eelteadmised selle kohta, kas konkreetse kirjelduse ja päritoluga kaubad vastavad liitu importimise või liidust eksportimise nõuetele). Teatud juhtudel võib ta töödelda ka teavet selle kohta, kas importija või eksportija on varem osalenud kaupade impordiga

seotud rikkumistes, on seotud kuritegelike organisatsioonidega või tema kohta on karistusregistris kanne seoses uimastikaubandusega. Sellised süsteemid ei kuulu keelu kohaldamisalasse, sest igasugune prognoos selle kohta, kas füüsiline isik on tõenäoliselt seotud ebaseadusliku kauba impordiga või ekspordiga, ei põhine üksnes profiilianalüüsil, vaid objektiivsel ja kontrollitaval teabel, mis on seotud kauba ja importija või eksportija varasema osalemisega kuritegelikus tegevuses, ning mille suhtes kohaldatakse inimkontrolli, et teha kindlaks, kas olukord nõuab tollikontrolli või riskimaandusmeedet või mitte.

5.3.3. Tehisintellektisüsteemid, mida kasutatakse kuritegevuse prognoosimiseks ja hindamiseks seoses juriidiliste isikutega

- (215) Tehisintellektimääruse artikli 5 lõike 1 punktis d sätestatud keeld kehtib ainult füüsiliste isikute individuaalsete prognooside ja riskihinnangute suhtes, jättes seega tavaliselt välja kuritegude prognoosimise süsteemid, mis teevad juriidiliste isikute, näiteks äriühingute või valitsusväliste organisatsioonide profiilianalüüse.

Näiteks:

- maksu- või tolliasutus kasutab tehisintellektisüsteemi, et analüüsida suuri andmehulki ettevõtete tehingute ja maksudeklaratsioonide ning tolliandmete kohta, et hinnata riski, et ettevõtte paneb toime maksu- või tollipettuse, mis kujutab endast kuritegu;
- tehisintellektisüsteemid, mida kasutatakse tolliasutuste abistamiseks, et aidata tuvastada olukordi, kus juriidilistele isikutele tuleks anda korraldus mitte saata ebaseaduslikku kaupa ELi.

- (216) Samal ajal võib esineda piiritletud juhtumeid, kus füüsiline isik tegutseb juriidilise isiku kaudu füüsilisest isikust ettevõtjana või vabakutselisena (nt advokaat). Sellistel asjaoludel võib kohaldada tehisintellektimääruse artikli 5 lõike 1 punktis d sätestatud keeldu, kui kõik tingimused on täidetud, sest tehisintellektisüsteem teeb konkreetse füüsilise isiku profiilianalüüsi ja hindab või prognoosib riski, et ta paneb toime kuriteo, isegi kui seda tehakse füüsilise isiku äritegevusega seotud eesmärkidel.

5.3.4. Haldusrikkumiste individuaalsete prognooside tegemiseks kasutatavad tehisintellektisüsteemid

- (217) Tehisintellektimääruse artikli 5 lõike 1 punktis d sätestatud keeldu kohaldatakse ainult kuritegude prognoosimise suhtes, jättes seega selle kohaldamisalast välja haldusrikkumised, mille eest vastutusele võtmine sekkub põhimõtteliselt vähem inimeste põhiõigustesse ja -vabadustesse.

Näiteks ei kuulu tehisintellektimääruse artikli 5 lõike 1 punktis d sätestatud keelu kohaldamisalasse ametiasutus, kes kasutab tehisintellekti haldusjuurdluse raames, et hinnata riski, et võimalikud õigusrikkujad panevad toime väiksemaid õigusrikkumisi (nt pisirikkumised liikluses) või rikkumisi maksu-, hanke- või kuluprotsessides, isegi juhul, kui haldusjuurdluse ja kontrolli tulemusena võidakse koguda teavet füüsiliste isikute kuritegudes osalemise kohta.

- (218) See, kas rikkumine on haldus- või kriminaalõiguslik, võib sõltuda liidu või riigisisestest õigusest. Selliste õigusrikkumiste puhul, mida liidu õigus otseselt ei reguleeri, peab Euroopa Liidu Kohus kontrollima õigusrikkumise riigisisest määratlust, kuna mõistel „kuritegu“ on ELi õiguses autonoomne tähendus ja seda tuleks kõigis liikmesriikides järjepidevalt tõlgendada. Euroopa Liidu Kohus on teises kontekstis jõudnud järeldusele, et süüteole liikmesriikide poolt antav määratlus ei ole otsustava tähtsusega¹⁴². Asjakohased kriteeriumid, mida kasutatakse (kriminaalse või muu) süüte olemuse hindamiseks, võib leida Euroopa Liidu Kohtu ja Euroopa Inimõiguste Kohtu asjakohasest kohtupraktikast¹⁴³.

5.4. Koostoime teiste liidu õigusaktidega

- (219) Tehisintellektimääruse artikli 5 lõike 1 punktis d sätestatud keelu koostoime õiguskaitsedirektiivi ja isikuandmete kaitse üldmäärusega on oluline, kui hinnatakse isikuandmete töötlemise seaduslikkust liidu andmekaitseõiguse, näiteks isikuandmete kaitse üldmääruse ja õiguskaitsedirektiivi alusel. Eelkõige on tehisintellektimääruse artikli 5 lõike 1 punktiga d kehtestatud õiguskaitseasutustele, muudele ametiasutustele ja eraõiguslikele isikutele, kes kuuluvad keelu kohaldamisalasse, konkreetne keeld hinnata või prognoosida riski, et füüsiline isik paneb toime kuriteo, tuginedes üksnes füüsilise isiku profiilialalüüsile või tema isikuomaduste ja erijoonte hindamisele. Seoses õiguskaitsedirektiiviga ei piira tehisintellektimääruse artikli 5 lõike 1 punkt d õiguskaitsedirektiivi artikli 11 lõike 3 kohaldamist, millega keelatakse (otsest või kaudset) diskrimineerimist põhjustavad profiilialalüüsid.
- (220) Asjakohane on ka tehisintellektimääruse artikli 5 lõike 1 punktis d sätestatud keelu ja direktiivi (EL) 2016/343 (süütuse presumptsiooni kohta) vastastikune mõju, kuna mõlemad õigusaktid on seotud – direktiivi puhul otseselt ja tehisintellektimääruse puhul kaudselt (vt selle põhjendust 42) – põhiõigusega olla süütuks peetav, kuni tema süü ei ole seaduse kohaselt tõendatud¹⁴⁴. Kui direktiivi kohaldatakse alates hetkest, mil isikut kahtlustatakse või süüdistatakse kuriteo toimepanemises,¹⁴⁵ siis on tehisintellektimääruse kohaldamisala laiem ja seda kohaldatakse juba prognoosimise ja kuriteoennetuse etapis enne konkreetse isiku suhtes ametliku kriminaaluurimise algatamist ning isegi juhul, kui selliseid prognoose ja riskianalüüse teevad

¹⁴² Vt näiteks kohtuotsus, Euroopa Kohus (suurkoda), 14. november 2013, Euroopa Kohtu (suurkoda), menetlus, mis käsitleb sellise rahalise karistuse täitmisele pööramist, mis määrati Marián Balázile, C-60/12, ECLI:EU:C:2013:733.

¹⁴³ Euroopa Liidu Kohtu praktika kohaselt peavad liikmesriigi kohtud otsustama, kas muid karistusi võib pidada kriminaalkaristusteks, arvestades nn Engeli kriteeriume, vt: kohtuotsus, Euroopa Inimõiguste Kohus, 8. juuni 1976, Engel jt vs. Madalmaad, taotlused nr 5100/71, 5101/71, 5102/71, 5354/72 ja 5370/72, CE:ECHR:1976:0608JUD000510071, punkt 82. Algselt Euroopa Inimõiguste Kohtu poolt välja töötatud ja hiljem Euroopa Liidu Kohtu poolt heaks kiidetud kriteeriumid on alternatiivsed, mitte kumulatiivsed. Karistuse kriminaalse olemuse kontrollimisel peaks pädev liikmesriigi kohus hindama järgmist: 1) asjakohaste sätete liigitus liikmesriigi õiguses, 2) õigusrikkumise laad, ja 3) karistuse raskusaste. Õigusrikkumise laadi hindamisel võetakse muu hulgas arvesse, kas menetluse on algatanud avalik asutus, kellel on seadusest tulenevad jõustamisvolitused; kas õigusnormil on karistuslik või hoiatav eesmärk; kas õigusnormi eesmärk on kaitsta ühiskonna üldisi huve, mida tavaliselt kaitseb kriminaalõigus; kas karistuse määramine sõltub süüdimõistmisest. Karistuse raskusastme puhul on asjakohane viidata riigisisese õiguses sätestatud maksimaalsele võimalikule karistusele. Need kriteeriumid on alternatiivsed ja mitte tingimata kumulatiivsed. Vt Euroopa Inimõiguste Kohus, Guide on Article 6 of the European Convention on Human Rights, Right to a fair trial (criminal limb), ajakohastatud 29. veebruaril 2024. Vt ka kohtuotsus, Euroopa Kohus, 5. juuni 2012, Bonda, C-489/10, EU:C:2012:319, punktid 37 jj; kohtuotsus, Euroopa Kohus, 26. veebruar 2013, Åkerberg Fransson, C-617/10, EU:C:2013:105, punkt 35.

¹⁴⁴ Süütuse presumptsioon on ELi põhiõiguste harta artiklis 48 sätestatud põhiõigus.

¹⁴⁵ Nagu Euroopa Liidu Kohus on täpsustanud, ei ole direktiivi kohaldamiseks nõutav, et pädev asutus teavitaks seda isikut tema staatusest kahtlusaluse/süüdistatava isikuna.

eraõiguslikud isikud, kes kuuluvad tehisintellektimääruse artikli 5 lõike 1 punkti d kohaldamisalasse, mitte aga pädevad õiguskaitseasutused, sealhulgas õigusasutused.

- (221) Isegi juhtudel, kui tehisintellektimääruse artikli 5 lõike 1 punktis d sätestatud keeldu ei kohaldata, on oluline rõhutada, et kohaldatav liidu ja riigisisene õigus jääb täielikult kohaldatavaks, sealhulgas eelkõige andmekaitse, kriminaalmenetluse ja politseiga seotud õigus ning kaitsemeetmed, mis võivad veelgi piirata või kehtestada lisatingimusi üksikisikute kuritegevust prognoosivate tehisintellektisüsteemide kasutamisele.

6. TEHISINTELLEKTIMÄÄRUSE ARTIKLI 5 LÕIKE 1 PUNKT E – NÄOKUJUTISTE KINDLA SUUNITLUSETA EKSTRAHEERIMINE

- (222) Tehisintellektimääruse artikli 5 lõike 1 punktis e on keelatud selliste tehisintellektisüsteemide turule laskmine või kasutusele võtmine sellel konkreetsel eesmärgil või nende kasutamine, mis loovad või laiendavad näotuvastuse andmebaase internetist või videovalve salvestistest näokujutiste kindla suunitluseta ekstraheerimise kaudu.

6.1. Põhjendus ja eesmärgid

- (223) Näokujutiste kindla suunitluseta ekstraheerimine internetist ja videovalve salvestistest riivab tõsiselt üksikisikute õigust eraelu puutumatusele ja andmekaitsele ning piirab nende isikute õigust jääda anonüümseks. Põhjenduses 43 põhjendatakse tehisintellektimääruse artikli 5 lõike 1 punktis e sätestatud keeldu seetõttu massilise jälgimise tundega ja põhiõiguste, sealhulgas eraelu puutumatuse õiguse ränga rikkumise ohuga.

6.2. Keelu põhimõisted ja komponendid

Tehisintellektimääruse artikli 5 lõike 1 punktis e on sätestatud:

„Järgmised tehisintellekti kasutusviisid on keelatud:

e) selliste tehisintellektisüsteemide turule laskmine või kasutusele võtmine sellel konkreetsel eesmärgil või nende kasutamine, mis loovad või laiendavad näotuvastuse andmebaase internetist või videovalve salvestistest näokujutiste kindla suunitluseta ekstraheerimise kaudu;“.

- (224) Selleks, et tehisintellektimääruse artikli 5 lõike 1 punktis e sätestatud keeld oleks kohaldatav, peavad olema täidetud mitu kumulatiivset tingimust:
- (i) kasutusviis peab kujutama endast tehisintellektisüsteemi turule laskmist, kasutusele võtmist sel konkreetsel eesmärgil või kasutamist;
 - (ii) seda tehakse näotuvastuse andmebaaside loomiseks või laiendamiseks;
 - (iii) andmebaasi täiendamiseks toimub kindla suunitluseta ekstraheerimine, mida tehakse tehisintellekti vahendite abil, ning
 - (iv) kujutised pärinevad kas internetist või videovalve salvestistest.

- (225) Keelu kohaldamiseks peavad kõik neli tingimust olema samal ajal täidetud. Punktis 2.3 on juba analüüsitud tehisintellektisüsteemi turule laskmise, kasutusele võtmise või kasutamise esimest elementi. Seega kehtib keeld nii tehisintellektisüsteemide pakkujate kui ka juurutajate suhtes, kes on oma vastutuse piires kohustatud selliseid süsteeme mitte turule laskma, kasutusele võtma ega kasutama. Järgnevalt kirjeldatakse ja analüüsitakse täpsemalt kindla suunitluseta ekstraheerimise keeluga seotud konkreetseid kriteeriume. Keeldu kohaldatakse ekstraheerimisvahendite suhtes, mis on turule lastud või kasutusele võetud sellel konkreetsetel eesmärgil, et ekstraheerida kindla suunitluseta näokujutisi internetist või videovalve salvestistest. See tähendab, et keeld ei kehti mis tahes ekstraheerimisvahendi suhtes, millega võib luua või laiendada näotuvastuse andmebaasi, vaid ainult kindla suunitluseta ekstraheerimise vahendite suhtes.

6.2.1. Näotuvastuse andmebaasid

- (226) Tehisintellektimääruse artikli 5 lõike 1 punktis e sätestatud keeld hõlmab tehisintellektisüsteeme, mida kasutatakse näotuvastuse andmebaaside loomiseks või laiendamiseks. Andmebaasi all tuleks käesolevas kontekstis mõista mis tahes andmete või teabe kogumit, mis on spetsiaalselt korraldatud kiireks otsinguks ja leidmiseks arvuti abil. Näotuvastuse andmebaas on võimeline viima inimese näo vastavusse digitaalsest kujutisest või videokaadrist pärit nägude andmebaasiga, võrdlema seda andmebaasis olevate kujutistega ja määrama, kas nende kahe vahel on tõenäoline kokkulangevus. Selline näotuvastuse andmebaas võib olla ajutine, tsentraliseeritud või detsentraliseeritud. Artikli 5 lõike 1 punkt e ei nõua, et andmebaasi ainus eesmärk oleks kasutada seda näotuvastuseks – piisab sellest, et andmebaasi saab kasutada näotuvastuseks.

6.2.2. Näokujutiste kindla suunitluseta ekstraheerimine

- (227) „Ekstraheerimine“ tähendab tavaliselt otsiämblike, robotite või muude vahendite kasutamist selleks, et ekstraheerida automaatselt andmeid või sisu erinevatest allikatest, sealhulgas videovalve salvestistest, veebilehtedelt või sotsiaalmeediast. Need tööriistad on tarkvara, mis on programmeeritud andmebaaside sõelumiseks ja teabe väljavõtmiseks ning teabe kasutamiseks muul eesmärgil.
- (228) „Kindla suunitluseta“ tähendab võtet, mis toimib nagu tolmuimeja, imedes endasse võimalikult palju andmeid ja teavet, ilma et ekstraheerimise subjektid oleksid konkreetsetelt ja individuaalselt sihtmärgiks võetud. Ekstraheerimise käigus kogutakse valimatult andmeid või sisu. Seega tähendab mõiste „kindla suunitluseta“ seda, et ei keskenduta konkreetsele üksikisikule või üksikisikute rühmale. Internetiprotokollide, nagu robot.txt mittekasutamine ei mõjuta ekstraheerimise kindla suunitluseta olemust.
- (229) Kui ekstraheerimisvahendile antakse korraldus koguda pilte või videoid, mis sisaldavad inimnägusid ainult konkreetsetest isikutest või eelnevalt määratletud isikute rühmast, siis muutub ekstraheerimine sihipäraseks, näiteks ühe konkreetse kurjategija leidmiseks või ohvrite rühma tuvastamiseks. Selline ekstraheerimine ei kuulu tehisintellektimääruse artikli 5 lõike 1 punktis e sätestatud keelu alla.

- (230) Näiteks ei hõlma keeld kujutiste sihipärast kogumist, kui selles keskendutakse ohvrite klassile, kogudes otsiämblike abil ohvrite kujutisi, mida inimkaubitsejad sotsiaalmeediakanalites avaldavad/reklaamivad. Kindla suunitluseta ekstraheerimist tuleks tõlgendada nii, et see ei võimaldaks keelust kõrvale hoida. Interneti või videovalve salvestiste ekstraheerimine järk-järgult andmebaasi loomiseks, valides seejuures iga kord konkreetsed isikute rühmad või muud kriteeriumid, peaks kuuluma tehisintellektimääruse artikli 5 lõike 1 punktis e sätestatud keelu alla, kui lõpptulemus on funktsionaalselt sama, mis algusest peale kindla suunitluseta toimuv ekstraheerimine.
- (231) Kui süsteemid kombineerivad piltide või videote sihipäraseid otsinguid kindla suunitluseta otsingutega, on kindla suunitluseta ekstraheerimine keelatud.

6.2.3. Internetist ja videovalve salvestistest

- (232) Tehisintellektimääruse artikli 5 lõike 1 punktis e sätestatud keelu kohaldamiseks võivad näokujutised olla pärit kas internetist või videovalve salvestistest. Mis puutub interneti, siis asjaolu, et isik on avaldanud enda näokujutised sotsiaalmeedia platvormil, ei tähenda, et ta on andnud oma nõusoleku nende piltide lisamiseks näotuvastuse andmebaasi. Näokujutiste ekstraheerimine videovalve salvestistest hõlmab näiteks pilte, mis on saadud sellistes kohtades nagu lennujaamad, tänavad, pargid jne kasutatavatest valvekaameratest.

Näide:

näotuvastustarkvara ettevõtte kogub pilte nägudest. Ettevõtte valduses olevad fotod on saadud sotsiaalmeediast (nt Facebook, YouTube, Twitter, Venmo) nn automatiseeritud kujutiste ekstraheerijaga, mis teeb internetiotsinguid ja tuvastab inimnägusid sisaldavad pildid. See kogub neid pilte koos kõigi nendega seotud andmetega (näiteks pildi allikas (URL), geograafiline asukoht ja mõnikord ka isikute nimed). Seejärel eraldatakse piltidelt näojooned ja teisendatakse matemaatilisele kujule, mis räsitakse indekseerimiseks ja edaspidiseks võrdlemiseks. Kui kasutaja laeb tehisintellektisüsteemi üles inimese pildi, määrab süsteem kindlaks, kas see pilt vastab andmebaasis olevale näole. Üleslaaditud pilt läbib sama matemaatilise teisendamise nagu ekstraheeritud pildid.

- (233) Kui tehisintellektisüsteem saab inimese pildi ja otsib selle näo kohta internetis vasteid, st kasutab nn pöördpildiotsingu mootorit, loetakse seda sihipäraseks ekstraheerimiseks. Lisaks on küsitav, kas need vasted oleksid kuskil andmebaasis.

6.3. Kohaldamisalast välja jäävad olukorrad

- (234) Tehisintellektimääruse artikli 5 lõike 1 punktis e sätestatud keeldu ei kohaldata muude biomeetriliste andmete kui näokujutiste (näiteks hääleproovide) kindla suunitluseta ekstraheerimise suhtes. Keeldu ei kohaldata ka juhul, kui ekstraheerimises ei osale tehisintellektisüsteem. Kohaldamisalasse ei kuulu ka näokujutiste andmebaasid, mida ei kasutata isikute tuvastamiseks, näiteks tehisintellekti mudeli treenimiseks või katsetamiseks kasutatavad näokujutiste andmebaasid, kus isikuid ei ole tuvastatud.

- (235) Tehisintellektimääruse artikli 5 lõike 1 punktis e sätestatud keeldu ei kohaldata tehisintellektisüsteemide suhtes, mis koguvad internetist suures koguses näokujutisi, et luua tehisintellekti mudeleid, mis loovad uusi pilte fiktiivsetest isikutest, sest selliste süsteemide tulemuseks ei ole reaalsete isikute tuvastamine. Sellised tehisintellektisüsteemid võiksid kuuluda tehisintellektimääruse artiklis 50 kirjeldatud läbipaistvusunõuete alla.
- (236) Tehisintellektimääruse artikli 5 lõike 1 punktis e sätestatud keeld hõlmab tehisintellektisüsteeme, mida kasutatakse näotuvastuse andmebaaside loomiseks või laiendamiseks. Kui tegemist on olemasolevate näoandmebaasidega, mis on loodud enne keelu kohaldamise algust ja mida ei laiendata edasi tehisintellekti abil tehtava kindla suunitluseta ekstraheerimise abil, peavad need andmebaasid ja nende kasutamine vastama kohaldatavatele liidu andmekaitseenormidele.
- (237) Tehisintellektimääruse artikli 5 lõike 1 punktis e sätestatud keeld on suunatud näotuvastuse andmebaaside loomisele või laiendamisele. Konkreetne biomeetriline tuvastamine on reguleeritud konkreetsete õigusnormidega, mis on sätestatud tehisintellektimääruses ja muudes asjakohastes liidu õigusaktides.

6.4. Koostoime teiste liidu õigusaktidega

- (238) Seoses liidu andmekaitsealaste õigusaktidega oleks interneti või videovalve salvestiste kindla suunitluseta ekstraheerimine näotuvastuse andmebaaside loomiseks või laiendamiseks, st isikuandmete töötlemine (andmete kogumine ja andmebaaside kasutamine), ebaseaduslik ning isikuandmete kaitse üldmäärus, ELi isikuandmete kaitse määrus ja õiguskaitseDirektiiv ei annaks selleks mingit õiguslikku alust.

7. TEHISINTELLEKTIMÄÄRUSE ARTIKLI 5 LÕIKE 1 PUNKT F – EMOTSIOONITUVASTUS

- (239) Tehisintellektimääruse artikli 5 lõike 1 punktis f on keelatud tuletada füüsilise isiku emotsioone töökoha ja haridusasutustega seoses, välja arvatud juhul, kui süsteemi kavatsetakse kasutusele võtta meditsiinilistel või ohutusega seotud põhjustel. Emotsioonituvastussüsteemid, mis ei kuulu keelu alla, loetakse tehisintellektimääruse III lisa punkti 1 alapunkti c kohaselt suure riskiga süsteemideks. Tehisintellektimääruse artikli 50 lõikes 3 on sätestatud emotsioonituvastussüsteemide kasutamise kohta teatavad läbipaistvusunõuded.

7.1. Põhjendus ja eesmärgid

- (240) Emotsioonituvastustehnoloogia areneb kiiresti ja hõlmab erinevaid tehnoloogialahendusi ja töötlemisoperatsioone, et emotsioone tuvastada, koguda, analüüsida, liigitada, neile reageerida ning inimestega suhelda ja neilt emotsioone õppida. Sellist tehnoloogiat nimetatakse ka „tundmustehnoloogiaks“. Emotsioonituvastust saab kasutada paljudes valdkondades mitmesuguste rakenduste

jaoks,¹⁴⁶ näiteks klientide käitumise analüüsiks¹⁴⁷ ning sihipäraseks reklaamiks ja neuroturunduseks;¹⁴⁸ meelelahutustööstuses, näiteks selleks, et anda isikupärastatud soovitusi või prognoosida reaktsioone filmidele; meditsiinis ja tervishoius, näiteks depressiooni avastamiseks, enesetappude ennetamiseks või autismi avastamiseks; hariduses, näiteks õppijate (eri vanuses õpilaste ja üliõpilaste) tähelepanu või kaasatuse jälgimiseks; tööhõives, näiteks värbamisprotsessi täiendamiseks, töötajate emotsioonide või tüdimuse jälgimiseks, aga ka heaolu rakendused töötajate õnnelikumaks muutmiseks;¹⁴⁹ õiguskaitseasutuste ja avaliku julgeoleku jaoks, näiteks valedetektoritega või suurüritustel emotsioonide jälgimisega, ja paljudel muudel eesmärkidel.

- (241) Sageli kaheldakse emotsioonituvastuse tõhususes või täpsuses¹⁵⁰. Tehisintellektimääruse põhjenduses 44 on selgitatud, et „[t]õsist muret tekitab selliste tehisintellektisüsteemide teaduslik alus, mille eesmärk on tuvastada või tuletada emotsioone, eelkõige seetõttu, et emotsioonide väljendamine on kultuuride ja olukordade lõikes ning isegi ühe inimese puhul väga erinev. Selliste süsteemide peamiseks puudusteks on piiratud usaldusväarsus, spetsiifilisuse puudumine ja piiratud üldistatavus“. Lisaks on seal selgitatud, et emotsioonituvastus võib viia „diskrimineerivate tulemusteni ning sekkuda asjaomaste isikute õigustesse ja vabadustesse“, eelkõige õigusesse eraelu puutumatusele, inimväärikusele ja mõttevabadusele. Sellel on oluline osa asümmeetrilistes suhetes, eriti töökohal ning haridus- ja koolitusasutustes, kus nii töötajad kui ka õpilased on eriti haavatavas olukorras. Samal ajal on emotsioonituvastus kasulik spetsiifilistes kasutuskontekstides, näiteks ohutus ja meditsiiniabi (nt ravi ja diagnoosimine)¹⁵¹.

7.2. Keelu põhimõisted ja komponendid

Tehisintellektimääruse artikli 5 lõike 1 punktis f on sätestatud:

„Järgmised tehisintellekti kasutusviisid on keelatud:

f) tehisintellektisüsteemide turule laskmine või kasutusele võtmine sellel konkreetsel eesmärgil või nende kasutamine füüsilise isiku emotsioonide tuletamiseks töökoha ja haridusasutustega seoses, välja arvatud juhul, kui tehisintellektisüsteemi kavatsetakse kasutusele võtta või turule viia meditsiinilistel või ohutusega seotud põhjustel;“.

¹⁴⁶ Emotsioonide kasutamist majanduslikel eesmärkidel tähistatakse inglise keeles ka nimetusega „emotionomics“ (tundemajandus).
¹⁴⁷ Vt nt G. Mangano, A. Ferrari, C. Rafale, E. Vezzetti, F. Marcolin, [Willingness of sharing facial data for emotion recognition: a case study in the insurance market](#), AI & Society, London, Springer, 2023.
¹⁴⁸ Vt N. Lee, A. J. Broderick ja L. Chamberlain, [What is 'neuromarketing'? A discussion and agenda for future research](#), International Journal of Psychophysiology, 63(2), 2007, lk 199–204, kus neuroturundus määratletakse valdkonnana, mis uurib neuroteaduslike meetodite kasutamist inimekäitumise analüüsimiseks ja mõistmiseks turgude ja turundusega seotud suhtluse kontekstis (lk 200).
¹⁴⁹ Vt E. Ackerman, & E. Strickland, Are you Ready for Workplace Brain Scanning? Extracting and using brain data will make workers happier and more productive, backers say, IEEE Spectrum, 19. november 2022, <https://spectrum.ieee.org/neurotech-workplace-innereye-emotiv>. Autorid selgitavad, et andurid tuvastavad elektrilist tegevust aju eri piirkondades ja selle tegevuse mustreid saab üldjoontes korreleerida erinevate tunnete või füsioloogiliste reaktsioonidega, näiteks stressi, keskendumise või väliste stiimulitele reageerimisega.
¹⁵⁰ Vt nt, J. Stanley, [Experts Say 'Emotion Recognition' lacks Scientific Foundation](#), 18.7.2019, ACLU, milles viidatakse L. Feldman Barrett'i jt uuringule [Emotional Expressions Reconsidered: Challenges to Inferring Emotion From Human Facial Movements](#), Psychological Science in the Public Interest, 2019, lk iii–90.
¹⁵¹ Vt nt R. El Kaliouby, R. Picard, S. Baron-Cohen, [Affective Computing and Autism](#), Annals New York Academy of Sciences, 2007, lk 228–248.

- (242) Selleks, et tehisintellektimääruse artikli 5 lõike 1 punktis f sätestatud keeld oleks kohaldatav, peavad olema täidetud mitu kumulatiivset tingimust:
- (i) kasutusviis peab kujutama endast tehisintellektisüsteemi turule laskmist, kasutusele võtmist sel konkreetsel eesmärgil või kasutamist;
 - (ii) tehisintellektisüsteemi kasutatakse emotsioonide tuletamiseks¹⁵²;
 - (iii) seda kasutatakse töökohal või haridus- ja koolitusasutustes ning
 - (iv) keelust on välja jäetud meditsiinilistel või ohutusega seotud põhjustel kasutamiseks mõeldud tehisintellektisüsteemid.
- (243) Keelu kohaldamiseks peavad kõik neli tingimust olema samal ajal täidetud. Esimest tingimust, st tehisintellektisüsteemi turule laskmist, kasutusele võtmist või kasutamist, on juba analüüsitud punktis 2.3. Seega kehtib keeld nii tehisintellektisüsteemide pakkujate kui ka juurutajate suhtes, kes on oma vastutuse piires kohustatud selliseid süsteeme mitte turule laskma, kasutusele võtma ega kasutama. Teisi keeluga seotud tingimusi kirjeldatakse ja analüüsitakse täpsemalt allpool.

7.2.1. Tehisintellektisüsteemid emotsioonide tuletamiseks

a) Tehisintellektisüsteemid emotsioonide tuletamiseks vs. emotsioonituvastussüsteemid

- (244) Tehisintellektimääruse artikli 3 punktis 39 on emotsioonituvastussüsteemid määratletud kui tehisintellektisüsteem, mille eesmärk on tuvastada või tuletada füüsiliste isikute emotsioone või kavatsusi nende biomeetriliste andmete põhjal. Tehisintellektimääruse artikli 5 lõike 1 punktis f sätestatud keelus ei viidata mitte emotsioonituvastussüsteemidele, vaid ainult tehisintellektisüsteemidele, mis võimaldavad tuletada füüsilise isiku emotsioone. Põhjenduses 44 selgitatakse täpsemalt, et see keeld hõlmab tehisintellektisüsteeme, mille eesmärk on tuvastada või tuletada emotsioone.
- (245) Tuletamine nõuab üldjuhul eeldusena tuvastamist, nii et keeldu tuleks mõista nii, et see hõlmab nii tehisintellektisüsteeme, mis tuvastavad emotsioone või kavatsusi, kui ka tehisintellektisüsteeme, mis tuletavad neid¹⁵³. Järjepidevuse huvides on ka oluline tõlgendada artikli 5 lõike 1 punktis f sätestatud keeldu nii, et sellel on samasugune kohaldamisala kui muudel emotsioonituvastussüsteemide suhtes kohaldatavatel õigusnormidel (tehisintellektimääruse III lisa punkti 1 alapunkt c ja artikkel 50), ning piirata seda isiku biomeetrilistel andmetel põhineva tuletamisega. Seepärast tuleks tehisintellektimääruse artikli 3 punktis 39 esitatud emotsioonituvastussüsteemi määratlust pidada tehisintellektimääruse artikli 5 lõike 1 punkti f puhul asjakohaseks.

b) Emotsioonide või kavatsuste tuvastamine ja tuletamine

- (246) Tuvastamine toimub siis, kui füüsilise isiku biomeetriliste andmete (näiteks hääle või näoilme) töötlemine võimaldab otseselt võrrelda ja tuvastada emotsiooni, mis on

¹⁵² Või tehnoloogiat, mis on võimeline emotsioone tuletama (st turule laskmise ajal).

¹⁵³ Vt ka tehisintellektimääruse põhjendus 18.

eelnevalt emotsioonituvastussüsteemi programmeeritud. Tuletamine toimub siis, kui süsteem ise teeb analüütiliste ja muude protsesside abil saadud teabe põhjal järeldusi. Sellisel juhul ei põhine teave emotsiooni kohta ainult füüsilise isiku kohta kogutud andmetel, vaid see tuletatakse muudest andmetest, sealhulgas masinõppe meetoditest, mis õpivad andmete põhjal, kuidas emotsioone tuvastada¹⁵⁴.

c) Emotsioonid

- (247) Tehisintellektimääruse artikli 5 lõike 1 punkti f kohaldamisel tuleks emotsioonide või kavatsuste mõistet mõista laias tähenduses ja mitte seda kitsendavalt tõlgendada. Tehisintellektimääruse põhjendus 18 on selles osas üksikasjalikum, loetledes selliseid emotsioone „nagu õnnetunne, kurbus, viha, üllatus, vastikus, piinlikkus, elevus, häbi, põlgus, rahulolu ja lõbustatus“. Neid näiteid on veelgi.
- (248) Keelust ei tohiks hoiakutele viidates kõrvale hoida ja see hõlmab ka juhtumeid, kus tehisintellektisüsteem leiab biomeetriliste andmete põhjal, et isiku puhul on näha näiteks vihast suhtumist.
- (249) Tehisintellektimääruse põhjenduses 18 selgitatakse, et emotsioonid või kavatsused ei hõlma „füüsilisi seisundeid, nagu valu või väsimus, sealhulgas näiteks süsteeme, mida kasutatakse kutseliste pilootide või sõidukijuhtide väsimuse avastamiseks, et õnnetusi ära hoida“. Lisaks selgitatakse, et emotsioonituvastussüsteemid ei hõlma „pelgalt kergesti arusaadavate ilmete, žestide või liigutuste kindlakstegemist, välja arvatud juhul, kui neid kasutatakse emotsioonide tuvastamiseks või tuletamiseks“, mida tuleks mõista nii, et see kehtib ka tehisintellektimääruse artikli 5 lõike 1 punkti f puhul. Nimetatud ilmed võivad olla tavalised näoilmed, näiteks kulmukortsutus või naeratus, või žestid, nagu käte- või pealiigutused, või isiku hääle erijooned, näiteks vali hääle või sosistamine. Kui aga neid kergesti nähtavaid väljendeid või žeste kasutatakse emotsioonide või kavatsuste tuvastamiseks või järeldamiseks, siis kohaldatakse nende suhtes kõnealust keeldu.

Näiteks:

- tähelepanek, et inimene naeratab, ei ole emotsioonituvastus;
- selle määramine, kas inimene on haige, ei ole emotsioonituvastus;
- kui teleringhääling kasutab seadet, mis võimaldab jälgida, mitu korda tema uudistelugejad kaamerasse naeratavad, ei ole tegemist emotsioonituvastusega;
- järeldus, et inimene on õnnelik, on emotsioonituvastus. Tehisintellektisüsteem, mis järeldab, et töötaja on klientidega suheldes õnnetu, kurb või vihane (nt kehakeele, kulmukortsutuse või naeratuse puudumise põhjal), on emotsioonituvastus;
- kui süsteem järeldab hääle või kehaliste žestide põhjal, et õpilane on vihane ja hakkab vägivaldseks muutuma, on see emotsioonituvastus;

¹⁵⁴

Vt tehisintellektimääruse põhjendus 12. Tuletatud andmed on seega sageli ka tõenäosuspõhiste analüütiliste (suurandmete) protsesside tulemus, mille eesmärk on leida andmekogumitest korrelatsioone ja mustreid.

– tehisintellektipõhiste tuvastussüsteemide kasutamine kutselise piloodi või autojuhi väsimuse tuvastamiseks, et hoiatada neid ja soovitada, millal nad peaksid õnnetuste vältimiseks pidurdama, ei ole emotsioonituvastus, sest emotsioonituvastus ei hõlma füüsilisi seisundeid, nagu valu või väsimus.

d) Biomeetriliste andmete põhjal

- (250) Vastavalt tehisintellektimääruse artikli 3 punktis 39 esitatud määratlusele on emotsioonide või kavatsuste tuvastamise süsteemid ainult need tehisintellektisüsteemid, mis tuvastavad või tuletavad emotsioone või kavatsusi biomeetriliste andmete põhjal¹⁵⁵.
- (251) Isikuomadused, millest saab biomeetrilisi andmeid koguda, on füüsilised või käitumuslikud tunnused. Füsioloogilise biomeetria puhul kasutatakse inimese füüsilisi, struktuurilisi ja suhteliselt staatilisi tunnuseid, näiteks sõrmejälgi, iirise mustrit, näo kontuure või käe veenide geomeetrist paiknemist. Mõned omadused on oma olemuselt mikroskoopilised, kuid neil on siiski bioloogilisi ja keemilisi struktuure, mida saab koguda ja identifitseerida, nt DNA ja lõhn¹⁵⁶. Käitumisbiomeetria jälgib üksikisikute liigutuste, žestide ja mootorsete oskuste iseloomulikke omadusi, kui nad täidavad ülesannet või ülesannete seeriat. See tähendab, et inimese liigutused, näiteks kõndimine (kõnnaku analüüs) või sõrme kokkupuude klaviatuuriga (klahvivajutused), salvestatakse ja neid analüüsitakse. Käitumisbiomeetria hõlmab mitmesuguseid mooduseid, mis näitavad nii tahtlikke kui ka tahtmatuid korduvaid liigutusi ja nendega seotud kehaomaduste rütmilist ajastust/rõhku, alates allkirjadest, kõnnakust, häälest ja klahvivajutustest kuni silmade jälgimise ja südamelöökid¹⁵⁷ elektroentsefalograafia¹⁵⁸ või elektrokardiogrammini¹⁵⁹. Biomeetiline sisend võib olla seotud ühe omadusega (nt näokujutised) või mitme omadusega (nt näoteave koos elektroentsefalogrammiga (EEG)). Põhjudes 18 tuuakse näiteks näoilmed, žestid, näiteks käte liikumine, või isiku hääle erijooned.

Näiteks:

- tehisintellektisüsteem, mis tuletab kirjalikust tekstist emotsioone (sisu-/tundeanalüüs), et määratleda teatud artikli stiili või tooni, ei põhine biomeetrilistel andmetel ja ei kuulu seega keelu kohaldamisalasse;

¹⁵⁵ Tehisintellektimääruse artikli 3 punkti 34 järgi on biomeetrilised andmed „konkreetselt tehnilise töötlemise abil saadavad isikuandmed füüsilise isiku füüsiliste, füsioloogiliste või käitumuslike omaduste kohta, näiteks näokujutis või sõrmejälgede andmed“. Vt ka tehisintellektimääruse põhjendus 18, mis käsitleb emotsioonide tuletamist hääle ja kõne põhjal.

¹⁵⁶ [Physiological and Behavioural Biometrics, Biometrics Institute](#).

¹⁵⁷ [Physiological and Behavioural Biometrics, Biometrics Institute](#).

¹⁵⁸ Vt Euroopa andmekaitseinspektor, [TechDispatch 1/2024 – Neurodata](#), 3.6.2024, milles käsitletakse ajuandmete ja nendega seotud tehnoloogia kasutamist ning õiguslikke tagajärgi, sealhulgas ettepanekut uute nn neuroõiguste, sealhulgas vaimse eraelu puutumatuse ja tervikluse kohta. Vt S. O’Sullivan, H. Chneiweiss, A. Pierucci ja K. Rommelfanger, [Neurotechnologies and Human Rights Framework: Do we need new Human Rights?](#), aruanne, OECD ja Euroopa Nõukogu, 9.11.2021, lk 33, kus käsitletakse neurotehnoloogia praegust taset ja õiguslikke aspekte.

¹⁵⁹ Vt [Hasnul et al., 2021, Electrocardiogram-Based Emotion Recognition Systems and Their Applications in Healthcare](#).

– tehisintellektisüsteem, mis tuleb emotsioone klahvivajutuse (trükkimise viis), näoilmete, kehaasendite või liigutuste põhjal, põhineb biomeetrilistel andmetel ja kuulub keelu kohaldamisalasse.

- (252) Tehisintellektimääruse biomeetriliste andmete määratlus on seega lai ja hõlmab kõiki biomeetrilisi andmeid, mida kasutatakse emotsioonide tuvastamiseks, biomeetriliseks liigitamiseks või muudel eesmärkidel¹⁶⁰.

7.2.2. Keelu piiramine töökoha ja haridusasutustega

- (253) Tehisintellektimääruse artikli 5 lõike 1 punktis f sätestatud keeld piirdub emotsioonituvastussüsteemidega „töökoha ja haridusasutustega seoses“. Nagu on selgitatud tehisintellektimääruse põhjenduses 44, on selle piirangu eesmärk käsitleda võimu ebavõrdsust töö või hariduse kontekstis.

a) „Töökoht“

- (254) Mõistet „töökoht“ tuleks tõlgendada laialt. See mõiste on seotud mis tahes konkreetse füüsilise või virtuaalse ruumiga, kus füüsilised isikud täidavad ülesandeid ja kohustusi, mille on neile määranud nende tööandja või organisatsioon, millega nad seotud on, näiteks füüsilisest isikust ettevõtja puhul. See hõlmab mis tahes keskkonda, kus tööd tehakse, ja see võib sõltuvalt töö iseloomust olla väga erinev, näiteks siseruumides asuvad kontorid, tehased ja laod; avalikult juurdepääsetavad ruumid, nagu poed, staadionid või muuseumid; vabaõhualad või autod, samuti ajutised või teisaldatavad töökohad. See ei sõltu töötaja, töövõtja, praktikandi, vabatahtliku jne staatusest¹⁶¹. Tehisintellektimääruse artikli 5 lõike 1 punktis f kasutatud mõistet „töökoht“ tuleks mõista nii, et see kehtib ka kandidaatide suhtes valiku- ja värbamisprotsessi ajal, kooskõlas tehisintellektimääruse muude sätetega, mis käsitlevad tehisintellektisüsteemide turule laskmist, kasutusele võtmist või kasutamist tööhõive, töötajate juhtimise ja iseenda tööandjana tegutsemise valdkonnas, arvestades võimu ebavõrdsust ning seda, et emotsioonituvastuse sekkuv iseloom võib avaldada mõju juba värbamisetapis.

Näiteks:

– veebikaamerate ja häältuvastussüsteemide kasutamine kõnekeskuses selle töötajate emotsioonide, näiteks viha jälgimiseks on keelatud¹⁶². Kui emotsioonituvastussüsteeme kasutatakse ainult isikliku koolituse eesmärgil, on need lubatud, kui tulemusi ei jagata personaliosakonna vastutavate isikutega ja need ei saa

¹⁶⁰ Tehisintellektimääruse biomeetriliste andmete määratlus ei sisalda sõnu „mis võimaldavad kordumatult tuvastada või kinnitada tuvastamist“ (biomeetriliste andmete funktsionaalne kasutamine), erinevalt isikuandmete kaitse üldmääruse biomeetriliste andmete määratlusest, mis sisaldab seda nõuet. Isikuandmete kaitse üldmääruse biomeetriliste andmete määratlust kohaldatakse isikuandmete töötlemise suhtes andmekaitsestandardite alusel (ja kui näiteks kohaldatakse isikuandmete kaitse üldmääruse artikli 9 lõiget 1 ja artikli 9 lõiget 2).

¹⁶¹ Vt ka põhjendusi, mis käsitlevad suure riskiga tehisintellektisüsteemide töökohal, näiteks põhjendus 56, milles kasutatakse laia tõlgendust. Vt ka III lisas esitatud suure riskiga tehisintellektisüsteemide loetelu, mille punktis 4 viidatakse iseenda tööandjana tegutsemisele. Füüsilisest isikust ettevõtjana tegutsemine on samuti suures osas hõlmatud ELi diskrimineerimisvastase õigusega.

¹⁶² Näiteks Boyd et al., 2023, [Automated Emotion Recognition in the Workplace: How Proposed Technologies Reveal Potential Futures of Work](#).

mõjutada koolitatava isiku hindamist, edutamist jne, tingimusel et keelust ei hoita kõrvale ja et emotsioonituvastussüsteemi kasutamine ei mõjuta töösuhteid;

- kõnekeskuses häälte tuvastamise süsteemide kasutamine klientide emotsioonide, näiteks viha või kannatamatuse jälgimiseks ei ole tehisintellektimääruse artikli 5 lõike 1 punktiga f keelatud (näiteks selleks, et aidata töötajatel toime tulla teatavate vihaste klientidega);
- keelatud on tehisintellektisüsteemid, mis jälgivad hübriidtöörühmade emotsionaalset tooni, tuvastades ja tuletades hübriidvideokõnede hääle ja pildi põhjal emotsioone, mis tavaliselt teeniks sotsiaalse teadlikkuse edendamise, emotsionaalse dünaamika juhtimise ja konfliktide ennetamise eesmärki;
- emotsioonituvastuse tehisintellektisüsteemide kasutamine värbamisprotsessis on keelatud;
- emotsioonituvastuse tehisintellektisüsteemide kasutamine katseajal on keelatud;
- kaamerate kasutamine supermarketites töötajate emotsioonide, näiteks õnnetunde jälgimiseks on keelatud;
- kaamerate kasutamine supermarketis või pangas kahtlaste klientide avastamiseks, näiteks selleks, et teha järelalus, et keegi kavatseb röövi toime panna, ei ole tehisintellektimääruse artikli 5 lõike 1 punkti f järgi keelatud, kui on tagatud, et töötajaid ei jälgita ja et on olemas piisavad kaitsemeetmed.

b) Haridusasutused

- (255) Viide **haridusasutustele** on lai ja seda tuleks mõista nii, et see hõlmab nii avalikke kui ka eraõiguslikke asutusi. Õpilaste või üliõpilaste tüüpide või vanuse või konkreetse keskkonna (internetis, kohapeal, kombineeritud õpe¹⁶³ jne) suhtes ei ole piiranguid. Näiteks kuuluvad tehisintellektimääruse artikli 5 lõike 1 punktis f sätestatud keelu kohaldamisalasse kõikide tasandite haridus- ja koolitusasutused, sealhulgas kutsekoolid, st koolid, kus õpilased õpivad oskusi, mis hõlmavad käelist tööd,¹⁶⁴ ja täiendkoolitus¹⁶⁵. Üldiselt akrediteerivad või kiidavad haridusasutusi heaks riiklikud haritusametid või samaväärsed ametiasutused. Oluline on see, et haridusasutused võivad anda tunnistuse (vastavalt sellele on osalemine tunnistuse saamise eeltingimus). Kõnealust keeldu tuleks mõista nii, et seda kohaldatakse kandidaatide suhtes ka vastuvõtuprotsessi käigus.

Näiteks:

- tehisintellektipõhine rakendus, mis kasutab emotsioonituvastust keele õppimiseks internetis väljaspool haridusasutust, ei ole tehisintellektimääruse artikli 5 lõike 1

¹⁶³ Kombineeritud õppimine tähendab rohkem kui ühe lähenemisviisi kasutamist haridus- ja koolitusprotsessis, sealhulgas digitaalsete (sealhulgas veebipõhise õppimise) ja mittedigitaalsete õppevahendite kombineerimist.

¹⁶⁴ Vt nt komisjoni ettepanekule lisatud mõjuhinnaangut, kus mainiti, et konkreetne tehisintellekti kasutamine kutseõppeasutustes kujutab endast intensiivset sekkumist paljudesse põhiõigustesse, nt hindamise ajal: Euroopa Komisjon, [komisjoni talituste töödokument, mõjuhinnaang, lisad, SWD\(2021\) 84 final, osa 2/2](#), lk 43. Vt ka I. Tuomi, *The use of Artificial Intelligence (AI) in education*, Euroopa Parlament, 2020, lk 9–10.

¹⁶⁵ Vt harta artikkel 14.

punkti f järgi keelatud. Seevastu kui õppeasutus nõuab õpilastelt rakenduse kasutamist, on sellise emotsioonituvastussüsteemi kasutamine keelatud;

- haridusasutus, mis kasutab õpilaste veebipõhistes eksamites tehisintellektipõhist tarkvara nende silmade fikseerimispunkti ja liikumise jälgimiseks (et leida pilgu fikseerimise punkt, nt loata materjali kasutamise tuvastamiseks), ei ole keelatud, sest süsteem ei tuvasta ega tuleta emotsioone. Kui süsteemi kasutatakse ka emotsioonide, näiteks emotsionaalse erutuse ja ärevuse tuvastamiseks, siis kuulub see keelu kohaldamisalasse;
- haridusasutustel on keelatud kasutada tehisintellektisüsteemi emotsioonide tuvastamiseks eesmärgiga teha järeldusi õpilaste huvi ja tähelepanu kohta. Kui neid kasutatakse ainult õppimise eesmärgil rollimängu kontekstis (näiteks näitlejate või õpetajate koolitamiseks), on emotsioonituvastussüsteemid lubatud, kui tulemused ei saa mõjutada koolitatava isiku hindamist või sertifitseerimist;
- haridusasutustel on keelatud kasutada tehisintellektisüsteemi emotsioonide tuvastamiseks uute õpilaste vastuvõtukatsete ajal;
- sellise tehisintellektisüsteemi kasutamine, mis võimaldab õppeasutusel veebipõhiste loengute ajal telefonide või muude kanalite kaudu üksteisega rääkivaid üliõpilasi jäädvustada, ei ole keelatud, kuna sellega ei tuletata emotsioone. Kui süsteemi kasutatakse ka emotsioonide, näiteks emotsionaalse erutuse, ärevuse ja huvi tuvastamiseks, kuulub see keelu kohaldamisalasse;
- haridusasutus, mis kasutab emotsioonituvastuse tehisintellektisüsteemi nii õpetajate (töökohal) kui ka õpilaste (hariduses) puhul, on keelatud.

7.2.3. Erandid meditsiinilistel ja ohutusega seotud põhjustel

- (256) Tehisintellektimääruse artikli 5 lõike 1 punktis f sätestatud keeld sisaldab selgesõnalist erandit emotsioonituvastussüsteemide kohta, mida kasutatakse töökohal ja haridusasutustes meditsiinilistel või ohutusega seotud põhjustel, näiteks terapeutiliseks kasutuseks mõeldud süsteemide puhul¹⁶⁶. Arvestades tehisintellektimääruse eesmärki tagada põhiõiguste kõrgetasemeline kaitse, tuleks seda erandit tõlgendada kitsalt.
- (257) Eelkõige tuleks terapeutilise kasutuse all mõista CE-märgistatud meditsiiniseadmete kasutamist. Lisaks ei hõlma see erand emotsioonituvastussüsteemide kasutamist heaolu üldiste aspektide tuvastamiseks. Stressitaseme üldine jälgimine töökohal ei ole tervishoiu või ohutuse eesmärgil lubatud. Näiteks tehisintellektisüsteem, mille eesmärk on tuvastada läbipõlemist või depressiooni töökohal või haridusasutustes, ei kuuluks erandi alla ja jääks keelatuks.
- (258) Selle erandi all tuleks ohutuse mõistet mõista nii, et seda kohaldatakse ainult seoses elu ja tervise kaitsmisega, mitte aga muude huvide, näiteks vara kaitsmiseks varguse või pettuse eest.

¹⁶⁶ Tehisintellektimääruse põhjendus 44.

- (259) Erandi kitsast tõlgendamisest tuleneb, et igasugune meditsiinilistel ja ohutusega seotud kasutus peaks alati piirduma rangelt vajaliku ja proportsionaalse, sealhulgas ajalise, isikliku ja ulatuse piiranguga, ning sellega peaksid kaasnema piisavad kaitsemeetmed. Sellised kaitsemeetmed võivad hõlmata näiteks eelnevat kirjalikku ja põhjendatud eksperdiarvamust, mis on seotud konkreetse kasutusjuhtumiga. Vajadust tuleks hinnata objektiivselt seoses meditsiinilise ja ohutuslase eesmärgiga, mitte viidata tööandja või haridusasutuse vajadustele. Selle hindamise käigus tuleks uurida, kas on olemas vähem sekkuvad alternatiivsed vahendid, mis saavutaksid sama eesmärgi.
- (260) Tööandjad ja pedagoogid peaksid kasutama emotsioonituvastussüsteeme meditsiinilistel ja ohutusega seotud põhjustel ainult selge vajaduse korral¹⁶⁷. Selles kontekstis kogutud ja töödeldud andmeid ei tohi kasutada ühelgi muul eesmärgil. See on eriti oluline, kuna on tõestatud, et tehisintellektipõhise juhtimistarkvara kasutamine töökohal võib negatiivselt mõjutada töötajate tervist ja ohutust. Ihunutikute kaudu toimuv pidev jälgimine võib näiteks suurendada tööstressi, mõjutades samal ajal tootlikkust¹⁶⁸.
- (261) Kuna tehisintellektimääruse põhjenduses 18 jäetakse emotsioonituvastussüsteemide määratlusest välja füüsilised seisundid, nagu valu või väsimus, siis ei kuulu mitmed ohutuse eesmärgil kasutatavad tehisintellektisüsteemid juba praegu selle määratluse alla, sealhulgas näiteks süsteemid, mida kasutatakse kutseliste pilootide või sõidukijuhtide väsimuse tuvastamiseks õnnetuste ennetamise eesmärgil.
- (262) Muud seadused, sealhulgas andmekaitse normid, jäävad tehisintellektimääruse artikli 5 lõike 1 punktis f sätestatud erandi tingimustele vastavate emotsioonituvastussüsteemide suhtes kohaldatavaks¹⁶⁹.
- (263) Emotsioonituvastussüsteemid, mis liigitatakse tehisintellektimääruse artikli 6 lõike 2 ja III lisa punkti 1 alapunkti c kohaselt suure riskiga süsteemideks, peavad vastama tehisintellektimääruse III peatüki 2. jaos kirjeldatud suure riskiga tehisintellektisüsteemidele esitatavatele nõuetele ja tehisintellektimääruse artikli 50 lõikes 3 sätestatud läbipaistvuskohustusele.

Näiteks:

emotsioonituvastust võib kasutada meditsiinilistel põhjustel, et aidata autistlikke töötajaid või õpilasi ning parandada ligipääsetavust pimedate või kurtide jaoks¹⁷⁰. Sellised kasutusviisid kuuluksid tehisintellektimääruse artikli 5 lõike 1 punkti f meditsiinilistel põhjustel tehtava erandi alla.

¹⁶⁷ Kooskõlas ELi tööõigusega peavad tööandjad sellise uue tehnoloogia kasutuselevõtmisel konsulteerima vastavalt liikmesriigi korrale ka töötajate või nende esindajatega. Ilma neid menetlusnõudeid järgimata ei saa selliseid süsteeme tehisintellekti käsitlevale määrusele viidates kasutusele võtta. Nende jaoks on vaja nõusolekut ka kohaldatavate andmekaitsealaste õigusaktide mõistes.

¹⁶⁸ „The Interconnection between the AI Act and the EU’s Occupational Safety and Health Legal Framework“, Global Workplace Law & Policy (kluwerlawonline.com).

¹⁶⁹ Alates 2026. aasta detsembrist kohaldatakse Euroopa Parlamendi ja nõukogu 23. oktoobri 2024. aasta direktiivi (EL) 2024/2831 platvormitöö tingimuste parandamise kohta.

¹⁷⁰ Süsteeme saaks kasutada selleks, et aidata töötajatel või üliõpilastel/õpilastel mõista kolleegide emotsioone jne.

Seevastu emotsioonide tuvastamine õpilaste või töötajate heaolu, motivatsiooniseme ja töö või õppimisega rahulolu hindamiseks ei ole meditsiinilistel põhjustel kasutamine ja see oleks keelatud.

Tööandjal oleks keelatud kasutada töökohal tehisintellektipõhiseid seadmeid või digitaalsete assistente, et mõõta ärevust mõõdetud stressitaseme alusel või mõõta töötajate igavust, välja arvatud juhul, kui kõrgendatud stressitase / kontsentratsiooni puudumine kujutab endast konkreetset ohtu, näiteks ohtlike masinate kasutamisel või ohtlike kemikaalide käitlemisel. Viimasel juhul ei tohi tööandja kasutada andmeid muudel eesmärkidel, näiteks töötaja töötulemuste hindamiseks.

7.3. Soodsamad liikmesriikide õigusaktid

- (264) Tehisintellektimääruse artikli 2 lõikes 11 on sätestatud, et liit või liikmesriigid võivad säilitada või kehtestada „õigus- ja haldusnorme, mis on töötajatele soodsamad, et kaitsta nende õigusi seoses tehisintellektisüsteemide kasutamisega tööandjate poolt“. Samuti võib lubada või edendada töötajate jaoks soodsamaid kollektiivlepinguid.

Näiteks võivad liikmesriigid võtta vastu seadusi, mis näevad ette, et emotsioonituvastussüsteeme ei tohi kasutada meditsiinilistel eesmärkidel.

7.4. Kohaldamisalast välja jäävad olukorrad

- (265) Nagu eespool mainitud, ei kuulu kohaldamisalasse:

- tehisintellektisüsteemid, mis järelavad emotsioone ja tundeid muu kui biomeetriliste andmete põhjal;
- tehisintellektisüsteemid, mis järelavad füüsilisi seisundeid, nagu valu ja väsimus.

- (266) Emotsioonituvastussüsteemid, mida kasutatakse kõikides muudes valdkondades peale töökoha ja haridusasutuste, ei kuulu tehisintellektimääruse artikli 5 lõike 1 punktis f sätestatud keelu alla. Selliseid süsteeme peetakse siiski suure riskiga tehisintellektisüsteemideks¹⁷¹. Samas võivad sellised süsteemid olla teatud juhtudel keelatud tehisintellektimääruse artikli 5 lõike 1 punktide a ja b (kahjulik manipuleerimine ja ärakasutamine) või muude liidu õigusaktide alusel. Kõik muud kohaldatavad õigusaktid, nagu liidu andmekaitsealased õigusaktid, tarbijakaitse jne, kehtivad selliste süsteemide suhtes edasi.

Näiteks:

emotsioonituvastussüsteemid, mida kasutatakse kaubanduslikus kontekstis klientide kõnetamiseks, ei kuulu tehisintellektimääruse artikli 5 lõike 1 punktis f sätestatud keelu alla, olenemata sellest, kas need põhinevad biomeetrilistel andmetel või mitte. Seega ei hõlma keeld selliseid näiteid nagu tehisintellektisüsteemid, mis võimaldavad emotsioonide tuvastamist klahvivajutuse või klientide häälsõnumite põhjal (nt vestlussõnumid, virtuaalsete häälassistentide kasutamine) ning mida kasutatakse

¹⁷¹ Tehisintellektimääruse artikli 6 lõige 2 ja III lisa punkti 1 alapunkt c.

internetiturunduses, et kuvada rakendustes, sealhulgas nutikeskkondades, personaliseeritud sõnumeid ja reklaami (nn arukad reklaamiplakadid).

Sellised kasutusviisid võivad siiski kuuluda tehisintellektimääruse artikli 5 lõike 1 punktides a ja b¹⁷² sätestatud kahjuliku manipuleerimise ja ärakasutamise keeldude kohaldamisalasse, kui kõik nende keeldude kohaldamise tingimused on täidetud.

a) Muud süsteemid, mis ei kuulu kohaldamisalasse

- (267) Rahvahulga kontrolli all hoidmine tähendab üldiselt inimrühmade käitumise kontrollimist ja jälgimist, et tagada (avalik) kord ja ürituse turvalisus. Seda seostatakse sageli suurte rahvahulkade üritustega (nt ameerika jalgpalli või jalgpallimängud, kontserdid jne) või konkreetsete kohtade, näiteks lennujaamade või rongidega. Rahvahulga kontrollimise süsteemid võivad toimida ilma üksikute inimeste emotsioonide tuletamiseta, kui nad näiteks analüüsivad üldist müra- ja meeleolutaset konkreetses kohas. Sellisel juhul ei kuuluks süsteem tehisintellektimääruse artikli 5 lõike 1 punkti f kohaldamisalasse, sest see ei tuleta (konkreetselt) füüsilise isiku emotsioone.
- (268) Siiski võib esineda juhtumeid, kus sellised rahvahulga kontrollimise süsteemid tuletavad üksikisikute emotsioone, näiteks seda, kas on palju vihaseid nägusid. Tavaliselt ei kuulu sellised tehisintellektisüsteemid tehisintellektimääruse artikli 5 lõike 1 punktis f sätestatud keelu alla, kuna neid ei kasutata tavaliselt töökohal ega haridusasutustes.
- (269) Samuti ei kuulu kohaldamisalasse süsteemid, mida kasutatakse meditsiinivaldkonnas, näiteks hooldusrobotid või meditsiinitöötajad, kes kasutavad emotsioonituvastussüsteeme oma töökohal läbivaatuse ajal, ja hääle jälgimise süsteemid, mis analüüsivad hädaabikõnesid.
- (270) Sellised süsteemid kontrollivad sageli isikuid, kes on seal töö kontekstis, näiteks jalgpallistaadioni või keskjaama turvamehed (kus selliseid süsteeme kasutatakse agressiivse käitumise tuvastamiseks) või meditsiinivaldkonna töötajad. Sellistel juhtudel peavad juurutajad kasutama kaitsemeetmeid, et vältida töötajate seiramist. Siiski ei saa täielikult vältida, et sellised süsteemid tuletavad ka nende töötajate emotsioone. Kuna süsteemi peamine eesmärk ei ole hinnata töötajate emotsioone, tuleks neid süsteeme pidada keelu kohaldamisalast välja jäävateks. Selliste süsteemide juurutajad jäävad vastutama selle eest, et nende kasutamine ei avalda töötajatele negatiivset mõju.

8. TEHISINTELLEKTIMÄÄRUSE ARTIKLI 5 LÕIKE 1 PUNKT G: BIOMEETRILINE LIIGITAMINE TEATAVATE TUNDLIKE OMADUSTE PUHUL

- (271) Tehisintellektimääruse artikli 5 lõike 1 punktiga g keelatakse biomeetrilise liigitamise süsteemid, mis liigitavad füüsilisi isikuid individuaalselt nende biomeetriliste andmete alusel, et tuletada või järeldada nende rassi, poliitilisi vaateid, ametiühingusse

¹⁷² Need olukorrad võivad olla keelatud ka muude õigusnormide alusel, näiteks andmete või tarbijakaitse puhul.

kuulumist, usulisi või filosoofilisi veendumusi, seksuaalelu või seksuaalset sättumust. See keeld ei hõlma liidu või riigisisese õiguse kohaselt saadud biomeetriliste andmekogumite märgistamist, filtreerimist või liigitamist, mida võib kasutada näiteks õiguskaitse eesmärgil¹⁷³.

8.1. Põhjendus ja eesmärgid

- (272) Biomeetrilistest andmetest võib isegi ilma asjaomaste isikute teadmata eraldada, tuletada või järeldada mitmesugust teavet, sealhulgas tundlikku teavet, et neid isikuid liigitada. See võib viia ebaõiglase ja diskrimineeriva kohtlemiseni, näiteks kui teenuse osutamisest keeldutakse, sest kedagi peetakse teatud rassi kuuluvaks. Tehisintellektipõhised biomeetrilise liigitamise süsteemid, mille eesmärk on määrata füüsilised isikud konkreetsetesse rühmadesse või kategooriatesse, mis on seotud selliste aspektidega nagu seksuaalne või poliitiline sättumus või rass, rikuvad inimväärikust ja kujutavad endast märkimisväärset ohtu teistele põhiõigustele, näiteks eraelu puutumatusele ja mittediskrimineerimisele. Seega on need tehisintellektimääruse artikli 5 lõike 1 punkti g kohaselt keelatud.

8.2. Keelu põhimõisted ja komponendid

Tehisintellektimääruse artikli 5 lõike 1 punktis g on sätestatud:

„Järgmised tehisintellekti kasutusviisid on keelatud:

g) selliste biomeetrilise liigitamise süsteemide turule laskmine või kasutuselevõtmine sellel konkreetsel eesmärgil või nende kasutamine, mis liigitavad füüsilisi isikuid individuaalselt *nende biomeetriliste andmete alusel*, et tuletada või järeldada nende rassi, poliitilisi vaateid, ametiühingusse kuulumist, usulisi või filosoofilisi veendumusi, seksuaalelu või seksuaalset sättumust; see keeld ei hõlma seaduslikult saadud biomeetriliste andmete, näiteks biomeetrilistel andmetel põhinevate piltide märgistamist või filtreerimist või biomeetriliste andmete kategoriseerimist õiguskaitse valdkonnas;“.

- (273) Selleks, et tehisintellektimääruse artikli 5 lõike 1 punktis g sätestatud keeld oleks kohaldatav, peavad olema täidetud mitu kumulatiivset tingimust:
- (i) kasutusviis peab kujutama endast tehisintellektisüsteemi turule laskmist, kasutusele võtmist sel konkreetsel eesmärgil või kasutamist;
 - (ii) süsteem peab olema biomeetrilise liigitamise süsteem;
 - (iii) liigitada tuleb isikuid individuaalselt;
 - (iv) nende biomeetriliste andmete põhjal;
 - (v) et tuletada või järeldada nende rassi, poliitilisi vaateid, ametiühingusse kuulumist, usulisi või filosoofilisi veendumusi, seksuaalelu või seksuaalset sättumust.
- (274) Keelu kohaldamiseks peavad kõik viis tingimust olema samal ajal täidetud. Esimest tingimust, st tehisintellektisüsteemi turule laskmist, kasutusele võtmist või kasutamist,

¹⁷³ Tehisintellektimääruse põhjendus 30.

analüüsitakse punktis 2.3. Seega kehtib keeld nii tehisintellektisüsteemide pakkujate kui ka juurutajate suhtes, kes on oma vastutuse piires kohustatud selliseid süsteeme mitte turule laskma, kasutusele võtma ega kasutama. Keelu¹⁷⁴ kohaldamise muid tingimusi kirjeldatakse ja analüüsitakse allpool.

- (275) Keeld ei hõlma seaduslikult omandatud biomeetriliste andmekogumite märgistamist või filtreerimist, sealhulgas õiguskaitse eesmärgil.

8.2.1. Biomeetrilise liigitamise süsteem

- (276) „Üksikisiku kategooriatesse jaotamine biomeetrilise süsteemiga on tavaliselt protsess, kus määratakse kindlaks, kas üksikisiku biomeetrilised andmed kuuluvad ühte eelnevalt määratletud omadustega rühma. Sel juhul ei ole tähtis üksikisikut tuvastada või kontrollida, vaid automatiseeritult talle teatav kategooria omistada. Näiteks võib reklaamiekraan näidata erinevaid kuulutusi sõltuvalt seda vaatava üksikisiku vanusest ja soost¹⁷⁵.“ Isikud võidakse liigitada ka lihtsalt statistika põhjustel, ilma et neid tuvastataks ja ilma et nende tuvastamine oleks olnud tegevuse eesmärk.
- (277) Tehisintellektimääruse artikli 3 punktis 40 on „biomeetrilise liigitamise süsteem“ määratletud kui „tehisintellektisüsteem, mille eesmärk on jagada füüsilisi isikuid nende biomeetriliste andmete põhjal konkreetsetesse kategooriatesse, välja arvatud juhul, kui see on teise äriteenuse lisateenus ja rangelt vajalik objektiivsetel tehnilistel põhjustel“. Nagu on selgitatud punktis 7.2.1.d, on mõiste „biomeetrilised andmed“ määratletud tehisintellektimääruse artikli 3 punktis 34. Biomeetrilised andmed hõlmavad eelkõige biomeetrilistel tunnustel põhinevaid käitumisjooni. Biomeetrilise liigitamise ulatus välistab liigitamise riiete või aksessuaaride, näiteks sallide või ristide, ning sotsiaalmeedia aktiivsuse alusel.
- (278) Biomeetriline liigitamine võib tugineda füüsiliste tunnuste kategooriatele (nt näojooned ja kuju, nahavärv), mille alusel isikud konkreetsetesse kategooriatesse liigitatakse. Mõned neist kategooriatest võivad olla eriti tundliku laadiga või liidu mittediskrimineerimise seaduse alusel kaitstud tunnused, näiteks rassiline kuuluvus. Biomeetriline liigitamine võib siiski põhineda ka DNA-l või käitumuslikel aspektidel, näiteks klahvivajutuse analüüsil või isiku kõnnakul¹⁷⁶.
- (279) Selleks, et tegevus ei kuuluks tehisintellektimääruse biomeetriliste andmete liigitamise määratluse kohaldamisalasse, peavad kumulatiivselt olema täidetud kaks tingimust, nimelt et tegevus „on teise äriteenuse lisateenus ja rangelt vajalik objektiivsetel tehnilistel põhjustel“.
- (280) Tehisintellektimääruse põhjenduse 16 järgi on puhtalt lisafunktsioon selline funktsioon, mis on lahutamatult seotud teise äriteenusega, mis tähendab, et seda funktsiooni ei saa objektiivsetel tehnilistel põhjustel kasutada ilma põhiteenuseta ning selle funktsiooni

¹⁷⁴ Tehisintellektisüsteemi turule laskmise, kasutusele võtmise või kasutamise kriteeriumi vt eestpoolt.

¹⁷⁵ Vt artikli 29 alusel asutatud andmekaitse töörühm, [Arvamus 3/2012 biomeetriliste tehnoloogiate arengu kohta](#), WP193, 27.4.2012, lk 6.

¹⁷⁶ Vt artikli 29 alusel asutatud andmekaitse töörühm, [Arvamus 3/2012 biomeetriliste tehnoloogiate arengu kohta](#), WP193, 27.4.2012, lk 16–17. Töörühm viitab siinkohal „pehmele tuvastusele“ (lk 17), st inimeste käitumise või erivajaduste tuvastamisele.

või funktsioonistiku integreerimine ei ole vahend tehisintellektimääruse normide kohaldamisest kõrvalehoidmiseks.

Näiteks on tehisintellektimääruse artikli 5 lõike 1 punkti g kohaselt lubatud järgmised tehisintellekti kasutamise viisid:

- sellised lisafunktsioonid võivad olla näiteks internetipõhistes kauplemiskohtades kasutatavad filtrid näojoonte või kehaehituse liigitamiseks, kuna neid saab kasutada ainult seoses põhiteenusega, mis seisneb toote müümises sellisel viisil, mis võimaldab tarbijal toote virtuaalset proovimist enda peal;
- lisafunktsiooniks võib pidada ka veebipõhistesse sotsiaalvõrgustike teenustesse integreeritud filtreid, millega liigitatakse näojooned või kehaehitus, et võimaldada kasutajatel lisada või muuta pilte või videoid, kuna sellist filtrit ei saa kasutada ilma sotsiaalvõrgustiku teenuste põhiteenuseta, mis seisneb veebisisu jagamises.

Keelatud on aga näiteks järgmised kasutusviisid:

- tehisintellektisüsteem, mis liigitab sotsiaalmeediaplatvormil aktiivseid isikuid nende eeldatava poliitilise orientatsiooni järgi, analüüsides nende platvormile üleslaaditud fotode biomeetrilisi andmeid, et saata neile sihipäraseid poliitilisi sõnumeid. Kuigi sellist süsteemi võidakse kasutada ainult poliitreklaami toetamiseks, ei oleks see „rangelt vajalik objektiivsetel tehnilistel põhjustel“, mistõttu ei ole täidetud tingimused selleks, et see biomeetrilise liigitamise määratluse kohaldamisalast välja jätta;
- tehisintellektisüsteem, mis liigitab sotsiaalmeediaplatvormil aktiivseid isikuid nende eeldatava seksuaalse sättumuse alusel, analüüsides sellel platvormil jagatud fotode biomeetrilisi andmeid, ja pakub selle alusel neile isikutele reklaami, kvalifitseerub biomeetriliseks liigitamiseks tehisintellektimääruse tähenduses. Ka sel juhul ei ole sellise lisafunktsiooni jaoks ranget vajadust, seega ei tehta sellele keelust erandit.

8.2.2. Isikuid liigitatakse individuaalselt nende biomeetriliste andmete alusel

- (281) Biomeetriliste andmete kasutamine füüsiliste isikute kategoriseerimiseks on keelu kohaldamiseks oluline element (vt punktid 8.2.1. ja 7.2.1.d eespool).
- (282) Lisaks sellele peavad füüsilised isikud olema keelu kohaldamiseks liigitatud individuaalselt. Kui see ei ole biomeetrilise liigitamise eesmärk või tulemus, näiteks kui liigitatakse terve rühm ilma üksikisikut uurimata, ei kohaldata selle suhtes keeldu.

Näiteid individuaalse liigitamise kohta:

- tehisintellektisüsteemid, mis hindavad atribuute (loendavad demograafilisi andmeid), sealhulgas näiteks vanust, sugu, etnilist päritolu, võttes aluseks kehalised tunnused, nagu näo, pikkuse või naha, silmade ja juuste värvi (või nende kombinatsiooni);
- tehisintellektisüsteemid, mis suudavad üksikisikuid liigitada ja neid eristada konkreetse tunnuse alusel (nt arm parema silma all) või selle pärast, et neil on tätoveering paremal käel.

Need kasutusjuhtumid on näited individuaalsete biomeetriliste kategooriate kohta. Selleks, et need näited kuuluksid tehisintellektimääruse artikli 5 lõike 1 punktis g sätestatud keelu alla, peavad kõik nimetatud sätte tingimused olema täidetud.

8.2.3. Et tuletada või järeldada nende rassi, poliitilisi vaateid, ametiühingusse kuulumist, usulisi või filosoofilisi veendumusi, seksuaalelu või seksuaalset sättumust

- (283) Tehisintellektimääruse artikli 5 lõike 1 punktis g on keelatud ainult biomeetrilise liigitamise süsteemid, mille eesmärk on tuletada või järeldada piiratud arvul tundlikke omadusi: rassi, poliitilisi vaateid, ametiühingusse kuulumist, usulisi või filosoofilisi veendumusi, seksuaalelu või seksuaalset sättumust.

Näiteks on tehisintellektimääruse artikli 5 lõike 1 punkti g kohaselt keelatud järgmised süsteemid:

- biomeetrilise liigitamise süsteem, mis väidab, et suudab inimese hääle põhjal järeldada tema rassi (see erineb süsteemist, mis liigitab inimesi naha või silmavärvi järgi, või süsteemist, mis analüüsib kuriteoohvrite DNA-d, arvestades nende päritolu. Need süsteemid ei oleks keelatud);
- biomeetrilise liigitamise süsteem, mis väidab, et on võimeline järeldama inimese usulisi veendumusi tema tätoveeringute või näo järgi.

8.3. Kohaldamisalast välja jäävad olukorrad

- (284) Artikli 5 lõike 1 punktis g sätestatud keeld ei hõlma tehisintellektimäärusega hõlmatud tehisintellektisüsteeme, mis tegelevad seaduslikult omandatud biomeetriliste andmekogumite, näiteks biomeetrilistel andmetel põhineva piltide märgistamise või filtreerimisega, sealhulgas õiguskaitse valdkonnas. Seda selgitatakse lähemalt tehisintellektimääruse põhjenduses 30¹⁷⁷.
- (285) Biomeetriliste andmekogumite märgistamine või filtreerimine võib toimuda biomeetrilise liigitamise süsteemide abil just selleks, et tagada, et andmed esindaksid võrdselt kõiki demograafilisi rühmi ja ei esindaks näiteks liiga palju ühte konkreetset rühma. Kui algoritmi treenimiseks kasutatavad andmed on konkreetse rühma suhtes kallutatud (st andmete kogumise viisist tulenevad süstemaatilised erinevused rühmade vahel või andmed on ajalooliselt kallutatud), võib algoritm seda kallutatust korrata, mille tulemuseks võib olla isikute või isikute rühmade ebaseaduslik diskrimineerimine¹⁷⁸. Seetõttu võib kvaliteetse teabe jaoks olla vaja teatud kaitstud tundlikku teavet märgistada – just nimelt selleks, et vältida diskrimineerimist. Tehisintellektimäärus võib isegi nõuda, et märgistamistoimingud vastaksid tehisintellektimääruse nõuetele suure riskiga tehisintellektisüsteemide kohta¹⁷⁹. Seega on selline biomeetriliste andmete märgistamine või filtreerimine selgesõnaliselt

¹⁷⁷ Tehisintellektimääruse põhjendus 30: „See keeld ei tohiks hõlmata selliste biomeetriliste andmetike seaduslikku märgistamist, filtreerimist või liigitamist vastavalt biomeetrilistele andmetele, mis on saadud kooskõlas liidu või liikmesriigi õigusega, nagu kujutiste sorteerimist vastavalt juuksevärvile või silmavärvile, mida saab kasutada näiteks õiguskaitse valdkonnas.“

¹⁷⁸ Samas.

¹⁷⁹ Vt nt tehisintellektimääruse artiklid 10 ja 17.

tehisintellektimääruse artikli 5 lõike 1 punktis g sätestatud keelust välja jäetud. Keeld kehtib ainult juhul, kui biomeetrilisi andmeid liigitatakse rassi, poliitiliste vaadete, ametiühingusse kuulumise, usuliste või filosoofiliste veendumuste, seksuaalelu või seksuaalse sättumuse tuletamiseks.

Märgistamine või filtreerimine on lubatud näiteks järgmistel juhtudel:

- biomeetriliste andmete märgistamine, et vältida juhtumeid, kus mingi etnilise rühma liikmel on väiksem võimalus saada kutse tööintervjuule, sest algoritmi on treenitud andmete põhjal, kus sellel konkreetsel rühmal on halvemad tulemused kui teistel rühmadel¹⁸⁰;
- pilte kasutades patsientide naha- või silmavärvi järgi liigitamine võib olla oluline meditsiinilise diagnoosimise, näiteks vähidiagnooside puhul.

- (286) Tehisintellektimääruse artikli 5 lõike 1 punktis g on samuti sätestatud, et selles sättes ette nähtud keeldu ei kohaldata õiguskaitse valdkonnas seaduslikult saadud andmekogumite märgistamise või filtreerimise suhtes¹⁸¹.

Näiteks hõlmab see seda, kui õiguskaitseasutus kasutab tehisintellektisüsteemi, mis võimaldab märgistada ja filtreerida andmekogumit, mille puhul kahtlustatakse, et see sisaldab laste seksuaalset kuritarvitamist kujutavat materjali. Esimeses etapis kasutaksid õiguskaitseasutused tehisintellektisüsteemide tuge, et tuvastada piltidelt tundlikke andmeid ja neid redigeerida. Lisaks sellele võib filtreerimine ja märgistamine soo, vanuse, biomeetriliste andmete, nagu silmade ja juuste värvuse, armide ja märgistuste järgi aidata ohvreid tuvastada või luua seoseid teiste juhtumitega. Samuti on lubatud kuritarvitajate käte filtreerimine ja märgistamine konkreetsete tunnuste, näiteks sõrmede pikkuse või mis tahes eristavate märkide või tätoveeringute alusel, et aidata tuvastada võimalikke kahtlusluseid.

8.4. Koostoime muude liidu õigusaktidega

- (287) Tehisintellektisüsteemid, mis on ette nähtud biomeetriliseks liigitamiseks isikuandmete kaitse üldmääruse artikli 9 lõikega 1 kaitstud tundlike atribuutide või erijoonte alusel, mis põhinevad biomeetrilistel andmetel, kui need ei ole käesoleva määrusega keelatud, on tehisintellektimääruse¹⁸² kohaselt liigitatud suure riskiga süsteemideks¹⁸³.
- (288) Tehisintellektimääruse artikli 5 lõike 1 punktiga g piiratakse veelgi isikuandmete seadusliku töötlemise võimalusi liidu andmekaitsealaste õigusaktide, nagu isikuandmete kaitse üldmääruse, õiguskaitse direktiivi ja ELi isikuandmete kaitse määruse alusel. Eelkõige välistab tehisintellektimääruse artikli 5 lõike 1 punkt g võimaluse füüsiliste isikute biomeetriliseks liigitamiseks nende biomeetriliste andmete alusel, nagu on määratletud tehisintellektimääruses, et teha järeldusi rassi, poliitiliste vaadete, ametiühingusse kuulumise, usuliste või filosoofiliste veendumuste,

¹⁸⁰ FRA, # *BigData. Discrimination in data supported decision making*, Luxembourg, 2018, 14, lk 5.

¹⁸¹ Tehisintellektimäärus, mis käsitleb biomeetrilise liigitamise süsteemide kasutamist õiguskaitstes, põhineb Euroopa Liidu toimimise lepingu artiklil 16. Vt ka tehisintellektimääruse põhjendus 3.

¹⁸² Tehisintellektimääruse põhjendus 54 ja III lisa punkti 1 alapunkt b.

¹⁸³ Tehisintellektimääruse põhjendus 54 ja III lisa punkti 1 alapunkt b.

seksuaalelu või seksuaalse sättumuse kohta, kuid seaduslikult saadud biomeetriliste andmekogumite märgistamise või filtreerimise suhtes, sealhulgas õiguskaitse valdkonnas, nagu on kirjeldatud eespool, võidakse erandit kohaldada. Lisaks sellele on tehisintellektimääruse artikli 5 lõike 1 punktis g sätestatud keeld kooskõlas õiguskaitse direktiivi artikli 11 lõikega 3, mis keelab selgesõnaliselt igasuguse profiilianalüüsi, mille tulemuseks on diskrimineerimine isikuandmete eriliikide, näiteks rassi, etnilise päritolu, seksuaalse sättumuse, poliitiliste vaadete või usuliste veendumuste alusel.

9. TEHISINTELLEKTIMÄÄRUSE ARTIKLI 5 LÕIKE 1 PUNKT H – REAALAJAS TOIMUVA BIOMEETRILISE KAUGTUVASTAMISE SÜSTEEMID ÕIGUSKAITSE EESMÄRGIL

- (289) Tehisintellektimääruse artikli 5 lõike 1 punktiga h keelatakse reaalajas toimuva biomeetrilise kaugtuvastamise süsteemide kasutamine avalikult juurdepääsetavas ruumis õiguskaitse eesmärkidel, välja arvatud piiratud erandid, mida on ammendavalt kirjeldatud tehisintellektimääruses. Täpsemalt on tehisintellektimääruse artikli 5 lõike 1 punkti h alapunktides i–iii ette nähtud kolm olukorda, kus selliste süsteemide kasutamine võib olla lubatud, kui see on lubatud riigisiseste õigusaktidega ja kui on täidetud tehisintellektimääruse artikli 5 lõigetes 2–7 sätestatud tingimused ja kaitsemeetmed.
- (290) Vastavalt tehisintellektimääruse artikli 5 lõikele 5 võivad liikmesriigid vabalt otsustada, kas ja millistes neist kolmest olukorrast on nende territooriumil lubatud reaalajas toimuva biomeetrilise kaugtuvastamise süsteemide kasutamine avalikult juurdepääsetavas ruumis õiguskaitse eesmärkidel. Kui sellist kasutamist lubavaid ja reguleerivaid riigisiseseid õigusakte ei ole olemas, ei tohi õiguskaitseasutused ja nende nimel tegutsevad üksused selliseid süsteeme õiguskaitse eesmärgil kasutada. Seega on sellise kasutamise eeltingimuseks riigisiseste õigusaktide olemasolu, mis vastavad tehisintellektimääruse asjakohastele nõuetele.
- (291) Tehisintellektimääruse artikli 5 lõike 1 punktiga h keelatakse reaalajas toimuva biomeetrilise kaugtuvastamise süsteemide kasutamine avalikult juurdepääsetavas ruumis ainult õiguskaitse eesmärgil, nii et see säte puudutab ainult selliste süsteemide juurutajaid. Selliste süsteemide turule laskmine ja kasutusele võtmine, samuti muude biomeetrilise kaugtuvastamise süsteemide kasutamine ei ole keelatud, kuid nende suhtes kohaldatakse suure riskiga tehisintellektisüsteeme käsitlevaid norme vastavalt tehisintellektimääruse artikli 6 lõikele 2 ja III lisa alapunktile a¹⁸⁴. Kui liikmesriik lubab reaalajas toimuva biomeetrilise kaugtuvastamise süsteemide kasutamist avalikult juurdepääsetavas ruumis õiguskaitse eesmärgil, lähtudes mis tahes kolmest tehisintellektimääruse artikli 5 lõike 1 punktis h loetletud eesmärgist, kohaldatakse selle kasutamise suhtes ka suure riskiga biomeetrilise kaugtuvastamise süsteeme käsitlevaid õigusnorme.

¹⁸⁴ Lisaks sellele kehtivad erieeskirjad, mida kohaldatakse biomeetrilise kaugtuvastamise süsteemide tagantjärele toimuva kasutamise suhtes õiguskaitse eesmärgil (tehisintellektimääruse artikli 26 lõige 10).

- (292) Lõpetuseks kohaldatakse õiguskaitse eesmärgil tagantjärele toimuva biomeetrilise kaugtuvastamise süsteemide kasutamise suhtes erieeskirju. Selline hilisem kasutamine ei ole keelatud, kuid selle suhtes kehtivad täiendavad kaitsemeetmed seoses suure riskiga tehisintellektisüsteemide kasutuselevõtuga (tehisintellektimääruse artikli 26 lõige 10).

9.1. Põhjendus ja eesmärgid

- (293) Tehisintellektimääruse põhjenduses 32 tunnistatakse, et avalikult juurdepääsetavas ruumis õiguskaitse eesmärgil reaajas toimuva biomeetrilise kaugtuvastamise süsteemid sekkuvad asjaomaste isikute õigustesse ja vabadustesse niivõrd, sest see võib mõjutada suure osa elanikkonna eraelu, tekitada pideva jälgimise tunde ning kaudselt veenda loobuma kogunemisvabaduse ja muude põhiõiguste kasutamisest. Füüsiliste isikute biomeetrilise kaugtuvastamise jaoks mõeldud tehisintellektisüsteemide tehniline ebatäpsus võib kaasa tuua tulemuste kallutatuse ja põhjustada diskrimineerimist. Sellised võimalikud kallutatud tulemused ja diskrimineeriv mõju on eriti olulised vanuse, etnilise päritolu, rassi, soo või puute puhul. Kuna selliste reaajas töötavate süsteemide kasutamise mõju on vahetu ja täiendava kontrolli või parandamise võimalused piiratud, seab selliste süsteemide kasutamine suuremasse ohtu õiguskaitsetoimingute mõjuvälja jäävate isikute õigused ja vabadused.
- (294) Kui aga selliste süsteemide kasutamine on olulise avaliku huvi eesmärgi saavutamiseks rangelt vajalik ja kui olukorrad, mille puhul selline kasutamine võib toimuda, on ammendavalt loetletud ja kitsalt määratletud, kaalub see kasutamine üles põhiõigustega seotud riskid (tehisintellektimääruse põhjendus 33). Selleks et tagada, et selliseid süsteeme kasutatakse vastutustundlikult ja proportsionaalselt, kohaldatakse nende kasutamise suhtes kaitsemeetmeid ning konkreetseid kohustusi ja nõudeid, mis on sätestatud tehisintellektimääruse artikli 5 lõigetes 2–7.

9.2. Keelu põhimõisted ja komponendid

Tehisintellektimääruse artikli 5 lõike 1 punkt h

„Järgmised tehisintellekti kasutusviisid on keelatud:

h) avalikult juurdepääsetavas ruumis reaajas toimuva biomeetrilise kaugtuvastamise süsteemide kasutamine õiguskaitse jaoks, välja arvatud juhul, kui selline kasutamine on vajalik rangelt ainult ühel järgmistest eesmärkidest, ja ainult selleks vajalikus ulatuses:

i) konkreetsete inimröövi, inimkaubanduse või seksuaalse ärakasutamise ohvrite sihipärane otsimine ning kadunud isikute otsimine;

ii) füüsiliste isikute elu või füüsilist turvalisust ähvardava konkreetse, suure ja vahetu ohu või tegeliku ja olemasoleva või tegeliku ja prognoositava terrorirünnaku ohu ärahoidmine;

iii) kuriteo toimepanemises kahtlustatava isiku asukoha kindlaks tegemine või tuvastamine kriminaaluurimise või süüdistuse esitamise või kriminaalkaristuse täitmisele pööramise eesmärgil II lisas osutatud kuritegude eest, mis on asjaomases

liikmesriigis karistatavad vabadusekaotuse või vabadust piirava julgeolekumeetmega, mille maksimaalne pikkus on vähemalt neli aastat.

Esimese lõigu punkt h ei piira määruse (EL) 2016/679 artikli 9 kohaldamist biomeetriliste andmete töötlemise suhtes muudel kui õiguskaitse eesmärkidel.“

- (295) Selleks, et tehisintellektimääruse artikli 5 lõike 1 punktis h sätestatud keeld oleks kohaldatav, peab olema täidetud mitu kumulatiivset tingimust:
- (i) tehisintellektisüsteem peab olema biomeetrilise kaugtuvastamise süsteem,
 - (ii) tegevus seisneb selle süsteemi kasutamises,
 - (iii) reaalajas,
 - (iv) avalikult juurdepääsetavas ruumis ja
 - (v) õiguskaitse eesmärgil.
- (296) Teist tingimust, st tehisintellektisüsteemi kasutamist, on juba analüüsitud suuniste punktis 2.3. Teisi eespool loetletud tingimusi kirjeldatakse ja analüüsitakse täpsemalt allpool.

9.2.1. Biomeetrilise kaugtuvastuse mõiste

- (297) Biomeetrilise tuvastamise tehnoloogia tuvastab, registreerib ja teisendab mõõdetavad füüsilised omadused (näiteks silmade kaugus ja suurus, nina pikkus jne) või käitumuslikud omadused (näiteks kõnnak või hää) masinloetavateks biomeetrilisteks andmeteks (vt punkt 7.2.1.d eespool). Need andmed on kättesaadavad eri vormides: kujutised või mallid, mis on isiku silmatorkavate tunnuste matemaatiline kujutis, mida kasutatakse äratundmise eesmärgil. Biomeetrilise tuvastamise tehnoloogiat kasutatakse kontrollimiseks ja identifitseerimiseks¹⁸⁵.
- (298) Tehisintellektimääruse artikli 3 punkti 41 kohaselt on biomeetrilise kaugtuvastamise süsteem
- „tehisintellektisüsteem, mille eesmärk on tuvastada füüsilisi isikuid tavaliselt eemalt ilma nende aktiivse osaluseta, võrreldes isiku biomeetrilisi andmeid võrdlusandmebaasis sisalduvate biomeetriliste andmetega“.
- (299) See määratlus hõlmab ainult biomeetriliste tuvastussüsteemide identifitseerimisfunktsiooni, mis eeldab asjaomaste isikute aktiivse osaluse puudumist (st neid ei ole sellesse aktiivselt kaasatud) ja mille tulemuseks on nende isikute tunnuste registreerimine tavaliselt eemalt. Identifitseerimiseks võrreldakse kogutud biomeetrilisi andmeid juba võrdlusandmebaasi salvestatud biomeetriliste andmetega (näiteks hoidlas, nagu kriminaalõiguslikus andmebaasis, mis sisaldab kahtlusaluste näokujutisi või malle).

¹⁸⁵ Nagu on biomeetria valdkonna inimesed on selle määratlenud ISO/IEC standardis 2382-37:2022 „Infotehnoloogia. Sõnavara. Biomeetria“ (termin 37.01.03).

a) Ainult identifitseerimise eesmärgil

- (300) Mõiste „biomeetiline tuvastamine“ on määratletud tehisintellektimääruse artikli 3 punktis 35 kui

„inimese füüsiliste, füsioloogiliste, käitumuslike või psühholoogiliste omaduste automaatne tuvastamine füüsilise isiku isikusamasuse kindlakstegemiseks, võrreldes isiku biomeetrilisi andmeid andmebaasis säilitatavate isikute biomeetriliste andmetega“.

- (301) Tehisintellektimääruse põhjenduses 15 on lisaks selgitatud, et sellised inimese tunnused võivad hõlmata

nägu, silmade liikumist, kehakuju, häält, prosoodiat, kõnnakut, kehahoiakut, südame löögisagedust, vererõhku, lõhna ja klahvivajutuste erijooni.

- (302) Biomeetrilise tuvastamise mõiste alla võivad kuuluda ka tehisintellektisüsteemid, mida kasutatakse füüsiliste isikute jälgimiseks, näiteks selleks, et näha, millises suunas kahtlusallane põgeneb. Seda võib järeldada tehisintellektimääruse artikli 5 lõike 1 punkti h alapunktist iii, mis võimaldab kuriteos kahtlustatavate isikute asukoha kindlaks tegemist. Asukoha kindlaks tegemine on võimalik, kui isikut jälgitakse.

- (303) Tehisintellektisüsteemid, mis on ette nähtud biomeetriliseks kontrollimiseks, ei kuulu tehisintellektimääruse artikli 5 lõike 1 punktis h sätestatud keelu kohaldamisalasse¹⁸⁶. Biomeetiline kontroll (või autentimine) seisneb selles, et võrreldakse anduril esitatud andmeid varem teise seadmesse, näiteks nutitelefonis, passi või ID-kaardile salvestatud andmekogumiga. Biomeetrilise kontrolli eesmärk on kontrollida, et konkreetne isik on see, kes ta väidab end olevat.

Biomeetrilise kontrolli näide on reisija näost passikontrolli automaadis tehtud skaneeringu võrdlemine tema passis oleva näokujutisega.

b) Kaugus

- (304) Tehisintellektimääruse artikli 3 punkti 41 kohaselt tähendab kaugtuvastamine biomeetriliste süsteemide võimet tuvastada füüsilisi isikuid tavaliselt eemalt ilma nende aktiivse osaluseta, võrreldes isiku biomeetrilisi andmeid võrdlusandmebaasis sisalduvate biomeetriliste andmetega.

- (305) Biomeetriliste süsteemide kasutamine füüsilise isiku identiteedi kinnitamiseks üksnes selleks, et saada juurdepääs teenusele, avada seade või saada juurdepääsuluba ruumidesse sisenemiseks, ei kuulu mõiste „kaugtuvastamine“ alla (tehisintellektimääruse põhjendus 15). Seda omadust kasutatakse näiteks juurdepääsukontrolli puhul¹⁸⁷.

Näiteks kasutatakse näotuvastussüsteemi selleks, et siseneda piiratud juurdepääsuga alale (nt elektrijaama territooriumile) näo skaneerimise tehnoloogia abil. Süsteem

¹⁸⁶ Tehisintellektimääruse põhjendus 17.

¹⁸⁷ Näiteks Ross A, Jain AK (2015), Biometrics, Overview, väljaandes Li S.Z. ja Jain A.K. (toim), Encyclopedia of Biometrics, (1. väljaanne. Springer Science, New York), lk 289–294.

võrdleb sissepääsukaameras esitatud isiku nägu võrdluspildiga, mis sisaldub hoonesse sisenemise loaga isikute võrdlusandmebaasis.

- (306) Tehisintellektimääruse põhjenduses 17 on selgitatud, et selline väljajätmine keelu kohaldamisalast on põhjendatud asjaoluga, et sellistel süsteemidel on tõenäoliselt väike mõju füüsiliste isikute põhiõigustele võrreldes selliste biomeetrilise kaugtuvastamise süsteemidega, mida võidakse kasutada suure hulga isikute biomeetriliste andmete töötlemiseks ilma nende aktiivse osaluseta. Selles põhjenduses on lisaks selgitatud, et biomeetrilise kaugtuvastamise süsteeme kasutatakse tavaliselt mitme isiku või nende käitumise samaaegseks tajumiseks, et oluliselt hõlbustada füüsiliste isikute tuvastamist ilma nende aktiivse osaluseta. Aktiivseks osaluseks ei piisa sellest, et inimesi teavitatakse kaamerate olemasolust, vaid nad peavad aktiivselt ja teadlikult astuma kaamera ette, mis on paigaldatud viisil, mis soodustab aktiivset osalemist.

Näiteks:

- biomeetrilise kaugtuvastamise süsteemid, mida kasutatakse metroojaamade seintele või lakke paigaldatud kaamerates järelevalve eesmärgil. Selline süsteem vastab kauguse tingimusele;
- seda tingimust ei täida süsteemid, mida kasutatakse metroojaama pääsemiseks, näiteks biomeetrilised metroopiletid, kus isikud osalevad aktiivselt ja lähenevad teadlikult biomeetrilisele andurile, et sisse pääseda.

- (307) Biomeetrilised tuvastussüsteemid, mis töötlevad (kontaktivabasid) sõrmejälgi, kõnnakut, häält, DNA-d, klahvivajutusi ja muid (biomeetrilisi) käitumissignaale, võivad samuti endast biomeetrilise kaugtuvastamise süsteeme kujutada¹⁸⁸.

Näiteks:

- häälel põhinevat biomeetrilise tehnoloogia süsteemi võib kasutada rääkiva isiku tuvastamiseks. Sellisel juhul kogub n-ö biomeetrilise proovi mikrofoni;
- videovalve kaudu võib kasutada kõnnakutuvastussüsteemi ja videotest kontrollitakse automaatselt, kas neid leidub eelnevalt salvestatud mallide vasteid;
- klahvivajutustel põhinevat biomeetrilist tehnoloogiat võib kasutada pettuse teel sõnumit sisestava isiku tuvastamiseks.

Asjaolu, et need süsteemid on toodud biomeetrilise kaugtuvastamise süsteemide näidetena, ei tähenda, et need on tehisintellektimääruse artikli 5 kohaselt keelatud.

- (308) Kui tegemist on ühe õiguskaitseametniku kasutatava kehakaameraga, millel on biomeetrilise kaugtuvastamise võimekus, loetakse kauguse tingimus täidetuks näiteks sadade osalejatega meeleavalduse ajal toimuva üldise filmimise korral.

¹⁸⁸ Euroopa Andmekaitsekoostöö ja Euroopa Andmekaitseinspektori ühisarvamus 5/2021, punkt 11; Euroopa Liidu Nõukogu õigustalituse arvamus, 12302/22, 12. september 2022, punkt 33, ja tehisintellektimääruse põhjendus 15.

c) Võrdlusandmebaas

- (309) Tuvastamine ei ole võimalik ilma võrdlusandmebaasita, mis sisaldab võrdlemiseks biomeetrilisi andmeid. Seega on võrdlusandmebaasi olemasolu tuvastamise eesmärgil võrdlemiseks **tingimata vajalik**¹⁸⁹.

Näiteks kadunud isikute puhul võiks Schengeni infosüsteemi¹⁹⁰ andmebaasi kasutada võrdlusandmebaasina näotuvastuse eesmärgil (kui see tööd alustab).

9.2.2. Reaalajas

- (310) „Reaalajas“ tähendab, et süsteem kogub ja töötleb biomeetrilisi andmeid „koheselt, peaaegu koheselt või igal juhul ilma märkimisväärse viivitusega“¹⁹¹. Kõik töötlemisetapid, st biomeetriliste andmete kogumine, võrdlemine ja tuvastamine, toimuvad samaaegselt või peaaegu samaaegselt, mis võib sisaldada „piiratud lühikest viivitust“, et vältida biomeetrilise kaugtuvastamise süsteemide tagantjärele kasutamise teel keelust kõrvalehoidmist¹⁹². Mõistet „ilma märkimisväärse viivitusega“ ei ole tehisintellektimääruses määratletud. Seda tuleb hinnata iga juhtumi puhul eraldi. Kuna reaalajas või kaugtuvastuseks kasutatavad seadmed on üha enam üks ja seesama seade, millel on erinevad funktsioonid, on erinevus ajaline. Üldiselt on viivitus märkimisväärne vähemalt siis, kui isik on tõenäoliselt lahkunud kohast, kus biomeetrilised andmed koguti.
- (311) Reaalajasüsteeme kasutatakse üldjuhul konkreetses kohas kiire reageerimise hõlbustamiseks, mitte aga isikute tagantjärele tuvastamiseks. Need annavad süsteemi kasutajale võimaluse jälgida jälgitavate isikute liikumist ja neid seirata.

- a) Tehisintellektisüsteem kontrollib kõiki kontserdipaika saabuvasid külastajaid: reaalajas toimuv biomeetriline kaugtuvastamine.
- b) Süsteem filmib kõiki kontserdile saabuvasid külastajaid. Kontserdil leiab aset vahejuhtum. Pärast kontserti kasutatakse videomaterjali peal tuvastussüsteemi, et tuvastada kurjategija: tagantjärele toimuv biomeetriline kaugtuvastamine.

- (312) Kui õiguskaitseasutus teeb isikust mobiilseadme abil salaja pildi ja edastab selle andmebaasi koheseks otsinguks, võib see sõltuvalt asjaoludest kuuluda tehisintellektimääruse artikli 5 lõike 1 punkti h keelu alla.

9.2.3. Avalikult juurdepääsetav ruum

- (313) Tehisintellektimääruse artikli 3 punktis 44 on **avalikult juurdepääsetav ruum** määratletud kui

¹⁸⁹ Tehisintellektimääruse põhjendus 34.

¹⁹⁰ Hoiatusteed teadmata kadunud isikute kohta (SIS II otsuse artikkel 32); nõukogu 12. juuni 2007. aasta otsus 2007/533/JSK, mis käsitleb teise põlvkonna Schengeni infosüsteemi (SIS II) loomist, toimimist ja kasutamist.

¹⁹¹ Tehisintellektimääruse põhjendus 17.

¹⁹² Tehisintellektimääruse artikli 3 punkti 42.

„avalikus või eraomandis füüsiline koht, millele on juurdepääs määramatul arvul füüsilistel isikutel, olenemata sellest, kas kohaldatakse teatavaid juurdepääsutingimusi, ja olenemata võimalikest mahutavuspiirangutest“.

(314) Tehisintellektimääruse põhjenduses 19 on loetletud mitu sellist ruumi iseloomustavat elementi.

- See on määratlemata arvu füüsiliste isikute jaoks juurdepääsetav, olenemata võimalike mahutavuse või turvalisusega seotud piirangutest, nt pääsme või sõidupileti ostmise, eelnev registreerimine või isikute teatav vanus. Ainuüksi juurdepääsu võimalus, näiteks lukustamata uks, ei tähenda, et ruum on avalikult juurdepääsetav, kui on olemas vastupidisele viitavad tähised või asjaolud, näiteks juurdepääsu piiravad märgid. Lisaks sellele võib juurdepääs olla piiratud konkreetsete ja kindlaksmääratud füüsiliste isikutega õiguse alusel, mis on seotud avaliku turvalisuse või julgeolekuga, või ruumi suhtes asjaomaseid volitusi omava isiku selge otsuse alusel.

Näiteks on avalikult juurdepääsetavad ruumid põhimõtteliselt:

- kontserdi toimumise koht, mille puhul osalejad maksavad sissepääsutasu;
- sündmuse toimumise koht, kus korraldatakse mess, mis on suunatud üle 50aastastele osalejatele.

Värvaga suletud ruumi, isegi kui värav on lukustamata, näiteks mitmest majast koosneva aiaga ümbritsetud elamurajooni sissepääsu, ei loeta tavaliselt avalikult juurdepääsetavaks ruumiks. Seevastu suletud elukohas asuvad parki, mille lahtiolekuajad on avalikud ja millele ei ole nendel aegadel juurdepääsupiiranguid, loetakse üldiselt nendel aegadel avalikult juurdepääsetavaks ruumiks ja väljaspool neid aegu suletud ruumiks.

- Omandiõiguse ebaolulisus, st ruum ei pea olema avalik-õiguslikus omandis, et seda saaks pidada avalikult juurdepääsetavaks ruumiks.

Näiteks võib ruum kuuluda eraõiguslikule üksusele või avalik-õiguslikule üksusele või kuuluda avalik-õiguslikule üksusele nii, et seda haldab eraõiguslik isik, ilma et see mõjutaks ruumi olemust.

- Puudub konkreetne tegevus, milleks ruumi kasutatakse – avalikult juurdepääsetav ala ei ole tingimata avaliku teenusega seotud ruum. Lisaks sellele võib avaliku teenusega seotud ruum hõlmata ka ruume, mis ei ole avalikult juurdepääsetavad, st omavalitsuses töötavate ametnike tööruume.

Näiteks võib avalikult juurdepääsetavat ruumi kasutada kaubanduseks, näiteks kauplused, restoranid, kohvikud jne; teenuste pakkumiseks, näiteks pangad, ametialane tegevus (nii arstikabinet kui ka raamatupidamisbüroo), külalismajandus (nt hotell) jne; spordi jaoks, näiteks ujulad, spordisaalid, staadionid jne; transpordi jaoks, nagu bussi-, metroo- ja raudteejaamad, lennujaamad, transpordivahendid jne;

meelelahutuseks, nagu kinod, teatrid, muuseumid, kontserdi- ja konverentsisaalid jne, või vaba aja veetmiseks või muuks, nt avalikud teed ja väljakud, pargid, metsad, mänguväljakud¹⁹³.

(315) Järgmised ruumid ei ole avalikult juurdepääsetavad ruumid tehisintellektimääruse artikli 5 lõike 1 punkti h tähenduses:

- küberruum, kuna see ei ole füüsiline koht tehisintellektimääruse artikli 3 punkti 44 tähenduses;

Seega ei kuulu keelu kohaldamisalasse näiteks jututoad, sotsiaalmeedia, digiplatvormid jne.

- teatud ruumid, mis on mõeldud piiratud arvule isikutele, näiteks tehased, ettevõtted ja töökohad, kus on sissepääsukontroll või piirangud asjaomastele töötajatele või teenusepakkujatele, kuna need on mõeldud ainult asjaomastele töötajatele ja teenusepakkujatele¹⁹⁴;

Näiteks töökohta, kuhu pääseb sissepääsukaardiga, ei loeta põhimõtteliselt avalikult juurdepääsetavaks ruumiks, samas kui kontor, kus ei rakendata sissepääsukontrolli, võib seda olla.

- **vanglad ja piirikontrolliala** ei ole avalikult juurdepääsetavad ruumid¹⁹⁵.

(316) Näiteks piiripunkt ei ole avalikult juurdepääsetav ruum, samas kui piiripunkti viiv tänav või selle läheduses asuv mets üldiselt on.

(317) Mõnel ruumil võib olla kahesugune funktsioon. Näiteks loetakse lennujaama üldkasutatavat ala avalikult juurdepääsetavaks ruumiks, kuid piirikontrolli jaoks ette nähtud ala (kus seisavad tolliametnikud ja toimub passide või isikutunnistuste kontroll) on keelu kohaldamisalast välja jäetud.

(318) Nagu on selgitatud tehisintellektimääruse põhjenduses 19, tuleks seda, kas ruum on avalikult juurdepääsetav, hinnata iga üksikjuhtumi puhul eraldi.

9.2.4. Õiguskaitse eesmärk

(319) Tehisintellektimääruse artikli 5 lõike 1 punktis h sätestatud keeld kehtib biomeetrilise kaugtuvastamise süsteemide õiguskaitse eesmärgil kasutamise suhtes, olenemata õiguskaitsetegevust teostavast üksusest, asutusest või organist.

(320) Tehisintellektimääruse artikli 3 punkti 46 kohaselt on õiguskaitse „tegevus, mida õiguskaitseasutus teostab kuritegude tõkestamiseks, uurimiseks, avastamiseks või nende eest vastutusele võtmiseks või kriminaalkaristuse täitmisele pööramiseks, sealhulgas avalikku julgeolekut ähvardavate ohtude eest kaitsmiseks ja nende ohtude

¹⁹³ Tehisintellektimääruse põhjendus 19.

¹⁹⁴ Tehisintellektimääruse põhjendus 19.

¹⁹⁵ Tehisintellektimääruse põhjendus 19. Muus kontekstis on piirikontrolli määratletud kui määruse (EL) 2016/399 (Schengeni piirieskirjad) kohaselt ja selle eesmärgil piiril toimuv tegevus, millega reageeritakse üksnes piiriületamise kavatsusele või piiriületuse toimingule. See ei hõlma nn piiriala, mis võib ulatuda kuni 50 kilomeetri kaugusele kummalgi pool piiri.

ennetamiseks“. Need eesmärgid on samad, mis on loetletud õiguskaitseDirektiivi artiklis 1¹⁹⁶. Seega võib nende eesmärkide mis tahes tõlgendamine seoses õiguskaitseDirektiiviga olla asjakohane ka tehisintellektimääruses kasutatud mõiste „õiguskaitse“ tõlgendamisel.

- (321) Õiguskaitse eesmärgid hõlmavad kuritegude uurimist, avastamist ja nende eest vastutusele võtmist. Need hõlmavad ka kuritegude tõkestamisega seotud tegevusi, sealhulgas avalikku julgeolekut ähvardavate ohtude eest kaitsmist ja nende ennetamist, enne kui kuritegu on tegelikult toime pandud. Näiteks võib politsei kuritegevuse ennetamise raames võtta sunnimeetmeid demonstratsioonidel, suurtel spordiüritustel ja massirahutustel¹⁹⁷. Lõpetuseks hõlmavad need tegevused karistuste rakendamist, näiteks nende täitmisele pööramist.
- (322) Tehisintellektimääruse artikli 3 punkti 46 kohaselt võivad õiguskaitsetegevust teostada õiguskaitseasutused. Tehisintellektimääruse artikli 3 punktis 45 esitatud mõiste „õiguskaitseasutused“ on sama tähendusega kui õiguskaitseDirektiivi „pädevate asutuste“ mõiste¹⁹⁸. See määratlus hõlmab õiguskaitseasutusi ja volitatud asutusi või üksusi (mis võivad olla eraõiguslikud isikud):

- (a) „ametiasutus, kes on pädev kuritegusid tõkestama, uurima, avastama või nende eest vastutusele võtma või kriminaalkaristusi täitmisele pöörama, sealhulgas kaitsma avalikku julgeolekut ähvardavate ohtude eest ja neid ohte ennetama, või

Selliste ametiasutuste hulka kuuluvad näiteks politsei- ja kriminaalõigusasutused (näiteks prokurörid), kui nad täidavad õiguskaitseülesandeid.

- (b) muu asutus või üksus, kellele liikmesriigi õiguse kohaselt on antud ülesanne teostada avalikku võimu kuritegude tõkestamise, uurimise, avastamise või nende eest vastutusele võtmise ja kriminaalkaristuste täitmisele pööramise, sealhulgas avalikku julgeolekut ähvardavate ohtude eest kaitsmise ja nende ennetamise eesmärgil“.

- (323) Tehisintellektimääruse kohaselt võivad õiguskaitsetegevust teostada muud üksused, asutused või isikud pärast seda, kui neile on liikmesriikide õigusaktidega usaldatud avaliku võimu teostamine eespool loetletud eesmärkidel.
- (324) „Nimel“ tähendab, et õiguskaitseasutus on delegeerinud õiguskaitsetegevuse (või selle osa) teostamise teisele üksusele või isikule, sealhulgas eraõiguslikele isikutele, või on konkreetsetel juhtudel palunud teisel üksusel või isikul tegutseda õiguskaitsetegevuse toetamiseks. Mõlemal juhul peavad õiguskaitseasutused andma juhiseid kõigis olulistes küsimustes ja tegema järelevalvet teise üksuse üle, sest isiku nimel tegutsemine eeldab iseenesest sellist tegutsemist.

¹⁹⁶ Mõned õiguskaitseasutuste tegevused on õiguskaitseDirektiivi kohaldamisalast välja jäetud; näiteks kui nad täidavad haldusülesandeid (nt personalitöö), siis need tegevused toimuvad väljaspool õiguskaitse raamistikku. Need kuuluvad isikuandmete kaitse üldmääruse alla. Vt isikuandmete kaitse üldmääruse põhjendus 19.

¹⁹⁷ ÕiguskaitseDirektiivi põhjendus 12.

¹⁹⁸ ÕiguskaitseDirektiivi artikli 3 punkt 7.

Ülesannete delegeerimine teistele asutustele võib hõlmata näiteks järgmist:

- ühistranspordiettevõtted, kellel on õiguskaitseasutused palunud tagada turvalisuse ühistranspordivõrgustikes õiguskaitseasutuste juhiste järgi ja järelevalve all;
- spordialaliidud, kellel on õiguskaitseasutused palunud tagada turvalisuse spordiüritustel õiguskaitseasutuste juhiste järgi ja järelevalve all;
- pangad, millel õiguskaitseasutused on palunud võtta teatavaid meetmeid konkreetsetel juhtumitel teatavate kuritegude tõkestamiseks õiguskaitseasutuste juhiste järgi ja järelevalve all.

Need tegevused kuuluvad mõiste „õiguskaitse eesmärgil“ alla, kuna need üksused tegutsevad õiguskaitseasutuste nimel. Kui need üksused tegutsevad kuritegude (nt pettus, rahapesu) avastamisel ja tõkestamisel enda nimel, ei loeta neid tehisintellektimääruse artikli 5 lõike 1 punkti h keelu alla kuuluvaks.

- (325) Muude organite või üksuste tegevus kuulub õiguskaitse alla ainult siis, kui neile on usaldatud konkreetne õiguskaitseülesanne.

9.3. Erandid keelust

- (326) Tehisintellektimäärus näeb ette kolm erandit üldisest keelust kasutada avalikult juurdepääsetavas ruumis õiguskaitse eesmärgil reaajas toimuvat biomeetrilist kaugtuvastamist. Tehisintellektimääruse artikli 5 lõike 1 punkti h alapunktides i–iii on ammendavalt loetletud kolm eesmärki, mille saavutamiseks võib anda loa reaajas toimuva biomeetrilise kaugtuvastamise jaoks, samas kui tehisintellektimääruse artikli 5 lõigetes 2–7 on sätestatud sellise loa andmise tingimused ja kaitsemeetmed. Tehisintellektimääruse artikli 5 lõike 1 punkti h alapunkte i–iii ei saa iseenesest kasutada avalikult juurdepääsetavas ruumis õiguskaitse eesmärgil reaajas toimuva biomeetrilise kaugtuvastamise õigusliku alusena. Pigem võib lubada reaajas toimuva biomeetrilise kaugtuvastamise kasutamist ainult liikmesriigi õigusaktiga, mis vastab eelkõige tehisintellektimääruse artikli 5 lõigetes 2–7 sätestatud nõuetele, nagu on nähtud ette tehisintellektimääruse artikli 5 lõikes 2. Järelikult on selline kasutamine alates 2. veebruarist 2025 keelatud, kui puudub liikmesriigi õigusakt, mis lubab reaajas toimuva biomeetrilise kaugtuvastamise kasutamist ühe või mitme nimetatud eesmärgi saavutamiseks.

9.3.1. Põhjendus ja eesmärgid

- (327) Tehisintellektimääruse artikli 5 lõike 1 punkti h alapunktides i–iii sätestatud eesmärkide eesmärk on võimaldada teatavate tehisintellektipõhiste ja uurimisvahendite kasutamist õiguskaitse eesmärkidel. Need eesmärgid on järgmised:

- i) kolme konkreetse raske kuriteo ohvrite ja kadunud isikute sihipärane otsimine (kaitse);
- ii) otsese ohu ennetamine elule või füüsilisele turvalisusele või tegeliku terrorirünnaku ohu ennetamine (ennetamine) ning

iii) teatavate II lisas loetletud raskete kuritegudega seotud kahtlusosaluste ja kurjategijate asukoha kindlaksmääramine või tuvastamine (süüdistuse esitamine / uurimine).

- (328) Nende stsenaariumide puhul on liidu seadusandja tasakaalustanud omavahel ühiskonna julgeolekuvajadusi ja riski, mida reaalses toimivas biomeetrilise kaugtuvastamise süsteemid kujutavad endast nende isikute põhiõigustele, kelle suhtes neid süsteeme rakendatakse. Tehisintellektimääruse põhjenduse 33 kohaselt peavad eesmärgid, mille saavutamiseks on lubatud avalikult juurdepääsetavas ruumis reaalses toimiva biomeetrilise kaugtuvastamise süsteemide kasutamine õiguskaitse eesmärgil, olema rangelt, ammendavalt ja kitsalt määratletud ning ilmnema juhul, kui on olemas range vajadus olulise avaliku huvi eesmärgi saavutamiseks, mille tähtsus kaalub üles põhiõigusi mõjutavad riskid. Igasugune muu avalikult juurdepääsetavas ruumis reaalses toimiva biomeetrilise kaugtuvastamise süsteemide kasutamine õiguskaitse eesmärgil, mida ei ole loetletud tehisintellektimääruse artikli 5 lõike 1 punkti h alapunktides i–iii, on keelatud.

Näiteks on keelatud see, kui politsei kasutaks reaalses biomeetrilise kaugtuvastamise süsteemi poevarga tuvastamiseks ja tema näokujutiste võrdlemiseks kriminaalõiguslike andmebaasidega, kuna see ei kuulu ühegi tehisintellektimääruse artikli 5 lõike 1 punkti h alapunktides i–iii loetletud eesmärgi alla.

9.3.2. Kolme liiki raskete kuritegude ohvrite ja kadunud isikute sihipärane otsimine

- (329) Vastavalt tehisintellektimääruse artikli 5 lõike 1 punkti h alapunktile i on avalikult juurdepääsetavas ruumis reaalses toimiva biomeetrilise kaugtuvastamise süsteemide kasutamine õiguskaitse eesmärgil lubatud inimröövi, inimkaubanduse või seksuaalse ärakasutamise ohvrite sihipäraseks otsimiseks ning kadunud isikute otsimiseks, kui see on rangelt vajalik ja vastab tehisintellektimääruse artikli 5 lõigetes 2–7 sätestatud tingimustele.

a) Kolme liiki kuritegude ohvrite sihipärane otsimine

- (330) Tehisintellektimääruse artikli 5 lõike 1 punkti h alapunktis i kirjeldatud stsenaariumi eesmärk on aidata õiguskaitseasutustel otsida kolme raske kuriteo ohvreid.
- (331) Sihipärane otsing hõlmaks ohvrite asukoha kindlaksmääramist ja tuvastamist.

Kolme liiki kuriteod

- (332) Tehisintellektimääruse artikli 5 lõike 1 punkti h alapunktis i on loetletus kolme raske kuriteo konkreetsete ohvrite sihipärane otsimine: inimrööv, inimkaubandus ja seksuaalne ärakasutamine¹⁹⁹.

¹⁹⁹

Inimrööv, inimkaubandus ja seksuaalne ärakasutamine on kolm kuriteoliiki, mille puhul võib Euroopa vahistamismäärus anda põhjuse Euroopa vahistamismääruse väljaandmiseks ning kahtlusosaluse või süüdistatava isiku vahistamismääruse väljaandnud riigile üleandmiseks. Need kolm kuritegu on enamasti (kuid mitte alati) seotud naiste ja lastega. Euroopa Komisjoni rände- ja siseasjade peadirektoraadi andmetel on peaaegu 40 protsenti ohvritest ELi kodanikud ning enamik neist on naised ja lapsed, kellega kaubitsetakse seksuaalse ärakasutamise eesmärgil. Meessoost ohvrite arv on kümne aastaga peaaegu kahekordistunud. Nendega

Kui näiteks laps röövatakse ja on konkreetseid märke sellest, et röövija kavatseb lapse autoga ühest kohast teise viia, võib politsei kasutada reaalsajas biomeetrilise kaugtuvastamise süsteemi selle lapse sihipäraseks otsimiseks, kuid ta peab määratlema lapse tuvastamiseks süsteemi kasutamise piirid ja kestuse.

b) Kadunud isikute otsimine

- (333) Esimene stsenaarium hõlmab ka kadunud isikute otsimist²⁰⁰.
- (334) Võib teha vahet kadunud laste ja kadunud täiskasvanute vahel, sest kadunud täiskasvanu vabatahtlik kadumine ei käivita alati otsinguid. Kehtivad õigusnormid kadunud laste kohta on liikmesriigiti väga erinevad²⁰¹. Igal juhul lubab tehisintellektimääruse artikli 5 lõike 1 punkti h alapunkt i kasutada reaalsajas toimuvat biomeetrilise kaugtuvastamise süsteemi ainult kadunud isikute otsimiseks õiguskaitse eesmärgil.
- (335) Täiskasvanu kadumine ei too alati kaasa seda, et politsei hakkab seda isikut otsima, sest täiskasvanutel on õigus kaduda. Otsimine võib olla seotud isiku õigusliku staatusega (hooldusallane), tema tervisliku seisundiga (psüühikahäire), enesetapukirja olemasoluga, aga ka lahkumisega ilma isiklike asjadeta. Kui kadumise asjaolud annavad põhjust muretsemiseks, võib kadumisest teatada politseile, et alustada otsinguid.
- (336) Mõnes liikmesriigis võib kadunud isiku otsimine toimuda haldusmenetluse raames, mitte õiguskaitse eesmärgil. Näiteks kui haavatav isik on kadunud, kuid puudub kuriteokahtlus või mõni muu õiguskaitse eesmärk, ei toimuks reaalsajas biomeetrilise kaugtuvastamise süsteemide kasutamine selle isiku otsimiseks õiguskaitse eesmärgil ja seega kuuluks see isikuandmete kaitse üldmääruse kohaselt sellise kasutamise eeskirjade alla.

9.3.3. Otseste elu ähvardavate ohtude ja terrorirünnakute ärahoidmine

- (337) Tehisintellektimääruse artikli 5 lõike 1 punkti h alapunktis ii on nimetatud teine stsenaarium, mille puhul on lubatud avalikult juurdepääsetavas ruumis reaalsajas toimuva biomeetrilise kaugtuvastamise kasutamine õiguskaitse eesmärgil, kui see on rangelt vajalik ja seda tehakse tehisintellektimääruse artikli 5 lõigetes 2–7 sätestatud tingimustel:

„füüsiliste isikute elu või füüsilist turvalisust ähvardava konkreetse, suure ja vahetu ohu või tegeliku ja olemasoleva või tegeliku ja prognoositava terrorirünnaku ohu ärahoidmine“.

kaubitsetakse sunniviisilise töö ja sunniviisilise kerjamise eesmärgil, samas kui enamiku naiste ja lastega kaubitsetakse seksuaalse ärakasutamise eesmärgil. https://home-affairs.ec.europa.eu/policies/internal-security/organised-crime-and-human-trafficking/together-against-trafficking-human-beings_en.

²⁰⁰ Mõistet „kadunud isik“ ei ole ELi tasandil määratletud. Nõukogu 2021. aasta detsembri järeldustes teadmata kadunud isikute osas tehtava piiriülese politseikoostöö tõhustamise kohta võtab nõukogu selle määratlemisel aluseks nii Euroopa Nõukogu soovitusel CM/Rec (2009) 12 kui ka riiklikes õigusnormides esitatud kadunud isiku määratluse. Nõukogu järeldused (2021) 14808/21, punkt 11, lk 4.

²⁰¹ Euroopa Komisjon, Euroopa rändevõrgustik, *How do EU Member States treat cases of missing unaccompanied minors?*, EMN Inform, 2020.

a) Füüsiliste isikute elu või füüsilist turvalisust ähvardav konkreetne, suur ja vahetu oht

- (338) Vastavalt harta artiklile 2, mis tagab õiguse elule, peavad liit ja liikmesriigid kaitsma üksikisikute elu. Tehisintellektimääruse artikli 5 lõike 1 punkti h alapunktis ii on sätestatud kriteeriumid, mis puudutavad ohtu elule ja mille korral võib avalikult juurdepääsetavas ruumis kasutada reaalsajas toimuva biomeetrilise kaugtuvastamise süsteeme, ning need eeldavad 1) konkreetse, 2) suure ja 3) vahetu ohu olemasolu 4) füüsiliste isikute elule või füüsilisele ohutusele. Oht ei pea piirduma tuvastatud üksikisikute või rühmaga, kuna see puudutab füüsilisi isikuid üldiselt.
- (339) Tehisintellektimääruse põhjenduses 33 on selgitatud, et vahetu oht füüsiliste isikute elule või füüsilisele turvalisusele võib hõlmata ka vahetut ohtu elutähtsale taristule,²⁰² „kui sellise elutähtsa taristu kahjustada saamine või hävimine ohustaks vahetult isiku elu või füüsilist turvalisust, sealhulgas elanikkonna esmatarbekaupadega varustamise või riigi põhiülesannete täitmise tõsise kahjustamise kaudu“.

Näiteks²⁰³:

elutähtsa taristu (nt elektrijaama, veevarustuse või haigla) tõsine kahjustada saamine ja hävimine võib põhjustada vahetut ohtu inimese elule või füüsilisele turvalisusele, kui elanikkonna esmatarbekaupadega varustamise katkemine (elektri või joogivee puudumine pikaks ajaks, eriti sooja või külma ilmaga jne) tekitab tõsist kahju.

- (340) Seda, mis kujutab endast otsest ohtu füüsiliste isikute elule või füüsilisele turvalisusele, määratletakse ja hinnatakse lõppkokkuvõttes liikmesriigi tasandil, tuginedes tema õigusaktidele kooskõlas ELi õigusega, võttes eelkõige arvesse tehisintellektimääruse artikli 5 põhielemente ja põhjendusi. See tuleb sätestada / sellele tuleb viidata õigusaktides, mille liikmesriigid peavad vastu võtma, et kasutada erandeid, mis puudutavad avalikult juurdepääsetavas ruumis reaalsajas toimuva biomeetrilise kaugtuvastamise süsteemide kasutamist õiguskaitse eesmärgil.
- (341) **Vahetu** oht elule või füüsilisele turvalisusele on oht, mis võib tekkida iga hetk ning mille tõttu „**on vaja võtta koheseid meetmeid**“²⁰⁴. **Suur** oht füüsilisele ohutusele on seotud tõsiste kehavigastustega.
- (342) Konkreetne oht tähendab, et oht on selgelt määratletud, individuaalne ja konkreetne, st see ei tohiks olla hüpoteetiline ega olla seotud teatud ohtudega üldiselt.

Näiteks antakse politseile teada, et endine üliõpilane plaanib oma endises ülikoolis inimohvritega rünnakut, kuna ta tahab kätte maksta mitmele endisele kursusekaaslasele. Politsei saab teavet rünnaku vahetusest, sihtkohaks olevast koolist ja relvadest, mida õpilane oma plaanide elluviimiseks kasutada kavatseb.

²⁰² Nagu on määratletud direktiivi (EL) 2022/2557 artikli 2 punktis 4.

²⁰³ Tehisintellektimääruse põhjendus 33.

²⁰⁴ Määruse (EL) 2023/1543 põhjendus 37.

- (343) Konkreetne oht ei pea olema tahtlik. Ka tahtmatu tegevus võib põhjustada ohtu elule või füüsilisele turvalisusele.

b) Tegelik ja olemasolev või tegelik ja prognoositav terrorirünnaku oht

- (344) See osa teisest stsenaariumist, mida on kirjeldatud tehisintellektimääruse artikli 5 lõike 1 punkti h alapunktis ii, koosneb mitmest elemendist: terrorirünnaku ohu olemasolu ja ohu tunnused, mis peavad olema tegelikud ja olemasolevad või tegelikud ja prognoositavad.

Terrorirünnaku oht

- (345) Ohu olemasolu ja raskusastme hindamine toimub riiklikul tasandil, kui hinnatakse riigi julgeoleku kaitsmiseks võetava meetme tegelikke asjaolusid, täpsemalt terrorirünnaku korral. **Terrorismiohu tase määratakse riiklikul tasandil** ning see erineb liikmesriikide lõikes. Näiteks Madalmaades on ohutasemeid viis,²⁰⁵ Belgias neli,²⁰⁶ Prantsusmaal kolm²⁰⁷ ja Rootsis viis²⁰⁸. Artikli 5 lõike 1 punkti h alapunktis ii kasutatud fraas „tegelik ja olemasolev või tegelik ja prognoositav oht“ on siiski liidu õiguse autonoomne mõiste ja seda tuleks seetõttu põhimõtteliselt hinnata riiklikest määratlustest sõltumatult. Oht ei ole seotud terrorismiga üldiselt, vaid konkreetselt terrorirünnaku ohuga.

Ohu omadused: tegelik ja olemasolev või tegelik ja prognoositav

- (346) Ohu raskusastme tase, mis peab olema saavutatud selleks, et võimaldada avalikult juurdepääsetavas ruumis reaajas biomeetrilise kaugtuvastamise süsteemide kasutamist õiguskaitse eesmärgil, on inspireeritud Euroopa Liidu Kohtu kohtupraktikast andmete säilitamise ja reisijate nimede registreerimise meetmete kohta, mille eesmärk on kaitsta riiklikku julgeolekut, eelkõige terrorirünnakute eest. Euroopa Liidu Kohtu sõnul peab nendes kontekstides „oht riigi julgeolekule olema tegelik ja vahetu või vähemalt ettearvatav, mis eeldab piisavalt konkreetsete asjaolude esinemist“²⁰⁹.

Ärahoidmine

- (347) Vastupidiselt tehisintellektimääruse artikli 5 lõike 1 punkti h alapunktile i ja artikli 5 lõike 1 punkti h alapunktile iii ei ole artikli 5 lõike 1 punkti h alapunktis ii kirjeldatud stsenaariumis täpsustatud, et reaajas toimuvat biomeetrilise kaugtuvastamist võib kasutada konkreetse isiku asukoha kindlaks tegemiseks või tuvastamiseks. Selle eesmärk on konkreetse ohu ärahoidmine. Seega võib stsenaarium hõlmata ka reaajas toimuvat biomeetrilise kaugtuvastamise kasutamist n-ö liikvel olevate terroristide, st mitme sama ohuga seotud isiku tuvastamiseks ja jälgimiseks, kui on konkreetseid

²⁰⁵ <https://www.government.nl/topics/counterterrorism-and-national-security/risk-of-an-attack-threat-level>.

²⁰⁶ <https://cuta.belgium.be>. <https://crisiscenter.be/en/risks-belgium/security-risks/terrorism-and-extremism>.

²⁰⁷ <https://www.sgdsn.gouv.fr/vigipirate#>; <https://www.sgdsn.gouv.fr/files/files/Vigipirate/20160130-np-sgdsn-pse-tackling-terrorism-together.pdf>.

²⁰⁸ <https://www.krisinformation.se/en/hazards-and-risks/terrorism>.

²⁰⁹ Kohtuotsus, Euroopa Kohus, 20. september 2022, *SpaceNet*, C-793/19 (liidetud kohtuasjad C-793/19, C-794/19), ECLI:EU:C:2022:702, punkt 93.

märke, et need isikud kavatsevad terrorirünnaku toime panna, kuid ei ole selge, kus nad seda kavatsevad.

Reaalajas biomeetriline kaugtuvastamine, et hoida ära terrorirünnak pargis

Politseile teatatakse, et üks isik jookseb pargis ringi ja otsib inimesi, keda noaga rünnata, karjudes samal ajal vägivaldseid äärmuslikke loosungeid, mis on tavaliselt seotud terrorirünnakute ja terrorirühmitustega. Kui liikmesriik on andnud loa reaalajas toimuva biomeetrilise kaugtuvastamise kasutamiseks tehisintellektimääruse artikli 5 lõike 1 punkti h alapunktis ii kirjeldatud stsenaariumi puhul, võivad õiguskaitseasutused kasutada reaalajas toimuvat biomeetrilist kaugtuvastamist isiku tuvastamiseks ja tema asukoha määramiseks pargis ja selle ümbruses, et rünnak ära hoida, kui muud artikli 5 lõigetes 2–7 sätestatud tingimused on täidetud.

9.3.4. Teatud kuritegudes kahtlustatavate isikute asukoha kindlaksmääramine ja tuvastamine

- (348) Tehisintellektimääruse artikli 5 lõike 1 punkti h alapunktis iii on lubatud reaalajas toimuva biomeetrilise kaugtuvastamise kasutamine avalikult juurdepääsetavas ruumis järgmisel eesmärgil: „kuriteo toimepanemises kahtlustatava isiku asukoha kindlaks tegemine või tuvastamine kriminaaluurimise või süüdistuse esitamise või kriminaalkaristuse täitmisele pööramise eesmärgil II lisas osutatud kuritegude eest, mis on asjaomases liikmesriigis karistatavad vabadusekaotuse või vabadust piirava julgeolekumeetmega, mille maksimaalne pikkus on vähemalt neli aastat“.

Tehisintellektimääruse II lisas on esitatud ammendav loetelu rasketest kuritegudest, mille puhul võib lubada reaalajas toimuva biomeetrilise kaugtuvastamise kasutamist eespool nimetatud eesmärgil. Need kuriteod on järgmised:

- terrorism,
- inimkaubandus,
- laste seksuaalne ärakasutamine ja lapsporno,
- ebaseaduslik kauplemine narkootiliste või psühhotroopsete ainetega,
- ebaseaduslik kauplemine relvade, laskemoona või lõhkeainetega,
- tahtlik tapmine, raskete kehavigastuste tekitamine,
- ebaseaduslik kauplemine inimorganite või -kudedega,
- ebaseaduslik kauplemine tuumamaterjalide ja radioaktiivsete ainetega,
- inimrööv, ebaseaduslik vabadusevõtmine või pantvangi võtmine,
- Rahvusvahelise Kriminaalkohtu pädevusse kuuluvad kuriteod,
- õhusõiduki või laeva kaaperdamine,
- vägistamine,

– keskkonna vastu suunatud kuriteod,
 – organiseeritud või relvastatud rööv,
 sabotaaž,
 osalemine kuritegelikus organisatsioonis, mis on seotud ühe või mitme eespool
 loetletud kuriteoga.

a) Asukoha kindlaks tegemine ja tuvastamine

- (349) Liikmesriik võib lubada avalikult juurdepääsetavas ruumis reaalajas toimuva biomeetrilise kaugtuvastamise süsteemide kasutamise õiguskaitse eesmärgil, et leida ja tuvastada kuriteos kahtlustatav isik, et viia läbi kriminaaluurimine, võtta kõnealune isik toime pandud kuriteo eest vastutusele või pöörata olemasolev karistus täitmisele.

b) Kahtlusalused ja kuriteo toimepanijad

- (350) Tehisintellektimääruse artikli 5 lõike 1 punkti h alapunkt iii hõlmab kahte isikute kategooriat: kahtlusalused ja kuriteo toimepanijad. Kahtlusalune on isik, kelle puhul on põhjendatud alust arvata, et ta on toime pannud kuriteo, ja kelle süüteo osalemise kohta on juba kogutud piisavalt tõendeid. Kuriteo toimepanija on isik, keda süüdistatakse või kes on süüdi mõistetud kuriteo toimepanemises. Samad tingimused (II lisas loetletud kuritegu ja maksimaalne karistusaeg vähemalt neli aastat) kehtivad ka tehisintellektimääruse II lisas loetletud kuritegude toimepanemise kaasosalise asukoha kindlaks tegemiseks või tuvastamiseks.

c) Raskete kuritegude loetelu

- (351) Ainult rasked kuriteod õigustavad avalikult juurdepääsetavas ruumis reaalajas biomeetrilise kaugtuvastamise süsteemide kasutamist õiguskaitse eesmärgil.
- (352) Esimesed viis tehisintellektimääruse II lisas loetletud kuritegu on samad kui piiriülese mõõtmega rasked kuriteod, mis on loetletud Euroopa Liidu toimimise lepingu artiklis 83, samas kui teised õigusrikkumised on õiguskaitsealase koostöö prioriteedid²¹⁰. Mõned neist (nt inimrööv, ebaseaduslik kauplemine tuumamaterjalide või radioaktiivsete ainetega) võivad olla seotud terrorismiga²¹¹.
- (353) Kuigi kõigi II lisas loetletud kuritegude puhul võib kahtlusaluse või kuriteo toimepanija jaoks väljastada Euroopa vahistamismääruse, ei ole reaalajas toimuva biomeetrilise kaugtuvastamise kasutamise puhul, et leida ja tuvastada mõne nimetatud raskes kuriteos kahtlustatav isik, vaja Euroopa vahistamismäärust.
- (354) Lisaks sellele peab reaalajas toimuva biomeetrilise kaugtuvastamise kasutamiseks olema asjaomane kuritegu asjaomases liikmesriigis karistatav vabadusekaotusega või vabadust piirava julgeolekumeetmega, mille maksimaalne pikkus on vähemalt neli aastat.

²¹⁰ Europol prioriteedid.

²¹¹ Vt põhjendus 33 ja vt terroriaktide määratlus direktiivi (EL) 2017/541 artiklis 3.

Ühes linnas rahvarohke festivali ajal kasutavad politseiasutused reaalsajas näotuvastustehnoloogiat, et jälgida festivali ümbrust ja tuvastada tagaotsitavad isikud, kellel on täitmata vahistamismäärus ebaseadusliku uimastikaubanduse ja seksuaalkuritegude eest. Erinevates festivali sissepääsudes kasutab politsei reaalsajas videomaterjali teisaldatava kaamera eest mööduvatest inimestest, et võrrelda nende nägusid tagaotsitavate isikute nägude jälgimisnimekirjaga.

Esiteks, mis puudutab õigusrikkumiste liike, siis saab biomeetrilist kaugtuvastamist kasutada ebaseadusliku uimastikaubanduse puhul. Seksuaalkuritegusid aga selles õigusrikkumiste loetelus ei ole, välja arvatud juhul, kui need on seotud laste seksuaalse ärakasutamise, laste seksuaalset kuritarvitamist kujutava materjali või vägistamisega. Politseil ei ole lubatud kasutada reaalsajas toimuva näotuvastuse tehnoloogiaid laialt ja konkreetselt suunitlemata viisil, st lootuses leida tagaotsitavad kurjategijad ja nad tänavalt kinni püüda.

Olukord on teistsugune, kui politsei on saanud füüsilise kirjelduse koos fotoga tagaotsitavast isikust, kelle kohta on väljastatud Euroopa vahistamismäärus ebaseadusliku uimastikaubanduse eest, ja neil on põhjust arvata, et ta viibib festivalil. Sellisel juhul võib reaalsajas näotuvastustehnoloogia kasutamine selleks, et tuvastada sihtmärgiks olev isik, kuuluda tehisintellektimääruse artikli 5 lõike 1 punkti h alapunkti iii kohaldamisalasse.

Pärast jõuluturul toimunud rasket terrorirünnakut, mille käigus hukkus 12 inimest, kasutab politsei reaalsajas näotuvastustehnoloogiat, et tuvastada kurjategija ja näha, kuhu ta põgeneb. Sellega seoses kasutavad nad ka reaalsajas näotuvastustehnoloogiat lähedalasuvast rongijaamas ja sealt vahetult pärast rünnakut väljuvate rongide sihtjaamades. Terrorirünnaku korral võib selline kasutamine olla tehisintellektimääruse artikli 5 lõike 1 punkti h alapunkti iii kohaselt lubatud.

- (355) Artikli 5 lõike 1 punkti h alapunktis i kirjeldatud stsenaariumiga hõlmatud kuritegude puhul võib luua seose tehisintellektimääruse artikli 5 lõike 1 punkti h alapunkti i ja artikli 5 lõike 1 punkti h alapunkti iii vahel. Kuigi reaalsajas toimuva biomeetrilise kaugtuvastamise süsteeme võib kasutada ohvri või kadunud isiku leidmiseks, võib neid süsteeme kasutada ka inimkaubanduse, laste seksuaalse ärakasutamise (nagu on loetletud II lisas) ja inimröövi (kui artikli 5 lõike 1 punkti h alapunktis i nimetatud inimröövi loetakse tehisintellektimääruse II lisas loetletud inimrööviks) toimepanija või selles kahtlustatava isiku asukoha kindlaks määramiseks ja tuvastamiseks. Samuti võib luua seose tehisintellektimääruse artikli 5 lõike 1 punkti h alapunktide ii ja iii vahel: reaalsajas toimuva biomeetrilise kaugtuvastamise süsteeme võib kasutada artikli 5 lõike 1 punkti h alapunkti ii kohaldamisalasse kuuluva ohu ennetamiseks ja kui oht realiseerub, võib neid süsteeme kasutada liikvel oleva kuriteo toimepanija tuvastamiseks/leidmiseks.

10. KAITSEMEETMED JA ERANDITE TEGEMISE TINGIMUSED (TEHISINTELLEKTIMÄÄRUSE ARTIKLI 5 LÕIKED 2–7)

10.1. Sihtmärgiks olev isik ja kaitsemeetmed (tehisintellektimääruse artikli 5 lõige 2)

Tehisintellektimääruse artikli 5 lõikes 2 on sätestatud:

„Kui kasutatakse reaalajas toimuva biomeetrilise kaugtuvastamise süsteemi avalikult juurdepääsetavas ruumis õiguskaitse jaoks ükskõik millisel lõike 1 esimese lõigu punktis h osutatud eesmärgil, toimub kasutus selles punktis sätestatud eesmärkidel üksnes selleks, et kinnitada konkreetselt sihtmärgiks oleva isiku isikusamasust, ning selle puhul võetakse arvesse järgmisi elemente:

- (a) millist laadi on olukord, kus süsteemi võidakse kasutada; eeskätt see, milline oleks kahju raskusaste, tõenäosus ja ulatus juhul, kui süsteemi ei kasutataks;
- (b) millised on süsteemi kasutamise tagajärjed kõigi asjaomaste isikute õiguste ja vabaduste seisukohast; eeskätt see, milline on tagajärgede raskusaste, tõenäosus ja ulatus.

Ühtlasi peab reaalajas toimuva biomeetrilise kaugtuvastamise süsteemi kasutamine avalikult juurdepääsetavas ruumis õiguskaitse jaoks ükskõik millisel käesoleva artikli lõike 1 esimese lõigu punktis h osutatud eesmärgil olema vastavuses kasutamise suhtes kehtivate vajalike ja proportsionaalsete kaitsemeetmete ja tingimustega kooskõlas selle kasutamist lubava siseriikliku õigusega ning seda eeskätt ajaliste, geograafiliste ja isikutega seotud piirangute osas. Reaalajas toimuva biomeetrilise kaugtuvastamise süsteemi kasutamine avalikult juurdepääsetavas ruumis on lubatud üksnes juhul, kui õiguskaitseasutus on viinud lõpule põhiõigustele avalduva mõju hindamise, nagu on sätestatud artiklis 27 ja on registreerinud süsteemi ELi andmebaasis vastavalt artiklile 49. Põhjendatud kiireloomulistel juhtudel võib selliseid süsteeme siiski hakata kasutama ilma neid ELi andmebaasis registreerimata, eeldusel et sellist luba taotletakse põhjendamatult viivitusega.“

- (356) Kui kasutatakse reaalajas toimuva biomeetrilise kaugtuvastamise süsteeme, et saavutada üks tehisintellektimääruse artikli 5 lõike 1 punkti h alapunktides i–iii loetletud eesmärkidest, kohaldatakse selle suhtes teatavaid kaitsemeetmeid ja tingimusi, mis on üksikasjalikult sätestatud tehisintellektimääruse artikli 5 lõigetes 2–7.
- (357) Esiteks on avalikult juurdepääsetavas ruumis reaalajas biomeetrilise kaugtuvastamise süsteemide kasutamine õiguskaitse eesmärgil lubatud ainult selleks, et „kinnitada konkreetselt sihtmärgiks oleva isiku isikusamasust“. Selle esimese tingimuse eesmärk on seada tasakaalu ühelt poolt olukorra tõsidus ja kahju, mille tooks kaasa süsteemi kasutamata jätmine, ning teiselt poolt tehnoloogia mõju üksikisikute õigustele ja vabadustele. Selle eesmärk on vältida massilist jälgimist, võttes reaalajas toimuvat biomeetrilist kaugtuvastamist juurutades sihtmärgiks üksikisiku. Sellest tulenevalt tuleks reaalajas toimuva biomeetrilise kaugtuvastamise süsteemi juurutamine avalikult

juurdepääsetavas ruumis õiguskaitse eesmärgil lubada ainult sihtmärgiks olevate isikute puhul.

- (358) Väljendi „isikusamasuse kinnitamine“ kasutamine, selle asemel et kasutada fraasi „tuvastamine“, on mõeldud põhiõiguste täiendavaks kaitseks, mis piirab konkreetse suunitlusega jälgimise ohtu, ning see tähendab, et isiku tuvastamine tehisintellektimääruse artikli 5 lõike 1 punkti h tähenduses peab olema sihipärane. Seda väljendit tuleks mõista nii, et reaajas toimuva biomeetrilise kaugtuvastamise võib käivitada ainult selliste konkreetsete isikute otsimiseks, kelle puhul õiguskaitseasutustel on põhjust arvata või kelle puhul on teatatud, et nad on tehisintellektimääruse artikli 5 lõike 1 punkti h alapunktis i loetletud kuritegude ohvrid või on seotud mõne tehisintellektimääruse artikli 5 lõike 1 punkti h alapunktis ii või artikli 5 lõike 1 punkti h alapunktis iii kirjeldatud olukorraga. Praktikast tähendab see reaajas kogutud andmete võrdlemist võrdlusandmebaasis sisalduvate andmetega. Mis puutub reaajas toimuva biomeetrilise kaugtuvastamise süsteemi kasutamisse tehisintellektimääruse artikli 5 lõike 1 punkti h alapunktis ii kirjeldatud olukordades ja kriminaaluurimise eesmärgil artikli 5 lõike 1 punkti h alapunktis iii määratletud tähenduses, siis ei pea õiguskaitseasutused enne süsteemi kasutamist tingimata teadma otsitavate isikute identiteeti. Kui neil on faktilisi andmeid ja teavet terrorirühmituse kavandatava terrorirünnaku kohta (teadmata, kes selle plaani ellu viib) konkreetsetel ajal ja kohas, võib biomeetrilise kaugtuvastamise süsteemi kasutada terrorirühmitusse kuuluva kurjategija tuvastamiseks, tingimusel et õiguskaitseasutused on loonud võrdlusandmebaasi, mis sisaldab terrorirühmitusse kuuluvate isikute biomeetrilisi andmeid. Kõigi kolme tehisintellektimääruse artikli 5 lõike 1 punkti h alapunktides i–iii kirjeldatud olukorra puhul võib isikusamasuse kinnitamine hõlmata ka asjaomase isiku asukoha kindlaksmääramist.

- (359) Teiseks tuleks enne süsteemi kasutamist hinnata süsteemi võimaliku kasutamise aluseks oleva olukorra laadi, eelkõige milline oleks füüsilistele isikutele, ühiskonnale ja õiguskaitse eesmärkidele tekkiva kahju raskusaste, tõenäosus ja ulatus, kui süsteemi ei kasutataks, võrreldes süsteemi kasutamise tagajärgedega asjaomaste isikute õigustele ja vabadustele, eelkõige nende tagajärgede raskusastme, tõenäosuse ja ulatusega. See peaks hõlmama ka selle hindamist, kas õiguskaitseasutused või nende nimel tegutsevad üksused saavad kasutada ka vähem sekkuvaid alternatiivseid lahendusi.

Näiteks on õiguskaitseasutustel keelatud kasutada tänavatel reaajas toimuva näotuvastuse süsteeme, lähtudes üldistest julgeoleku, kuritegevuse ennetamise ja ülerahvastatuse probleemidest, kuna see tähendaks kõigi isikute pidevat jälgimist ja järelevalvet ning see ei oleks ajaliselt piiratud, mistõttu ei vastaks see artikli 5 lõike 1 punktis h sätestatud keelust erandi tegemise kriteeriumidele.

- (360) **Raskusastme** kriteerium, mida siinkohal kasutatakse võimaliku kahju ja tagajärgede puhul, viitab sellele, et kõnealustesse põhiõigustesse võidakse sekkuda erineval määral,

mis on seotud proportsionaalsuse põhimõttega²¹². Mõned põhiõigustesse sekkumise viisid on raskemad kui teised.

- (361) **Ulatuse** kriteerium viitab eelkõige nende isikute arvule ja kategooriatele, keda sekkumine mõjutab (sealhulgas lapsed ja haavatavad või tõrjutud isikud).
- (362) Viimaks tähistab **tõenäosus** sündmuse toimumise tõenäosust.
- (363) Kahju raskusastme, ulatuse ja tõenäosuse ning tagajärgede hindamine peaks olema osa põhiõigustele avalduva mõju hindamisest, mida õiguskaitseasutus on kohustatud tegema (vt allpool). Seda hinnatakse iga juhtumi puhul eraldi.
- (364) Kolmandaks peaks biomeetrilise kaugtuvastamise reaalajas kasutamine olema geograafilise ulatuse, kestuse ja sihtrühma osas selgelt piiratud. Sellega tagatakse, et biomeetrilise kaugtuvastamise süsteemi kasutatakse ainult siis, kui see on hädavajalik.
- (365) **Geograafilise piirangu** puhul võib see hõlmata ühte või mitut geograafilist piirkonda, mis põhineb objektiivsetel ja mittediskrimineerivatel teguritel. Biomeetrilise tuvastamise puhul tähendab see, et geograafiline piirang vastab selgelt määratud piirile, mille puhul on olemas andmed sündmuse toimumise kohta. Selline piiritlemine ei tohiks (tavatingimustes) hõlmata tervet linna või riiki, vaid peaks olema sihipärasem.
- (366) Teine kaitsemeede on seotud meetme **isikulise kohaldamisalaga**, st asjaomaste isikute **kategooriate määratlemisega**. See välistaks isikute konkreetse suunitluse ja valimatu tuvastamise, ilma oleks mingeid täpsemaid märke juhtumi toimumisest.
- (367) Lõpetuseks vastab **ajaline piirang** ajavahemikule, mis on rangelt vajalik, kuid mida võib vajaduse korral kehtivate õigusnormide järgi pikendada. Reaalajas toimuva biomeetrilise kaugtuvastamise süsteemide kasutamine ei saa seega toimuda tähtajatult või ebamäärase ajavahemiku jooksul. Ajavahemiku kindlaksmääramisel tuleb võtta arvesse konkreetseid näitajaid, mis toovad kaasa biomeetrilise kaugtuvastamise süsteemide kasutamise.
- (368) Neljandaks peab reaalajas biomeetrilise kaugtuvastamise süsteemi juurutav õiguskaitseasutus olema enne süsteemi juurutamist teinud põhiõigustele avalduva mõju hindamise ja registreerinud süsteemi ELi andmebaasis (välja arvatud nõuetekohaselt põhjendatud juhtudel).

10.1.1. Põhiõigustele avalduva mõju hindamine

- (369) Tehisintellektimääruse artikli 5 lõike 2 kohaldamisel tehtud põhiõigustele avalduva mõju hindamine peab vastama tehisintellektimääruse artiklis 27 sätestatud tingimustele. Kõnealuses sättes on ette nähtud suure riskiga tehisintellektisüsteemide suhtes kohaldatavate põhiõigustele avalduva mõju hindamise nõuded.
- (370) Ajavahemikul, mil tehisintellektimääruse artikli 5 kohased keelud hakkavad kehtima (pärast 2. veebruari 2025), kuid suure riskiga tehisintellektisüsteeme käsitlevad sätted ei ole veel kohaldatavad (enne 2. augustit 2026), peaksid tehisintellektimääruse

²¹² Kohtuotsus, Euroopa Kohus, 2. oktoober 2018, Ministerio Fiscal, C-207/16, ECLI:EU:C:2018:788, punkt 55, kus kohus märgib, et juurdepääs „peab olema proportsioonis selle tegevusega kaasneva põhiõiguste riive raskusega“.

artiklis 27 sätestatud põhiõigustele avalduva mõju hindamise nõudeid rakendama reaalajas kasutatavate biomeetrilise kaugtuvastamise süsteemide juurutajad, kes vastavad ühe või mitme tehisintellektimääruse artikli 5 lõike 1 punktis h sätestatud erandi kohaldamise tingimustele. Järgnevad ajutised suunised käsitlevad ainult avalikult juurdepääsetavas ruumis reaalajas toimuva biomeetrilise kaugtuvastamise süsteemide kasutamist õiguskaitse eesmärgil enne seda, kui suure riskiga tehisintellektisüsteemide kohustusi hakatakse kohaldama ning komisjon võtab vastu põhiõigustele avalduva mõju hindamise malli ja annab täpsemaid suuniseid tehisintellektimääruse artikli 27 kohase kohustuse kohta.

- (371) Põhiõigustele avalduva mõju hindamine on uut tüüpi mõjuhindang, mille eesmärk on kindlaks teha, millist mõju võivad teatud suure riskiga tehisintellektisüsteemid, sealhulgas biomeetrilise kaugtuvastamise süsteemid, avaldada põhiõigustele. Põhiõigustele avalduva mõju hindamine on aruandlusvahend. Põhiõigustele avalduva mõju hindamine ei asenda olemasolevat andmekaitsealast mõjuhindangut, mida vastutavad töötajad (st isikuandmete töötlemise eest vastutavad isikud) peavad tegema õiguskaitsedirektiivi artikli 27, isikuandmete kaitse üldmääruse artikli 35 või ELi isikuandmete kaitse määruse artikli 39 alusel.

Näiteks tuleb teha andmekaitsealane mõjuhindang, kui biomeetrilisi andmeid töödeldakse uute tehnoloogiate abil, mis tõenäoliselt kujutavad endast suurt ohtu füüsiliste isikute õigustele ja vabadustele (näiteks videovalve, tehisintellektipõhine näotuvastus ja kehal kantavad kaamerad) avalikult juurdepääsetavas ruumis.

- (372) Kui andmekaitsealane mõjuhindang keskendub sellele, millist ohtu tekitab isikuandmete töötlemine üksikisikute õigustele ja vabadustele, siis põhiõigustele avalduva mõju hindamine hõlmab tehisintellektisüsteemide võimalikku mõju üksikisikute põhiõigustele üldisemalt. Seega on põhiõigustele avalduva mõju hindamine hõlmatud tegevuse ja hinnatud põhiõiguste mõistes laiem. Kui isikuandmeid töödeldakse tehisintellektisüsteemi abil (millega on tegemist biomeetrilise kaugtuvastamise süsteemide puhul), peaks põhiõigustele avalduva mõju hindamine täiendama andmekaitsealast mõjuhindangut, mille teeb juurutaja kui vastutav töötaja,²¹³ ilma et see hõlmaks juba andmekaitsealases mõjuhindangus käsitletud aspekte ja vältides kattuvust. Nendes suunistes esitatud põhiõigustele avalduva mõju hindamise analüüs piirdub biomeetrilise kaugtuvastamise lubatud kasutamisega reaalajas ja selle eesmärk on anda juurutajatele esialgseid juhiseid sellel üleminekuperioodil, kuni Euroopa tehisintellektiamet avaldab vastava malli²¹⁴.
- (373) Tehisintellektimääruse artikli 5 lõike 2 kohane kohustus teha põhiõigustele avalduva mõju hindamine on pandud biomeetrilise kaugtuvastamise süsteemi juurutajatele, mitte üksustele või asutustele või kellelegi teisele, kes tegutseb nende nimel. Kui teised osalejad tegutsevad juurutaja/õiguskaitseasutuse nimel, peavad nad andma

²¹³ Tehisintellektimääruse artikli 27 punkt 4.

²¹⁴ Seega ei hõlma analüüs üldiselt suure riskiga tehisintellektisüsteeme.

põhiõigustele avalduva mõju hindamise ettevalmistamiseks kogu asjakohase teabe, et tagada selle nõuetekohane toimumine.

- (374) Enne lubatud reaalarajalise biomeetrilise kaugtuvastamise süsteemi juurutamist tuleb teha põhiõigustele avalduva mõju hindamine.
- (375) Vastavalt tehisintellektimääruse artiklile 27 peaks põhiõigustele avalduva mõju hindamine sisaldama järgmist teavet:
- biomeetrilise kaugtuvastamise kasutamise kirjeldus ja juurutaja kasutamisprotsessid koos kavandatud kasutuseesmärgiga;

Selles tuleb ära näidata:

- juurutaja nimi;
- õiguskaitse eesmärk (eesmärgid), milleks reaalarajas biomeetrilise kaugtuvastamise süsteemi kasutatakse;
- võrdlusandmebaasi kirjeldus, millega biomeetrilist tuvastamist võrreldakse, sealhulgas kasutatavate biomeetriliste andmete allikad (näokujutised, hääleproovid jne);
- süsteemi aluseks oleva tehnoloogia kirjeldus, et selgitada selle toimimist (viidates pakkuja esitatud olemasolevale dokumentatsioonile ja selle nimetusele)²¹⁵;
- õiguslik alus, mille alusel reaalarajas toimuvat biomeetrilist kaugtuvastamist kasutatakse.

- kasutusaeg ja -sagedus;

Iga reaalarajas toimuva biomeetrilise kaugtuvastamise süsteemi juurutamine ühe lubatud erandi puhul peab enne selle kasutamist saama loa õigusasutuselt või muult sõltumatult asutuselt vastavalt tehisintellektimääruse artikli 5 lõikele 3. Seevastu põhiõigustele avalduva mõju hindamise puhul peavad juurutajad esitama üldised andmed kavandatud kasutusperioodi ja eeldatava sageduse kohta.

- isikute ja rühmade kategooriad, keda süsteem mõjutab;

Tehisintellektimääruse artikli 5 lõike 1 punktis h sätestatud erandi kohaldamisel tuleks põhiõigustele avalduva mõju hindamises eristada järgmist:

- sihtmärgiks olev isik, kes võib olla kuriteo ohver, kuriteo toimepanija või kahtlusalune,
- isikud, kelle biomeetrilised andmed on võrdlusandmebaasis olemas, ja
- isikute kategooriad, kes viibivad piirkonnas, kus biomeetrilise kaugtuvastamise süsteemi kasutatakse.

²¹⁵

Kui suure riskiga tehisintellektisüsteemi käsitlevad eeskirjad jõustuvad, saab selle tegemiseks viidata süsteemi registreerimisnumbrile ELi andmebaasis ja selles sisalduvale süsteemiga seotud olemasolevale teabele.

Reaalajas toimuva biomeetrilise kaugtuvastamise süsteemide kasutamine ei mõjuta mitte ainult sihtmärgiks oleva isiku põhiõigusi. See mõjutab ka teiste isikute õigusi, kelle biomeetrilisi andmeid kasutatakse võrdluseks, samuti möödakäijate ja juhuslikult otsingualal viibivate inimeste õigusi. Reaalajas toimuva biomeetrilise kaugtuvastamise süsteemiga hõlmatud otsinguala(de) geograafilise ulatuse kirjeldus mõjutab süsteemiga hõlmatud isikute arvu.

- konkreetsed ohud kahjustatud isikutele.

(376) Põhiõigused, mida võib mõjutada avalikult juurdepääsetavas ruumis reaalajas toimuva biomeetrilise kaugtuvastamise süsteemide kasutamine õiguskaitse eesmärgil, hõlmavad eelkõige järgmist:

- õigus era- ja perekonnaelu puutumatusele, sealhulgas inimeste mõistlik ootus anonüümsusele avalikus ruumis;
- õigus andmekaitsele, kuna biomeetrilise kaugtuvastamise süsteemid tuginevad biomeetriliste andmete ja muude isikuandmete (nt nimed, isikukoodid ja tundlikud andmed, nagu etniline päritolu) töötlemisele, et tuvastada konkreetseid isikuid;
- mõtte-, südametunnistuse- ja usuvabadust, sõnavabadust ning kogunemis- ja ühinemisvabadust avalikus ruumis, kus otsingud toimuvad ja millele biomeetrilise kaugtuvastamise süsteemide kasutamine võib avaldada pärssivat mõju, takistades üksikisikuid täielikult oma õigusi ja vabadusi kasutamast, sest kui üksikisikud teavad, et neid jälgitakse, võivad nad muuta oma käitumist või isegi takistada end teatud viisil käitumast;
- õigus tõhusale õiguskaitsevahendile ja õiglasele kohtumenetlusele;
- õigus mittediskrimineerimisele, kui süsteem sisaldab eelarvamusi (näiteks soolisi, etnilisi või rassilisi eelarvamusi) ja viib kahtlusaluse või kuriteo toimepanija valesti tuvastamiseni;
- õigus inimväärikusele, kuna isik võib tunda, et teda koheldakse ainult süsteemi objektina;
- süütuse presumptsioon ja kaitseõigus, kuna ühtegi üksikisikut kahjustavat otsust ei tohi teha üksnes reaalajas toimuva biomeetrilise kaugtuvastamise süsteemi väljundite põhjal;
- lapse õigused juhul, kui ohver, kadunud isik või kahtlusalune on alaealine;
- eakate õigused kadunud isiku puhul.

Selleks, et hinnata konkreetseid kahjuriske, mis tõenäoliselt mõjutavad tuvastatud mõjutatud isikut (isikuid) või isikute rühma(sid), tuleb põhiõigustele avalduva mõju hindamisel määrata kindlaks nende isikute põhiõigused ja hinnata nende põhiõigustele avalduvat mõju, sealhulgas mõju raskusastet ja ulatust, võttes arvesse potentsiaalselt mõjutatud isikuid.

See osa põhiõigustele avalduva mõju hindamisest peaks sisaldama ka hinnangut selle kohta, kas reaalajas toimuva biomeetrilise kaugtuvastamise süsteemi kasutamine on vajalik ja proportsionaalne, arvestades eesmäärke ja asjaolusid, mille puhul seda kavatsetakse kasutada, sealhulgas vähem sekkuvate alternatiivide olemasolu või puudumist. Põhiõigustele avalduva mõju hindamine peaks kirjeldama süsteemi toimivust ja täpsuse taset, tuginedes tehnilisele dokumentatsioonile ja võimaluse korral koolitusandmetele, mille põhjal tehnoloogiat testiti ja välja arendati, et vältida eelarvamusi ja diskrimineerimist.

Põhiõigustele avalduva mõju hindamine peaks samuti kindlaks määrama reaalajas toimuva biomeetrilise kaugtuvastamise süsteemi kasutamise mõju kõigi potentsiaalselt mõjutatud isikute, eelkõige kahtlusosaluse või kuriteo toimepanija, otsitava ohvri ja teiste isikute põhiõigustele, kes viibivad avalikult juurdepääsetavas ruumis, kus otsimine toimub. Kuivõrd süsteem töötleb nende isikute biomeetrilisi andmeid, mõjutab see nende õigust era- ja perekonnaelu puutumatusele ja andmekaitsele, mida hinnatakse andmetöötlustoimingute puhul andmekaitsealase mõjuhinnangu raames. Muude tegevuste puhul, mis on seotud reaalajas toimuva biomeetrilise kaugtuvastamise süsteemide kasutamisega ja mõjuga muudele põhiõigustele, täiendab põhiõigustele avalduva mõju hindamine andmekaitsealast mõjuhinnangut. Sõltuvalt juurutamise kontekstist võib see mõjutada nende isikute muid põhiõigusi, nagu õigus inimväärikusele, mõtte-, südametunnistuse- ja usuvabadus, kogunemis- või sõnavabadus, õigus tõhusale õiguskaitsevahendile ja õiglasele kohtulikule arutamisele, süütuse presumptsioon ja kaitseõigus ning lapse õigused.

Enne tehisintellektisüsteemi esmakordset kasutusele võtmist tuleks teha põhiõigustele avalduva mõju hindamine abstraktsel tasandil. Iga biomeetrilise kaugtuvastamise süsteemi kasutamise kohta esitatavas individuaalses taotluses, millega taotletakse õigusasutuse või muu sõltumatu haldusasutuse luba, tuleks täpsemalt kirjeldada kontekstist sõltuvaid konkreetseid kaalutlusi, mis määravad kasutamise mõju igal üksikjuhul, kui kasutatakse reaalajas toimuvat biomeetrilise kaugtuvastamise süsteemi (vt punkt 10.23.8.3 allpool).

- Inimjärelvalve meetmed

Vastavalt tehisintellektimääruse artikli 5 lõikele 3 ei tohi ühtegi üksikisikut kahjustavat otsust teha üksnes reaalajas toimuva biomeetrilise kaugtuvastamise süsteemi tulemuste põhjal. Sellest tulenevalt tuleks põhiõigustele avalduva mõju hindamises kirjeldada menetlusi, mida süsteemi toimimise ajal järgitakse, ja seda, kuidas väljundit otsustusprotsessis tõlgendatakse. Menetlustes tuleks anda juhiseid biomeetrilise kaugtuvastamise süsteemi juurutamiseks, selgitada inimese rolli väljundite kontrollimisel ja tõlgendamisel ning pakkuda väljaõpet süsteemi kasutamiseks. Inimjärelvalve eest vastutaval isikul peaks olema „piisav tehisintellektipädevus, ning et neid on koolitatud ja neil on volitused“,²¹⁶ et mõista, kuidas süsteem toimib ja millal see ei toimi piisavalt hästi või ei ole töökorras.

Asjakohased on ka muud inimjärelvalve ja seirega seotud kaalutlused vastavalt tehisintellektimääruse artiklitele 14 ja 26 ja neid tuleks kirjeldada.

- Riskimaandusmeetmed

Lisaks inimjärelvalve meetmete rakendamisele (sealhulgas diskrimineerivate meetmete vältimiseks) peaks juurutaja selgitama õiguskaitsemeetmeid juhuks, kui risk realiseerub, sealhulgas juhtimismenetlusi ja kaebuste esitamise mehhanisme (näiteks valesti tuvastamise korral).

10.1.2. Lubatud biomeetrilise kaugtuvastamise süsteemide registreerimine

- (377) Tehisintellektimääruse artikli 5 lõikes 2 on avalikult juurdepääsetavas ruumis õiguskaitse eesmärgil kasutatava reaalsajas toimuva biomeetrilise kaugtuvastamise süsteemi juurutajale seatud kohustus registreerida süsteem tehisintellektimääruse artiklis 49 sätestatud ELi andmebaasis. Nõuetekohaselt põhjendatud hädaolukorras (näiteks otsese ohu korral) võib siiski alustada juurutamist ka enne registreerimist, tingimusel et õiguskaitseasutus registreerib süsteemi põhjendamatu viivitusega. „Põhjendamatu viivitusega“ peaks tähendama „nii kiiresti kui võimalik“, arvestades hädaolukorra asjaolusid, mis takistasid süsteemi registreerimist enne selle kasutamist. Seda, kas registreerimine vastab sellele kriteeriumile, tuleb hinnata iga juhtumi puhul eraldi. Seda ei saa määratleda eelnevalt täpse ajalise piiranguga. Viivitus ei tohiks olla tingitud tahtlikust tegevusest. Vastavalt tehisintellektimääruse artikli 49 lõikele 4 registreeritakse õiguskaitse eesmärgil kasutatavad biomeetrilise kaugtuvastamise süsteemid andmebaasi turvalises mitteavalikus osas, kus on piiratud teave ja piiratud juurdepääs sellele teabele.

Näiteks võib mõistlikuks viivituseks pidada õiguskaitseasutuste taotlust registreerida biomeetrilise kaugtuvastamise süsteem 24 tunni jooksul pärast kasutamist, kui süsteemi kasutati olukorras, kus oli otsene oht elule, näiteks kui tegemist oli reaalsajas tulistamisega.

10.2. Eelneva loa vajadus

- (378) Tehisintellektimääruse artikli 5 lõike 3 kohaselt on reaalsajas toimuva biomeetrilise kaugtuvastamise süsteemi igaks kasutamiseks vaja **eelnevat luba** ja keelatud teha kahjulikke õiguslikke tagajärgi põhjustavaid otsuseid **üksnes sellise süsteemi tulemuste põhjal**.

Tehisintellektimääruse artikli 5 lõikes 3 on sätestatud:

„Lõike 1 esimese lõigu punkti h ja lõike 2 kohaldamisel on reaalsajas toimuva biomeetrilise kaugtuvastamise süsteemi igaks kasutamiseks avalikult juurdepääsetavas ruumis vaja eelnevat luba, mille annab selle liikmesriigi, kus kasutamine hakkab toimuma, õigusasutus või sõltumatu haldusasutus, kelle otsus on siduv, ja mis antakse põhjendatud taotluse põhjal kooskõlas lõikes 5 osutatud üksikasjalike siseriiklike õigusnormidega. Põhjendatud kiireloomulistel juhtudel

võib siiski hakata sellist süsteemi kasutama ilma loata, tingimusel et sellist luba taotletakse põhjendamatu viivitusega ja hiljemalt 24 tunni jooksul. Kui selline luba lükatakse tagasi, lõpetatakse kasutamine viivitamata ning kõik andmed ning selle kasutamise tulemused ja väljundid jäetakse viivitamata kõrvale ja kustutatakse.

Pädev õigusasutus või sõltumatu haldusasutus, kelle otsus on siduv, annab loa üksnes juhul, kui on talle esitatud objektiivsete tõendite või selgete asjaolude põhjal veendunud, et kõnealuse reaalajas toimuva biomeetrilise kaugtuvastamise süsteemi kasutamine on vajalik ja proportsionaalne mõne lõike 1 esimese lõigu punktis h täpsustatud ja taotluses nimetatud eesmärgi saavutamiseks, ning et eelkõige piirdub süsteemi kasutamine sellega, mis on rangelt vajalik seoses ajavahemiku ning geograafilise ja isikulise kohaldamisalaga. Kõnealune asutus võtab taotluse kohta otsuse tegemisel arvesse lõikes 2 osutatud elemente. Ühtki isiku suhtes kahjulikke õiguslikke tagajärgi põhjustavat otsust ei tohi teha üksnes reaalajas toimuva biomeetrilise kaugtuvastamise süsteemi tulemuste põhjal.“

10.2.1. Eesmärk

- (379) Selle eesmärk, et reaalajas toimuva biomeetrilise kaugtuvastamise süsteemi mis tahes kasutamiseks avalikult juurdepääsetavas ruumis õiguskaitse eesmärgil nõutakse eelnevat luba, on vajadus hinnata ja otsustada, kas sellise süsteemi kavandatav kasutamine sellistel eesmärkidel:
- on vajalik ja proportsionaalne, et saavutada mõni artikli 5 lõike 1 punkti h alapunktides i–iii loetletud eesmärkidest, st konkreetsete ohvrite sihipärane otsimine, konkreetsete ohtude ennetamine või õigusrikkujate asukoha kindlaksmääramine või tuvastamine, ning
 - piirdub ajavahemiku ning geograafilise ja isikulise kohaldamisala mõistes ainult rangelt vajalikuga.
- (380) Nende nõuete tulemusel tuleks enne mis tahes reaalajas toimuva biomeetrilise kaugtuvastamise süsteemi juurutamist avalikult juurdepääsetavas ruumis õiguskaitse eesmärgil hinnata selle vajalikkust ja proportsionaalsust. Esiteks peaks kasutaja koostama põhiõigustele avalduva mõju hindamise tegemisel hinnangu, nagu on nõutud tehisintellektimääruse artikli 5 lõikes 2. Teiseks peab kohtu- või sõltumatu haldusasutus hindama tehisintellektimääruse artikli 5 lõike 3 kohaselt ka sellise süsteemi kasutamise vajalikkust ja proportsionaalsust sellise kasutamise õiguslikuks aluseks oleva liikmesriigi õiguse piires, võttes arvesse hartat ja muud liidu õigust. Sellest tulenevalt võib selliseid süsteeme kasutada ainult 1) pärast põhiõigustele avalduva mõju hindamist ja 2) kui pädev riiklik asutus on andnud selleks loa.
- (381) Tehisintellektimääruse artikli 5 lõiget 3 tuleb lugeda ja mõista koos tehisintellektimääruse artikli 5 lõikega 5: reaalajas toimuva biomeetrilise kaugtuvastamise süsteemi kasutamise lubamiseks peab olema asjaomases liikmesriigis vastu võetud õigusakt, mis lubab sellist kasutamist²¹⁷. Teatavates liikmesriikides on

²¹⁷

Vt ka tehisintellektimääruse artikli 5 lõige 2: „[...] kooskõlas selle kasutamist lubava siseriikliku õigusega [...]“.

juba kehtestatud eelneva loa andmise süsteem, mis võimaldab biomeetriliste süsteemide kasutamist muude liidu või riigisiseste õigusaktide, näiteks andmekaitseaduse alusel.

10.2.2. Peamine põhimõte Eelnev luba õigusasutuselt või sõltumatult haldusasutuselt

- (382) Reaalajas toimuva biomeetrilise kaugtuvastamise süsteemide kasutamine, et saavutada üks tehisintellektimääruse artikli 5 lõike 1 punkti h alapunktides i–iii loetletud eesmärkidest ning mis on ette nähtud asjaomase liikmesriigi õigusaktides, peab **enne selle kasutamist** saada loa õigusasutuselt või sõltumatult haldusasutuselt. See on peamine põhimõte.
- (383) Kiireloomuliste juhtumite puhul võidakse siiski teha erand. See peab olema **põhjendatud**²¹⁸. Kiireloomulisust kirjeldatakse „kus vajadus asjaomaste süsteemide kasutamise järele on selline, et enne tehisintellektisüsteemi kasutamise **algust ei ole reaalselt ega objektiivselt võimalik luba saada**²¹⁹. Sellistes kiireloomulistes olukordades peaks tehisintellektisüsteemi kasutamine piirduma hädavajaliku miinimumiga ning selle suhtes peaksid kehtima **asjakohased kaitsemeetmed ja tingimused**, mis on kindlaks määratud riigisiseses õiguses ja mida õiguskaitseasutus iga individuaalse kiireloomulise kasutusjuhtumi korral täpsustab“.

10.2.2.1. Eelnev ja põhjendatud taotlus vastavalt riigisisestele menetlusnormidele

a) Kelle taotlus?

- (384) Kuigi seda ei ole täpsustatud, võib eeldada, et taotluse algatab tavaliselt juurutaja, st seda teeb **pädev (õiguskaitse)asutus**. Vastavalt tehisintellektimääruse artikli 3 punkti 45 alapunktis b esitatud õiguskaitseasutuse määratlusele loetakse õiguskaitseasutuseks mis tahes muud asutust või üksust, „kellele liikmesriigi õiguse kohaselt on antud ülesanne teostada avalikku võimu kuritegude tõkestamise, uurimise, avastamise või nende eest vastutusele võtmise ja kriminaalkaristuste täitmisele pööramise, sealhulgas avalikku julgeolekut ähvardavate ohtude eest kaitsmise ja nende ennetamise eesmärgil“ ning selline asutus võib olla ka pädev asutus, kes vastutab eelneva loa taotluse esitamise eest.
- (385) Reaalajas toimuva biomeetrilise kaugtuvastamise süsteemi kasutamine tegevuseks, mis ei kuulu tehisintellektimääruse kohaldamisalasse, ei vaja tehisintellektimääruse artikli 5 lõike 3 kohast luba. Kui sellist süsteemi kasutatakse hiljem õiguskaitse eesmärkidel, kuulub selline kasutamine tehisintellektimääruse kohaldamisalasse ja selleks on vaja luba, kui on täidetud tehisintellektimääruse artikli 5 lõike 1 punkti h tingimused.

b) Millise kasutusviisi taotlus?

- (386) Reaalajas toimuva biomeetrilise kaugtuvastamise kasutamiseks avalikult juurdepääsetavas ruumis **õiguskaitse eesmärgil** on vaja eelnevat luba, isegi kui

²¹⁸ See tähendab, et õiguskaitseasutus peaks sellistel juhtudel kõnealust luba taotlema, põhjendades, miks ta ei saanud seda varem, põhjendamatu viivitusega ja hiljemalt 24 tunni jooksul taotleda (tehisintellektimääruse põhjendus 35).

²¹⁹ Tehisintellektimääruse põhjendus 35.

süsteeme käitavad õiguskaitseasutuse nimel muud pooled, näiteks spordiklubides või ostukeskustes.

Näiteks:

- organisatsioon, kellele on usaldatud ressursid kadunud laste otsimiseks, otsustab kasutada reaajas toimuva biomeetrilise kaugtuvastamise süsteemi. Tal ei ole volitusi avaliku võimu teostamiseks või kuritegude tõkestamiseks või avalikku julgeolekut ähvardavate ohtude ennetamisega seotud ülesannete täitmiseks. Selline kasutamine ei kuulu tehisintellektimääruse artikli 5 lõike 1 punktis h sätestatud keelu alla, kuna see ei ole õiguskaitse eesmärgil. See süsteem liigitatakse siiski suure riskiga süsteemiks (III lisa punkti 1 alapunkt a) ja vastavalt isikuandmete kaitse üldmääruse artiklile 36 võib olla vaja konsulteerida eelnevalt andmekaitseasutusega. Sõltuvalt kohaldatavast riigisisestest õigusest ja sellest, kas kehtib mõni isikuandmete kaitse üldmääruse artikli 9 lõike 1 eranditest, võib sellise töötlemise jaoks olla vajalik ka eelnev luba. Seevastu kui õiguskaitseasutused paluksid samal organisatsioonil tegutseda nende nimel kadunud laste otsimiseks õiguskaitse kontekstis ning pädevate õiguskaitseasutuste järelevalve all ja juhiste alusel, oleks tehisintellektimääruse artikli 5 lõike 3 kohaselt vaja eelnevat luba;
- eraorganisatsioon, kellele on usaldatud vahendite eraldamine selliste inimeste abistamiseks, keda ähvardab oht langeda loodusõnnetuse ohvriks,²²⁰ otsustab kasutada selleks reaajas toimiva biomeetrilise kaugtuvastamise süsteemi. Selline kasutamine ei kuulu tehisintellektimääruse artikli 5 lõike 1 punktis h sätestatud keelu alla, kuna see ei ole õiguskaitse eesmärgil. See süsteem liigitatakse siiski suure riskiga süsteemiks (III lisa punkti 1 alapunkt a) ja vastavalt isikuandmete kaitse üldmääruse artiklile 36 võib olla vaja konsulteerida eelnevalt andmekaitseasutusega. Sõltuvalt kohaldatavast riigisisestest õigusest ja sellest, kas kehtib mõni isikuandmete kaitse üldmääruse artikli 9 lõike 1 eranditest, võib sellise töötlemise jaoks olla vajalik ka eelnev luba.

c) Millal? „Iga kasutamine“

- (387) Tehisintellektimääruse artikli 5 lõike 3 järgi on „igaks kasutamiseks“ vaja eelnevat luba. See tähendab, et sellise loa saamise otsustavaks hetkeks ei ole mitte reaajas toimiva biomeetrilise kaugtuvastamise süsteemide paigaldamisele eelnev hetk, vaid iga konkreetne kasutuskord.

Näiteks:

- politsei paigaldab biomeetrilised valvekaamerad linna peamisse raudteejaama (selleks ei ole vaja tehisintellektimääruse kohast luba, kuid biomeetriline süsteem peab vastama suure riskiga süsteemide nõuetele, enne esimest kasutamist tuleb teha põhiõigustele avalduva mõju hindamine ja enne iga üksikut süsteemi kasutamist on vaja kohtu või sõltumatu haldusasutuse luba).

²²⁰

Looduskatastroofide hulka kuuluvad näiteks jõe üleujutus või looduslik tulekahju.

Politseil on konkreetseid andmeid, et terrorist saabub rongiga linna (reaalajas tuvastamiseks on vaja eelnevat luba).

d) Motiveeritud taotlus

- (388) Tehisintellektimääruse artikli 5 lõikes 3 on nõutud, et iga reaalajas toimuva biomeetrilise kaugtuvastamise kasutamise taotlus oleks põhjendatud, s.o et selle jaoks oleks olemas alus ja ajend.
- (389) Teatavad liikmesriigid lubavad selliseid taotlusi esitada internetis²²¹. Kooskõlas tehisintellektimääruse artikli 5 lõikega 5 tuleks riigisisestes õigusaktides sätestada nõuded taotluse täpse sisu kohta, võttes samas täielikult arvesse eespool kirjeldatud nõudeid, sealhulgas piisavad tõendid, et määrata kindlaks reaalajas toimuva biomeetrilise kaugtuvastamise kasutamise range vajadus ja proportsionaalsus ning muud asjakohased aspektid, mis näitavad sellise kasutamise lubamise erandlikkust.

10.2.2.2. Õigusasutuse või sõltumatu haldusasutuse luba

- (390) Loa võib anda ainult õigus- või sõltumatu haldusasutus, kelle otsus on siduv.

a) Sõltumatu asutus

- (391) Euroopa Liidu Kohus on tõlgendanud mõistet „sõltumatus“ erinevates kontekstides. Näiteks kohtuasjas HK vs. Prokuratuur selgitas Euroopa Liidu Kohus, et sõltumatus tähendab, et asutus säilitab „neutraalse positsiooni“²²². Euroopa Liidu Kohus täpsustas, et varasemates uurimistes osalenud asutusel, kõnealusel juhul prokuratuuril, ei ole sellist sõltumatust. Sarnased kaalutlused võivad kehtida ka seoses tehisintellektimääruse artikli 5 lõikes 3 nõutud sõltumatusega, mis tähendab, et luba andev asutus peab olema sõltumatu asutusest, kes kasutab biomeetrilise kaugtuvastamise süsteemi. See ei kehtiks mitte ainult politsei, vaid ka uurimiskohtunike või prokuröride puhul, kes teevad järelevalvet politsei töö ning biomeetrilise kaugtuvastamise kasutamise üle, milleks luba taotletakse.
- (392) Kohtuasjas komisjon vs. Poola, mis käsitles küsimust, millal saab asutust pidada raudteeohutuse kontekstis sõltumatuks, leidis Euroopa Liidu Kohus, et „avalik-õigusliku organi puhul tähendab sõltumatus harilikult staatust, mis tagab asjaomasele organile võimaluse tegutseda täiesti sõltumatult nendest organitest, kelle suhtes nende sõltumatus peab olema tagatud, sõltumata mis tahes juhenditest ning surveta“²²³. Sarnased kaalutlused võivad olla asjakohased ka tehisintellektimääruse artikli 5 lõike 3 kontekstis.
- (393) Demokraatliku ühiskonna õigusasutused on üldjuhul samuti sõltumatud asutused. Kohtusüsteemil on oluline roll siis, kui see on sõltumatu täitevvõimust ja seadusandjast, jälgides ja kontrollides õigusaktide ning põhiõiguste ja -vabaduste kohaldamist autonoomselt ja sõltumatult. Kohtute sõltumatus on üks õigusriigi põhimõtte olulisi

²²¹ Vt näiteks Prantsusmaa andmekaitseasutusele (CNIL) esitatud loataotlused.

²²² Kohtuotsus, Euroopa Kohus, 2. märts 2021, Prokuratuur, C-746/18, ECLI:EU:C:2021:152, punkt 54.

²²³ Kohtuotsus, Euroopa Kohus, 13. juuni 2018, komisjon vs. Poola, C-530/16, ECLI:EU:C:2018:430, punkt 67.

tahke, mis on tagatud harta artikliga 47 ning inimõiguste ja põhivabaduste kaitse konventsiooni artikli 6 lõikega 1²²⁴.

b) Kasutamise asukoha ametiasutus

- (394) Luba peab olema adresseeritud riigisisese õiguse kohaselt pädevale ametiasutusele²²⁵.

c) Luba ainult juhul, kui see on ühe erandites sätestatud eesmärgi saavutamiseks „vajalik ja proportsionaalne“

- (395) Kui antakse mis tahes luba avalikult juurdepääsetavas ruumis reaalajas toimuva biomeetrilise kaugtuvastamise süsteemide kasutamiseks õiguskaitse eesmärgil, tuleb hinnata, kas tehisintellektimääruse artikli 5 lõike 3 nõuded on täidetud.

Väga sekkuv

- (396) Andmekaitse kontekstis on Euroopa andmekaitseinspektor (EDPS) ja Euroopa Andmekaitsekohtu (EDPB) oma suunistes 5/2022 käsitlenud biomeetriliste andmete, eelkõige näotuvastustehnoloogia kasutamist kui mitut põhiõigust ja -vabadust mõjutava tegevusena. Seda seisukohta jagavad ka Euroopa Liidu Põhiõiguste Amet ja Euroopa Nõukogu²²⁶. Nii Euroopa Liidu Kohus²²⁷ kui ka Euroopa Inimõiguste Kohus²²⁸ on kinnitanud biomeetriliste andmete töötlemise tundlikkus laadi.

- (397) Igasugusel sekkumisel **põhiõigustesse ja -vabadustesse peab alati arvestama nende õiguste ja vabaduste olemust**. See tuleneb harta artikli 52 lõikest 1.

- (398) Põhiõiguste ja -vabaduste „olemuse“ mõiste on välja töötatud Euroopa Liidu Kohtu praktikas ning sellel on liidu õiguskorras iseseisev tähendus. Kui põhiõiguse või -vabaduse olemust ei austata, tähendab see, et meede riivab õigust või vabadust põhjendamatult, nii et mis tahes sekkumise jaoks ei tohi anda eelnevat luba.

Ainult „kui see on vajalik ja proportsionaalne“

- (399) Igasugune sekkumine põhiõigustesse ja -vabadustesse nõuab õigusakti, mis peaks põhimõtteliselt järgima harta artikli 52 kohast vajalikkuse ja proportsionaalsuse põhimõtet (vt allpool tehisintellektimääruse artikli 5 lõike 5 all). Tehisintellektimääruse artikli 5 lõikes 3 on nõutud, et riigisisestes õigusaktides, milles lubatakse avalikult juurdepääsetavas ruumis reaalajas toimuva biomeetrilise kaugtuvastamise süsteemide kasutamine õiguskaitse eesmärgil, peab olema sätestatud, et (ametiasutus) „annab loa üksnes juhul, kui [ta] on talle esitatud objektiivsete tõendite või selgete asjaolude põhjal veendunud, et [...] kasutamine on“ tehisintellektimääruse artikli 5 lõike 1 punktis h nimetatud eesmärgi saavutamiseks „vajalik ja proportsionaalne“. Riiklikud

²²⁴ Vt R. Manko, *Judicial independence in the case law of the European Court of Human Rights*, ülevaade, Euroopa Parlamendi uuringuteenistus, 2022, lk 12; X, *ECJ case law on judicial independence. A Chronological overview*, ülevaade, Euroopa Parlamendi uuringuteenistus, 2023, lk 12.

²²⁵ Vt kohtuotsus, Euroopa Kohus, 6. oktoober 2015, Schrems, C-362/14, <https://eur-lex.europa.eu/legal-content/ET/TXT/PDF/?uri=CELEX:62014CJ0362>, ECLI:EU:C:2015:650, punkt 44.

²²⁶ Isikuandmete automatiseeritud töötlemisel isiku kaitse konventsiooni (Euroopa Nõukogu lepingute sari nr 108) nõuandekomitee, *Guidelines on Facial Recognition*, 2021.

²²⁷ Kohtuotsus, Euroopa Kohus, 26. jaanuar 2023, Ministerstvo na vatrešnite raboti, C-205/21, ECLI:EU:C:2023:49, punktid 60–76 ja 116–134.

²²⁸ Kohtuotsus, Euroopa Inimõiguste Kohus, 4. juuli 2023, Glukhin vs. Venemaa, taotlus nr. 11519/20, ECLI:CE:ECHR:2023:0704JUD001151920, punktid 88 ja 90.

ametiasutused peavad kontrollima, kas biomeetriline tuvastamine on tingimata vajalik²²⁹. See hindamine peaks põhinema põhiõigustele avalduva mõju hindamisel, mis peaks juba enne loa taotlemist sisaldama iga konkreetsete asjaoludega seotud kasutamise puhul üldist hinnangut vajalikkuse ja proportsionaalsuse kohta.

10.2.2.3. Erand eelneva loa nõudest: taotlus 24 tunni jooksul ja selle tagasilükkamise tagajärjed

- (400) Kiireloomulistel juhtudel võib kasutaja esitada loataotluse 24 tunni jooksul alates reaalajas toimuva biomeetrilise kaugtuvastamise süsteemi kasutamise hetkest. Praktikaks on see tavaliselt hetk, mil biomeetrilise suutlikkusega kaamerad on sisse lülitatud ja juurutatud ning süsteemiga tehakse esimene biomeetriline võrdlus. Ametiasutusele tuleks teha kättesaadavaks töötlemistoimingute logi, et tõendada taotluse õigeaegsust²³⁰.
- (401) Sellisel juhul tuleks taotluses põhjendada, miks taotlust ei esitatud enne süsteemi kasutamise alustamist.

10.2.2.4. Kohene lõpetamine, kui loataotlus lükatakse tagasi, ja andmete kustutamine

- (402) Tehisintellektimääruse artikli 5 lõikes 3 on lisaks sätestatud, et kui kiireloomuline loataotlus lükatakse tagasi, tuleb reaalajas toimuva biomeetrilise kaugtuvastamise süsteemi kasutamine viivitamata lõpetada. Sellisel juhul tuleb kõik andmed, sealhulgas selle kasutamise tulemused ja väljundid, viivitamata kõrvale jätta ja kustutada²³¹. Tehisintellektimääruse artikli 5 lõige 3 on selles osas väga selge ja selles ei ole erandeid ette nähtud. Juurutajal on:
- a) võrdlusandmebaas, mis sisaldab biomeetrilisi andmeid (nt näokujutised, häälesalvestuse jupid jne) ja vajaduse korral nendega seotud isikuandmeid, millega
 - b) võrreldakse avalikult juurdepääsetavas ruumis viibivate isikute biomeetrilisi andmeid, et neid isikuid tuvastada ja teistest eristada;
 - c) see võrdlus viib võrdlustulemuseni.
- (403) Kogutud ja töödeldud andmete kõrvale jätmise ja kustutamise nõue tähendab ka seda, et kui loata biomeetrilise tuvastamise jaoks kasutatud võrdlusandmebaas(id) loodi spetsiaalselt vaidlustatud otsingu jaoks, tuleb see (need) eemaldada ja kustutada. Andmebaasi võib säilitada üksnes juhul, kui õiguskaitseasutused on loonud andmebaasi, mida kasutatakse tuvastamiseks *seaduslikul viisil* ja õigustatud eesmärgil, mis *ei ole* reaalajas toimuva biomeetrilise kaugtuvastamise lubamatu kasutamine, ja kavatsevad seda andmebaasi säilitada.

²²⁹ Vt ka andmete kogumise kohta: kohtuotsus, Euroopa Kohus, 28. november 2024, Ministerstvo na vatreshnite raboti, C-80/23, ECLI:EU:C:2024:991.

²³⁰ Automaatselt genereeritud andmelogisid tuleb suure riskiga tehisintellektisüsteemide puhul säilitada vähemalt kuus kuud ning need peavad III lisa punkti 1 alapunktis a nimetatud suure riskiga süsteemide puhul sisaldama iga kasutuse algus- ja lõpukuupäeva ja -kellaega. Vt tehisintellektimääruse artikli 12 lõike 3 punkt a ja artikkel 19.

²³¹ Järelevalveasutustel peaks olema ka volitused selle fakti järelkontrolliks ja kontrolliks. Vt tehisintellektimääruse artikli 5 lõige 5.

- (404) Lisaks biomeetrilisi andmeid sisaldava (ebaseadusliku) andmebaasi kustutamisele tuleb kustutada ka kõik kogutud kujutised ja muud isikuandmed, sealhulgas metaandmed, tehnilised töötlemisandmed, sealhulgas mallid ja muud isikuandmed, ning muud reaalses toimuva biomeetrilise kaugtuvastamise süsteemi ebaseadusliku kasutamise käigus saadud võrdlus- ja väljundandmed.
- (405) Kui õiguskaitseasutus vaidlustab taotluse tagasilükkamise, võib andmeid säilitada usaldushaldur, kuni taotluse kohta on tehtud lõplik otsus. Selle aja jooksul ei tohiks neid andmeid üldiselt õiguskaitseasutuse käsutusse anda³¹⁰.

10.2.2.5. Otsuseid ei tehta ainult reaalses toimuva biomeetrilise kaugtuvastamise süsteemi väljundi põhjal

- (406) Tehisintellektimääruse artikli 5 lõike 3 kohaselt ei tohiks juhul, kui reaalses toimuva biomeetrilise kaugtuvastamise süsteemi juurutaja saab vastava loa, teha üksnes selle süsteemi tulemuste põhjal ühtki isiku suhtes kahjulikke õiguslikke tagajärgi põhjustavat otsust.

Näiteks:

– isik arreteeritakse ja vangistatakse raske kuriteo eest üksnes näotuvastussüsteemi abil tuvastamise alusel, ilma et seda oleks täpsemalt kontrollitud. See lisandub inimjärelvalvele, mis on ette nähtud tehisintellektimääruse artiklis 14. Kontrollimine võib olla seotud näiteks sellega, kas konkreetne isik on käinud mõnes teises kohas või kas on muid põhjusi, miks ta ei saaks olla otsitav isik.

Tehisintellektimääruse artikli 14 nõuded inimjärelvalve kohta

- (407) Reaalses toimuva biomeetrilise kaugtuvastamise kasutamine, mis on lubatud, sest sellel on üks artikli 5 lõike 1 punktis h loetletud eesmärkidest, ja mis vastab tehisintellektimääruse artikli 5 lõigetele 2–6, kuulub siiski suure riskiga süsteemide eeskirjade kohaldamisalasse. Tehisintellektimääruse artikli 14 kohaselt projekteeritakse ja arendatakse suure riskiga tehisintellektisüsteeme selliselt, et füüsilised isikud saaksid teha süsteemide kasutamise ajal nende üle reaalsel järelvalvet, muu hulgas asjakohaste inimene-masin kasutajaliidestite abil. Tehisintellektimääruse artikli 14 lõike 5 kohaselt ei tee ega otsusta juurutaja süsteemist saadud tuvastamise põhjal midagi, „kui seda tuvastamist ei ole eraldi kontrollinud ja kinnitanud vähemalt kaks füüsilist isikut, kellel on vajalik pädevus, väljaõpe ja volitused“ või „kui liidu või riigi õiguse kohaselt peetakse selle nõude kohaldamist ebaproportsionaalseks“. Tehisintellektimääruse artiklis 4 on tehisintellektisüsteemide pakkujatele ja kasutajatele nähtud ette tehisintellekti alaste oskuste arendamise meetmed, et tagada „töötajate ja kõigi teiste nende nimel tehisintellektisüsteemide käitamise ja kasutamisega tegelevate isikute piisav tehisintellektipädevus“ ning arvestada isikuid, kelle puhul neid süsteeme kasutatakse.
- (408) Nagu Euroopa Andmekaitsekoostöögrupp on andmekaitse kontekstis märkinud, on inimjärelvalve tõhusaks toimimiseks väga oluline, et „isik mõistaks (konkreetsel juhul näotuvastus)süsteemi ja selle piiranguid ning tõlgendaks selle tulemusi õigesti. Samuti

on vaja luua tööpaik ja -korraldus, mis tasakaalustaksid automatiseerimise eelistamist ning väldiksid tulemuste kriitikata aktsepteerimist näiteks ajasurve, koormavate menetluste, võimaliku kahjuliku karjäärimõju jms tõttu²³². Sarnased kaalutlused võivad olla asjakohased ka tehisintellektimääruse kontekstis.

10.3. Ametivõimude teavitamine iga kord, kui reaajas toimuva biomeetrilise kaugtuvastamise süsteemi kasutatakse avalikult juurdepääsetavas ruumis õiguskaitse eesmärgil

Tehisintellektimääruse artikli 5 lõikes 4 on sätestatud:

„Ilma et see piiraks lõike 3 kohaldamist, teavitatakse asjaomast turujärelevalveasutust ja riiklikku andmekaitseasutust igast reaajas toimuva biomeetrilise kaugtuvastamise süsteemi kasutamisest avalikult juurdepääsetavas ruumis õiguskaitse eesmärgil kooskõlas lõikes 5 osutatud siseriiklike õigusnormidega. Teates esitatakse vähemalt lõikes 6 täpsustatud teave ning teade ei sisalda tundlikke operatiivandmeid.“

- (409) Iga kord, kui kasutatakse biomeetrilise kaugtuvastamise süsteemi, mille eesmärk on üks tehisintellektimääruse artikli 5 lõike 1 punkti h alapunktides i–iii loetletud eesmärkidest, tuleb teavitada asjaomast turujärelevalveasutust ja riiklikku andmekaitseasutust. Teatada tuleb pärast iga kasutuskorda, et oleks võimalik anda teavet lubade arvu ja nende tulemuste kohta. Selline teade ei pea sisaldama tundlikke operatiivandmeid. „Tundlikud operatiivandmed“ on tehisintellektimääruse artikli 3 punkti 38 kohaselt operatiivandmed, mis on seotud õiguskaitsealase tegevusega (kuritegude tõkestamine, avastamine, uurimine või nende eest vastutusele võtmine) ning mille avalikustamine võib ohustada kriminaalmenetluse terviklikkust.
- (410) Aruandlusnõude üksikasjad on esitatud punktis 10.6 allpool.

10.4. Vajadus riigisiseste õigusaktide järele, mis jäävad tehisintellektimääruse erandite piiridesse

10.4.1. Põhimõte: vaja on riigisisest õigusakti, mis annab õigusliku aluse kõigi või mõne(de) erandi(te) jaoks loa andmiseks

- (411) Riigisisest õigusaktid on vajalikud selleks, et rakendada reaajas toimuva biomeetrilise kaugtuvastamise süsteemi kasutamist avalikult juurdepääsetavas ruumis õiguskaitse jaoks. Samal ajal on tehisintellektimääruse artikli 5 lõikes 5 sätestatud, et liikmesriigid võivad vabalt otsustada, kas nad võtavad selliseid õigusakte vastu. Kui võetakse vastu riigisisene õigusakt, millega lubatakse reaajas toimuva biomeetrilise kaugtuvastamise kasutamist, on tehisintellektimääruses täpsustatud, milliseid sisulisi elemente sellised õigusaktid peavad sisaldama, et need vastaksid kõnealuses määruses sätestatud nõuetele.

Tehisintellektimääruse artikli 5 lõige 5

²³² Euroopa Andmekaitseamet, „Suunised 05/2022 näotuvastustehnoloogia kasutamise kohta õiguskaitse valdkonnas“, versioon 2.0, 26. aprill 2023, lk 22.

Liikmesriik võib otsustada näha ette võimaluse täielikult või osaliselt lubada reaalajas toimuva biomeetrilise kaugtuvastamise süsteemi kasutamist avalikult juurdepääsetavas ruumis õiguskaitse jaoks lõike 1 esimese lõigu punktis h ning lõigetes 2 ja 3 loetletud piirides ja tingimustel. Asjaomased liikmesriigid kehtestavad oma õigusaktides lõikes 3 osutatud lubade taotlemise, andmise ja kasutamise ning nende lubadega seotud järelevalve ja aruandluse jaoks vajalikud üksikasjalikud õigusnormid. Kõnealustes õigusnormides tuleb täpsustada, milliste lõike 1 esimese lõigu punktis h loetletud eesmärkide, sealhulgas milliste punkti h alapunktis iii osutatud kuritegude puhul võib anda pädevatele asutustele loa kasutada neid süsteeme õiguskaitse jaoks. Liikmesriigid teatavad nendest õigusnormidest komisjonile hiljemalt 30 päeva jooksul pärast nende vastuvõtmist. Liikmesriigid võivad kooskõlas liidu õigusega kehtestada biomeetrilise kaugtuvastamise süsteemide kasutamise kohta piiravaid õigusakte.

10.4.2. Riigisisene õigus peab järgima tehisintellektimääruse artikli 5 lõike 1 punktis h sätestatud piiranguid ja tingimusi

- (412) Kuna reaalajas toimuva biomeetrilise kaugtuvastamise süsteemide kasutamist avalikult juurdepääsetavas ruumis õiguskaitse eesmärgil peetakse põhiõigustesse sekkumiseks, on tehisintellektimääruse artikli 5 lõikes 5 sätestatud, et selline kasutamine kehtestatakse riigisisises õiguses. Need liikmesriigi õigusaktid annavad õigusliku aluse selliste süsteemide kasutamiseks.
- (413) Riigisisised õigusaktid ei tohi ületada tehisintellektimääruse artikli 5 lõike 1 punktis h sätestatud piire ja peavad järgima kõiki muid tehisintellektimääruses sätestatud tingimusi. See tähendab, et liikmesriigid ei tohi laiendada eesmärke, mille saavutamiseks võib reaalajas toimuvat biomeetrilist kaugtuvastamist kasutada avalikult juurdepääsetavas ruumis õiguskaitse eesmärkidel, üle piiride, mis on loetletud tehisintellektimääruse artikli 5 lõike 1 punkti h alapunktides i–iii²³³.
- (414) Liikmesriigid teatavad oma õigusaktidest komisjonile hiljemalt 30 päeva jooksul pärast nende vastuvõtmist. Selline teatamine ei anna eeldust, et liikmesriikide õigusaktid on kooskõlas tehisintellektimäärusega. Pärast teate saamist saadab Euroopa tehisintellektiamet kinnituse teate kättesaamise kohta. Liikmesriikidel soovitatakse enne kavandatud riigisisese (või piirkondliku) õigusakti vastuvõtmist saata Euroopa tehisintellektiametile selle esialgne versioon. Igal juhul võib see, kui pärast vastuvõtmist ei esitata Euroopa tehisintellektiametile artikli 5 lõikes 5 sätestatud 30päevase tähtaja jooksul teadet, tähendada, et riigisisene õigus ei ole kohtumenetluses jõustatav, nagu eri kontekstides on leitud²³⁴. Komisjon avaldab liikmesriikide õigusaktid avalikul veebisaidil.
- (415) Liikmesriigid võivad kooskõlas liidu õigusega kehtestada piiravaid seadusi, st seadusi, mis sisaldavad rangemaid nõudeid kui need, mis on sätestatud tehisintellektimääruse artikli 5 lõike 1 punktis h ja lõigetes 2–7.

²³³ Vt kohtuotsus, Euroopa Kohus, 5. aprill 2022, Commissioner of An Garda Síochána, C-140/20, ECLI:EU:C:2022:258, punkt 54: „Proportsionaalsuse nõude järgimiseks peavad liikmesriigi õigusaktis olema ette nähtud selged ja täpsed reeglid, mis reguleerivad asjaomase meetme ulatust ja kohaldamist ning millega on kehtestatud miinimumnõuded.“

²³⁴ Vt analoogselt kohtuotsus, Euroopa Kohus, 19. detsember 2019, Airbnb Ireland, C-390/18, EU:C:2019:1112, punktid 96–97.

10.4.3. Üksikasjalikud riigisisesed õigusaktid loa taotlemise, andmise ja kasutamise kohta

- (416) Loa taotlemise, andmise ja kasutamise suhtes kohaldatavad üksikasjalikud õigusnormid kehtestatakse riigisiseses õiguses. Iga liikmesriik, kes soovib lubada kõnealuste süsteemide kasutamist, peab oma õiguses täpsustama sellised õigusnormid, mille eesmärk on anda luba andvale asutusele asjakohast ja täielikku teavet reaalajas toimuva biomeetrilise kaugtuvastamise süsteemide kasutamise kohta, et ta saaks otsustada, kas selline kasutamine on rangelt vajalik ja proportsionaalne.

Reaalajas toimuva biomeetrilise kaugtuvastamise süsteemide kasutamist lubav riigisise õigus võib reguleerida näiteks järgmist:

- kes on pädevad asutused, kelle suhtes kohaldatakse tehisintellektimääruse artikli 5 lõike 1 punkti h, ja liikmesriigi sõltumatud asutused, kes on pädevad lube väljastama või sellest keelduma;
- nende eesmärkide üksikasjalik ulatus, mille saavutamiseks võib avalikult juurdepääsetavas ruumis kasutada reaalajas toimuvat biomeetrilist kaugtuvastamist õiguskaitse eesmärgil (ilma artikli 5 lõike 1 punkti h alapunktides i–iii loetletud eesmärkidest kaugemale minemata, kuid potentsiaalselt neid veelgi kitsamalt piiritledes);
- nõue, et taotlused peavad olema kirjalikud, ja nõue, et konkreetse kuriteo/olukorra puhul tuleb konkreetse kasutamise ja kavandatud kasutamise kohta esitada üksikasjalik selgitus, mis õigustab süsteemi kasutamist;
- nõue, et selgitataks motivatsiooni ja esitataks tõendusmaterjal (ja selle tõlge, kui see on asjakohane), mis põhjendab süsteemi kasutamist tehisintellekti määruse artikli 5 lõike 1 punkti h alapunktides i–iii loetletud eesmärkide saavutamiseks, eelkõige seoses koha, ajavahemiku ja isikulise kohaldamisalaga ning põhjendades süsteemi kasutamise ranget vajadust ja proportsionaalsust, sealhulgas selle asjakohasust, piisavust ja tõhusust ning vähem sekkuvate vahendite puudumist;
- kasutatava tehnoloogia kirjeldus ja andmete kogumise asukohapunktid;
- kasutatavate süsteemide minimaalne usaldusväärsus, kasutatud künnis ja täpsusmäärad;
- võimalus esitada esitatud teavet, sealhulgas tehnilisi üksikasju ja täpsuskriteeriume, et luba andev asutus saaks igal ajal *ex ante* ja *ex post* kontrolle teha;
- kasutatavate võrdlusandmebaaside tehniline kirjeldus;
- kogutud andmete ja kõigi muude kasutatud isikuandmete säilitamise kestus;
- turvameetmed, sealhulgas andmete ebaseadusliku juurdepääsu vastu;
- muud kaitsemeetmed (kui see on asjakohane);
- erasektori või ametiasutustega, sealhulgas teiste riikide ametiasutustega tehtava koostöö ning andmeedastuse ja -vahetuse kirjeldus;

- protsessi jälgitavus;
- juurutajate vastutavate isikute nimed;
- muud lubade andmisega seotud ametlikud elemendid:
- kirjaliku menetluse võimalus koos ärakuulamisega;
- keeldumise põhjused;
- nende isikute õigused, keda otsitakse, nende isikute õigused, kelle andmeid kogutakse, ja kolmandate isikute võimalikud õigused²³⁵;
- tähtajad, mille jooksul ametiasutused peavad oma otsuse tegema;
- mis tahes vajadus ametlike teatiste järele, kui antakse luba või keeldutakse selle andmisest;
- karistused (formaalsete ja oluliste) nõuete täitmata jätmise eest;
- õigus esitada kaebus loa andmisest keeldumise kohta;
- seoses loa kasutamisega:
- reaalajas toimuva biomeetrilise kaugtuvastamise süsteemide kasutamise registreerimine keskregistris koos sisuliste elementide kokkuvõttega;
- võimalikud edasised aruandluskohustused;
- loa pikendamise või muutmise menetlus.

10.4.4. Üksikasjalikud riigisisised õigusaktid, mis käsitlevad järelevalvet ja aruandlust seoses loa andmisega

- (417) Tehisintellektimääruse artikkel 70 kohustab liikmesriike looma vähemalt ühe teavitava asutuse ja vähemalt ühe turujärelevalveasutuse. Tehisintellektimääruse artikli 74 lõikes 8 on sätestatud, et „määravad liikmesriigid käesoleva määruse kohaldamisel turujärelevalveasutuseks kas määruse (EL) 2016/679 või direktiivi (EL) 2016/680 kohaselt pädeva andmekaitse järelevalveasutuse või mis tahes muu direktiivi (EL) 2016/680 artiklites 41–44 sätestatud samadel tingimustel määratud asutuse“.
- (418) See lisandub luba andva asutuse määramisele, mida liikmesriik peab tegema enne, kui ta saab lubada reaalajas toimuva biomeetrilise kaugtuvastamise süsteemide kasutamist tehisintellektimääruse artikli 5 lõike 1 punkti h alapunktides i–iii loetletud eesmärkidel.

10.5. Riiklike turujärelevalveasutuste ja liikmesriikide andmekaitseasutuste aastaaruanded

Tehisintellektimääruse artikli 5 lõikes 6 on sätestatud:

„Riiklikud turujärelevalveasutused ja liikmesriikide riiklikud andmekaitseasutused, keda on lõike 4 kohaselt teavitatud reaalajas toimuva biomeetrilise kaugtuvastamise süsteemide kasutamisest avalikult juurdepääsetavas ruumis õiguskaitse eesmärkidel,

²³⁵

Vt nt Euroopa Andmekaitsekoostöögrupp, „Suunised 05/2022 näotuvastustehnoloogia kasutamise kohta õiguskaitse valdkonnas“, versioon 2.0, 26. aprill 2023, lk 24 jj.

esitavad komisjonile sellise kasutamise kohta aastaaruanded. Selleks esitab komisjon liikmesriikidele ning riiklikele turujärelevalve- ja andmekaitseasutustele vormi, mis sisaldab teavet pädevate õigusasutuste või sõltumatu haldusasutuse poolt, kelle otsus on siduv, lõike 3 kohaste loataotluste suhtes tehtud otsuste arvu ja nende tulemuste kohta.“

- (419) Riiklikud turujärelevalveasutused ja liikmesriikide riiklikud andmekaitseasutused, keda on juurutajad teavitanud reaalajas toimuva biomeetrilise kaugtuvastamise süsteemide kasutamisest avalikult juurdepääsetavas ruumis õiguskaitse eesmärkidel (vt artikli 5 lõige 4), peavad esitama komisjonile sellise kasutamise kohta aastaaruanded. Need aruanded koostatakse komisjoni esitatud vormi alusel. See vorm luuakse hiljem.
- (420) Kui juurutaja on ELi institutsioon, asutus või amet, on Euroopa andmekaitseinspektor kohustatud igal aastal teavitama komisjoni reaalajas toimuva biomeetrilise kaugtuvastamise süsteemidest, mida kasutatakse avalikult juurdepääsetavas ruumis õiguskaitse eesmärgil.
- (421) Ajavahemikku 2. veebruarist 2025 kuni 2. augustini 2025 hõlmab ainult riikliku andmekaitseasutuse aruanne, kuna tehisintellektimäärus ei nõua liikmesriikidelt riikliku turujärelevalveasutuse määramist enne viimasena nimetatud kuupäeva.
- (422) Riiklikud turujärelevalveasutused ja riiklikud andmekaitseasutused võivad vabalt otsustada, kas nad soovivad esitada eraldi aruanded või ühisaruande liikmesriigi kohta.

10.6. Komisjoni aastaaruanded

Tehisintellektimääruse artikli 5 lõikes 7 on sätestatud:

„Komisjon avaldab lõikes 6 osutatud aastaaruannete põhjal aastaaruanded reaalajas toimuva biomeetrilise kaugtuvastamise süsteemide kasutamise kohta avalikult juurdepääsetavates ruumides õiguskaitse eesmärgil, tuginedes liikmesriikide koondandmetele. Nimetatud aastaaruanded ei sisalda asjaomase õiguskaitsealase tegevuse tundlikke operatiivandmeid.“

- (423) Tehisintellektimääruses on nõutud, et komisjon avaldaks igal aastal koondandmete põhjal aruanded selle kohta, kuidas liikmesriigid ning liidu institutsioonid, ametid ja asutused kasutavad reaalajas toimuva biomeetrilise kaugtuvastamise süsteeme avalikult juurdepääsetavas ruumis õiguskaitse eesmärgil. Need aruanded põhinevad tabelil, mille riiklikud ametiasutused on tehisintellektimääruse artikli 5 lõike 6 kohaselt edastanud.
- (424) Komisjoni aastaaruanne ei sisalda tundlikke operatiivandmeid. Tundlikud operatiivandmed on „operatiivandmed, mis on seotud kuritegude tõkestamise, avastamise, uurimise või nende eest vastutusele võtmisega ning mille avalikustamine võib ohustada kriminaalmenetluse terviklikkust“²³⁶. See võib tähendada, et konkreetseid üksikasju, mis võivad käimasolevad või varasemad uurimised päevavalgele tuua, nagu näiteks asukohad ja kasutatud kaamerad, ei avaldata.

10.7. Kohaldamisalast välja jäävad olukorrad

²³⁶

Tehisintellektimääruse artikli 3 punkt 38.

- (425) Kõik muud biomeetrilise kaugtuvastamise süsteemide kasutusviisid, mis ei kuulu tehisintellektimääruse artikli 5 lõike 1 punktis h sätestatud keelu alla, kuuluvad artiklis 6 määratletud ja tehisintellektimääruse III lisa punkti 1 alapunktis a loetletud suure riskiga tehisintellektisüsteemide kategooriasse, tingimusel et need kuuluvad tehisintellektimääruse kohaldamisalasse.
- (426) Biomeetrilise kaugtuvastamise süsteemid, mis ei kuulu tehisintellektimääruse artikli 5 lõike 1 punktis h sätestatud keelu kohaldamisalasse, hõlmavad biomeetrilisi kontrolli-/autentimissüsteeme ja biomeetrilise kaugtuvastamise süsteemide tagasiulatuvat kasutamist avalikult juurdepääsetavas ruumis õiguskaitse eesmärgil. Näiteks võivad politseiasutused olla riigisisese õiguse kohaselt volitatud kasutama tagasiulatuvat näotuvastust, et võrrelda kuriteos kahtlustatavate pilte kriminaalõiguslikus andmebaasis salvestatud näokujutistega²³⁷. Teine kasutusviis, mis ei kuulu keelu kohaldamisalasse, on reaalajas biomeetrilise kaugtuvastamise süsteemide kasutamine õiguskaitse eesmärkidel kas eraviisiliselt (näiteks kellegi juures) või veebiruumis (näiteks jututoa või veebimängu kasutamine laste seksuaalset kuritarvitamist kujutava materjali levitamises kahtlustatava isiku tuvastamiseks). Lõpuks, biomeetrilise kaugtuvastamise süsteemide kasutamine eraõiguslike isikute poolt nii reaalajas kui ka tagantjärele (nagu näotuvastustehnoloogia kasutamine reaalajas, et tuvastada supermarketis teadaolevaid poevargaid, näotuvastustehnoloogia kasutamine spordiareenil, et tuvastada isikud, kellel on keelatud siseneda areenile, või näotuvastustehnoloogia kasutamine koolides turvalisuse ja koolikohustuse täitmise eesmärgil) ei kuulu keelu kohaldamisalasse.
- (427) Lisaks õigusnormidele, mida kohaldatakse üldiselt suure riskiga tehisintellektisüsteemide suhtes, kohaldatakse **biomeetrilise kaugtuvastamise süsteemide õiguskaitse eesmärgil tagantjärele kasutamise** suhtes lisatingimusi ja -kaitsemeetmeid vastavalt tehisintellektimääruse artikli 26 lõikele 10 (kohaldatakse alates 2. augustist 2026)²³⁸.
- (428) Kasutamine **muul kui õiguskaitse eesmärgil** peab igal juhul vastama **andmekaitse normidele**. Allpool esitatud juhtumid illustreerivad isikuandmete kaitse üldmääruse artikli 9 lõike 2 tõlgendamist sellise kasutamise korral ja biomeetriliste andmete töötlemise erandeid.

Näiteks:

- Prantsuse halduskohus leidis, et kahes avalikus koolis juurdepääsukontrolli ja turvalisuse eesmärgil toimunud näotuvastustehnoloogia katsetamine ei olnud (andmekaitse normide kohaselt) vajalik ega proportsionaalne. Olemas olid alternatiivsed lahendused, mis olid õpilaste jaoks vähem sekkuvad, nt märkide kasutamine. Lisaks ei olnud täidetud selgesõnalise nõusoleku tingimused. Seetõttu

²³⁷ Näiteks *Traitement des Antécédents Judiciaires* andmebaas Prantsusmaal, mis on loodud dekreediga nr 2012-652 (*Décret no. 2012-652 du 4 mai 2012 relatif au Traitement des Antécédents Judiciaires*).

²³⁸ Tehisintellektimääruse artikli 26 lõike 10 ja põhjendus 94.

ei saanud nõusolekut kasutada keskkoolides näotuvastustehnoloogia katsetamise õigusliku alusena²³⁹;

- üks Hollandi supermarket ei tohtinud kasutada poevarguste tõkestamiseks näotuvastustehnoloogiat. Ilma kliendi selgesõnalise nõusolekuta või olulise avaliku huvi (nt turvalisuse) eesmärgil töötlemist võimaldava õigusliku aluseta ei saanud supermarket töödelda biomeetrilisi andmeid ja seega kasutada näotuvastustehnoloogiat²⁴⁰;
- Prantsusmaal²⁴¹ keelati reaalajas näotuvastustehnoloogia kasutamine jalgpalliklubi sissepääsu juures fännide tuvastamiseks ja Hispaanias keelati selle kasutamine pealtvaatajate ohutuse tagamiseks²⁴².

10.8. Kasutusnäited

Politsei paigaldab Euroopa meistrivõistluste mängu ajal jalgpallistaadioni peasissekäigu juurde politseibussile tehisintellektipõhise näotuvastustehnoloogiaga varustatud mobiilsed valvekaamerad, et tagada ala turvalisus ja tuvastada isikud, kelle näod on salvestatud tagaotsitavate isikute sihtotstarbelisse jälgimisnimekirja. See jälgimisnimekiri sisaldab isikuid, keda kahtlustatakse kuriteo toimepanemises (alates rasketest kuritegudest kuni pettuste ja sissemurdmisteni), isikuid, kes võivad pakkuda huvi luure seisukohalt, ja haavatavaid isikuid, kellel on vaimse tervise probleeme. Politsei näotuvastustehnoloogiatega kasutamine ei ole seotud teabega selle kohta, kas konkreetne isik viibib üritusel. Kuigi tõenäoliselt on jälgimisnimekirjas inimesi, kelle otsimiseks oleks lubatud reaalajas toimuva biomeetrilise kaugtuvastamise kasutamine, on see nimekiri liiga suunitlemata ja ei ole seotud jalgpallimängu sündmusega. Seega oleks selline kasutamine keelatud.

Biomeetriline tuvastussüsteem (mitte kaugjuhitav) kontrollib, kas inimestel on juurdepääs tuumaelektrijaama. Kui inimesed ilmuvad (ilmselge) kaamera ette ja süsteem keeldub neile juurdepääsu võimaldamast, püüab süsteem seejärel kindlaks teha, kas isik on terroristide jälgimisnimekirjas. Süsteem ei ole kaugjuhitav. Isikud osalesid aktiivselt kontrollimisel, et saada sissepääs jaama. Kõnealune kasutusjuhtum ei kuulu tehisintellektimääruse artiklis 5 sätestatud keelu alla.

Ühe tiheda liiklusega linna politseiasutused kasutavad tehisintellektipõhiseid valvekaameraid, mis suudavad rakendada näotuvastustehnoloogiat otseülekandes. Võimalik, et näotuvastusfunktsioonile lisatakse ka muid funktsioone, näiteks objektide tuvastamine ja rahvahulga liikumine.

Nad paigutavad need kaamerad mitmesse kohta, sealhulgas pühakodadesse, mitmesse kohta, mida külastavad LGBT+ kogukonna esindajad, arstikabinettidesse, apteekidesse ning erinevatesse restoranidesse ja baaridesse. Biomeetriliste kaamerate

²³⁹ TA Marseille (Marseille' halduskohus), 27. veebruar 2020, nr 1901249.

²⁴⁰ <https://www.autoriteitpersoonsgegevens.nl/en/current/dutch-dpa-issues-formal-warning-to-supermarket-for-use-of-facial-recognition-technology>.

²⁴¹ <https://www.cnil.fr/fr/reconnaissance-faciale-et-interdiction-commerciale-de-stade-la-cnif-adresse-un-avertissement-un-club>

²⁴² <https://www.biometricupdate.com/202401/spanish-data-authority-opposes-facial-recognition-for-football-stadium-access>

paigaldamine kui selline ei ole tehisintellektimäärusega keelatud. Teatavad kasutusviisid, sealhulgas füüsiliste isikute suunitlemata ja valimatu tuvastamine, on siiski keelatud.

Suvevaheajal toimus elamurajoonis mitu sissemurdmist. Politsei saab kahtlusaluse kirjelduse pealtnägijatel, kes nägid kahtlusalust ümbruskonnas erinevatel hetkedel enne sissemurdmist. Kahtlusaluse tuvastamiseks ja kinnipidamiseks kasutab politsei nädalavahetusel naabruskonnas mitmes kohas reaajas näotuvastustehnoloogiat. Pealtnägijate teadete põhjal lõi politsei kahtlusaluse näo komposiitkujutise ja võttis andmebaasist mitu pilti isikutest, kelle nägu sellega sarnanes.

Isegi kui politsei kasutab näotuvastustehnoloogiat sihtmärgiks oleva kahtlusaluse suhtes ja on kindlaks määranud piirkonna ja kasutamisaja, ei ole selle kasutamine lubatud sellise õigusrikkumise puhul, mida ei ole loetletud tehisintellektimääruse II lisas.

Politsei jälgib jalgpallistaadionil biomeetrilise tuvastussüsteemi abil fännide emotsioone. Süsteem märkab potentsiaalset agressiooni ja rakendab selles staadioni osas kohe reaajas toimuvat biomeetrilist kaugtuvastamist, et tuvastada huligaanid, kes on varem vägivallatsenud.

Emotsioonide jälgimine staadionil ei ole tehisintellektimääruse kohaselt keelatud (kuid see kuulub siiski tehisintellektimääruse suure riskiga süsteemide kategooriasse). Reaajas toimuva biomeetrilise kaugtuvastamise rakendamine oleks aga tehisintellektimääruse kohaselt keelatud, eelkõige juhul, kui biomeetriline süsteem otsustab, kas isikuid on vaja õiguskaitse eesmärgil tuvastada.

Politsei tugineb linna ja metroosse paigaldatud videovalvõrgule, et tuvastada poliitiline meelevaldaja, kes organiseeris tänaval ühisprotesti. Asjaomasel liikmesriigis peavad avalikel teedel ja avalikel aladel, näiteks tänavatel, toimuvate ühismeeleavalduste korraldajad teavitama kohalikke omavalitsusi kolm päeva enne kavandatud meelevaldust, et vältida avalikku korra rikkumist ja vägivald. Teatamata jätmine on kuritegu, mille eest võib määrata kuni kuue kuu pikkuse vangistuse ja maksimaalselt 8 000 euro suuruse trahvi. Meelevaldaja tuvastamiseks kasutab politsei tänavatele paigaldatud valvekaamerate videovooge ja teeb nende põhjal tagasiulatuva näotuvastuse, võrreldes saadud pilte sotsiaalmeedias avaldatud fotodega.

Näotuvastustehnoloogia tagasiulatuva kasutamine ei ole tehisintellektimäärusega keelatud. Sellist kasutamist peetakse suure riskiga süsteemiks ja see peaks vastama tehisintellektimääruses selliste süsteemide kohta kehtestatud nõuetele²⁴³.

²⁴³

Biomeetriliste andmete töötlemine õiguskaitse eesmärgil kuulub endiselt direktiivi artikli 10 kohaldamisalasse, mida tuleb rakendada riiklikul tasandil. Nende töötlemine selleks, et kasutada näotuvastustehnoloogiat tagasiulatuvalt, peaks olema lubatud ainult siis, kui see on hädavajalik, ja selle suhtes tuleks kohaldada asjakohaseid kaitsemeetmeid. On küsitav, kas näotuvastustehnoloogia tagasiulatuva kasutamine on meelevaldaja tuvastamiseks rangelt vajalik. Selle stsenaariumi aluseks olevas otsuses kohtuasjas Glukhin vs. Venemaa otsustas Euroopa Inimõiguste Kohus, et kuigi kuritegude avastamine võib olla õiguspärane eesmärk, oli näotuvastustehnoloogia kasutamine – nii tagantjärele kui ka reaajas – ebaproportsionaalne, kuna ei olnud ohtu avalikule korrale ega

Veel näiteid kasutusviisidest, mis EI OLE keelatud:

- hotellid kasutavad VIP-külaliste äratundmiseks reaalajas toimuvat biomeetrilist kaugtuvastamist. See ei ole õiguskaitse;
- kaubanduskeskused kasutavad reaalajas toimuvat biomeetrilist kaugtuvastamist, et tuvastada poevargaid. See ei ole õiguskaitse.

Keelatud:

kaubanduskeskus kasutab politsei loal poevaraste leidmiseks reaalajas toimuvat biomeetrilist kaugtuvastamist. Süsteemi kasutatakse avalikult juurdepääsetavas ruumis õiguskaitse eesmärgil. Selline kasutamine on keelatud, sest poevaraste otsimine ei kuulu ühegi tehisintellektimääruse artikli 5 lõike 1 punktis h loetletud erandi alla.

11. KOHALDAMINE

- (429) Tehisintellektimääruse artikli 113 kohaselt kohaldatakse tehisintellektimääruse artiklit 5 alates 2. veebruarist 2025. Selles sättes sätestatud keelud kehtivad põhimõtteliselt kõigile tehisintellektisüsteemidele, olenemata sellest, kas need on turule lastud või kasutusele võetud enne või pärast kõnealust kuupäeva²⁴⁴.
- (430) 2. augustil 2025 hakatakse kohaldama peatükke juhtimise ja karistuste kohta. Sellest tulenevalt ei kohaldata enne 2. augustit 2025 sätteid, mis käsitlevad karistusi tehisintellektimääruse artikli 5 sätete rikkumise eest. Sellel üleminekuperioodil ei ole ka turujärelevalveasutusi, kes jälgiksid, kas keelde järgitakse nõuetekohaselt.
- (431) Sellest hoolimata on keelud isegi sellel üleminekuperioodil täielikult kohaldatavad ning tehisintellektisüsteemide pakkujatele ja juurutajatele kohustuslikud. Seepärast peaksid kõnealused ettevõtjad võtma vajalikke meetmeid tagamaks, et nad ei laseks turule, ei võtaks kasutusele ega kasutaks tehisintellektisüsteeme, mis võivad tehisintellektimääruse artikli 5 kohaselt kujutada endast keelatud kasutusviisi. Isegi kui järelevalvet ja trahve käsitlevad sätted hakkavad kehtima alles hiljem, on keeldudel endil otsene mõju ning võimaldavad seega mõjutatud isikutel neid riiklikes kohtutes täitmisele pöörata ja taotleda ajutisi ettekirjutusi keelatud kasutusviiside vastu.

12. KOMISJONI SUUNISTE LÄBIVAATAMINE JA AJAKOHASTAMINE

- (432) Need suunised on tehisintellektimääruse artiklis 5 sätestatud keeldude esimene tõlgendus koos praktiliste näidetega. Komisjon pakub operaatoritele ja ametiasutustele täiendavat tuge, kuidas mõista keelde ja koguda täiendavaid praktilisi kasutusjuhtumeid, mille kohta annavad tagasisidet tehisintellektisüsteemide pakkujad ja juurutajad, Euroopa tehisintellekti nõukoda ja muud asjaomased sidusrühmad.
- (433) Komisjon vaatab suunised läbi niipea, kui see on vajalik, võttes arvesse keeldude rakendamisel saadud praktilisi kogemusi ning tehnoloogia, ühiskonna ja regulatiivse arengu tempot selles valdkonnas. See hõlmab ka kõiki asjakohaseid kogemusi

²⁴⁴ liiklusohutusele. Kohus rõhutas näotuvastustehnoloogia „väga sekkuvat“ olemust. Selles kohtuasjas jõudis kohus järeldusele, et näotuvastustehnoloogia kasutamine ei täitnud pakilist sotsiaalset vajadust ega olnud demokraatlikus ühiskonnas vajalik. Vt tehisintellektimääruse artikli 111 lõiked 1 ja 2, milles täpsustatakse, et ajutiselt kohaldatava varasemalt kehtinud nõude klausel ei piira tehisintellektimääruse artikli 5 kohaldamist, millele on osutatud tehisintellektimääruse artikli 113 kolmanda lõigu punktis a.

turujärelevalve jõustamise meetmete ja selle kohta, kuidas Euroopa Liidu Kohus tõlgendab nendes suunistes käsitletud tehisintellektimääruse keelde ja muid sätteid. Sellise läbivaatamise käigus võib komisjon otsustada suunised tagasi võtta või neid muuta. Komisjon julgustab tehisintellektisüsteemide pakkujaid ja juurutajaid, riiklikke turujärelevalveasutusi Euroopa tehisintellekti nõukoja kaudu, tehisintellekti nõuandvat kogu, teadusringkondi ja kodanikuühiskonna organisatsioone selles protsessis osalema, vastates tulevastele üleskutsetele avalikuks aruteluks.

TÕESTATUD KOOPIA
Peasekretäri nimel

Martine DEPREZ
Direktor
Otsustusprotsess ja kollegiaalsus
EUROOPA KOMISJON