Euroopa Liidu
Nõukogu

Brüssel, 23. aprill 2021
(OR. en)

8115/21

Institutsioonidevaheline dokument: 2021/0106(COD)

TELECOM 156
JAI 429
COPEN 191
CYBER 108
DATAPROTECT 103
EJUSTICE 41
COSI 69
IXIM 74
ENFOPOL 148
FREMP 103
RELEX 347
MI 271
COMPET 275
IA 60
CODEC 573

SAATEMÄRKUSED

Saatja:	Euroopa Komisjoni peasekretär, allkirjastanud Martine DEPREZ, direktor
Kättesaamise kuupäev:	22. aprill 2021
Saaja:	Jeppe TRANHOLM-MIKKELSEN, Euroopa Liidu Nõukogu peasekretär
Komisjoni dok nr:	COM(2021) 206 final
Teema:	Ettepanek: EUROOPA PARLAMENDI JA NÕUKOGU MÄÄRUS, MILLEGA NÄHAKSE ETTE TEHISINTELLEKTI KÄSITLEVAD ÜHTLUSTATUD ÕIGUSNORMID (TEHISINTELLEKTI KÄSITLEV ÕIGUSAKT) JA MUUDETAKSE TEATAVAID LIIDU ÕIGUSAKTE

Käesolevaga edastatakse delegatsioonidele dokument COM(2021) 206 final.

Lisatud: COM(2021) 206 final

EUROOPA
KOMISJON

Brüssel, 21.4.2021
COM(2021) 206 final

2021/0106 (COD)

Ettepanek:

EUROOPA PARLAMENDI JA NÕUKOGU MÄÄRUS,

MILLEGA NÄHAKSE ETTE TEHISINTELLEKTI KÄSITLEVAD ÜHTLUSTATUD ÕIGUSNORMID (TEHISINTELLEKTI KÄSITLEV ÕIGUSAKT) JA MUUDETAKSE TEATAVAID LIIDU ÕIGUSAKTE

{SEC(2021) 167 final} - {SWD(2021) 84 final} - {SWD(2021) 85 final}

SELETUSKIRI

1. ETTEPANEKU TAUST

1.1. Ettepaneku põhjused ja eesmärgid

Käesolev seletuskiri lisatakse ettepanekule võtta vastu määrus, millega nähakse ette tehisintellekti käsitlevad ühtlustatud õigusnormid (tehisintellekti käsitlev õigusakt). Tehisintellekt on kiirelt arenev tehnoloogiaharu, mis võib luua mitmesuguseid majanduslikke ja ühiskondlikke hüvesid kõigis tööstusharudes ja kogu ühiskonnas. Prognooside täiustamise, tegevuse ja vahendite jaotuse optimeerimise ja personaalsema teenuseosutamisega võib tehisintellekt toetada ühiskonnale ja keskkonnale kasulikke tulemusi ning luua olulise konkurentsieelise ettevõtjatele ja Euroopa majandusele. Selline tegevus on eriti vajalik suure mõjuga valdkondades, sealhulgas kliimamuutused, keskkond ja tervis, avalik sektor, rahandus, liikuvus, siseküsimused ja põllumajandus. Samad elemendid ja meetodid, mis aitavad tehisintellektil luua sotsiaal-majanduslikke hüvesid, võivad aga kaasa tuua uusi riske või negatiivseid tagajärgi üksikisikutele või ühiskonnale. Arvestades tehniliste muutuste kiirust ja võimalikke probleeme, püüab EL saavutada tasakaalustatud käsitust. ELi huvides on säilitada tehnoloogia vallas juhtpositsioon ja tagada, et eurooplased saavad kasu uuest tehnoloogiast, mis on välja arendatud ja toimib kooskõlas liidu väärtuste, põhiõiguste ja põhimõtetega.

Käesoleva ettepanekuga täidetakse president von der Leyeni poolt järgmisele komisjonile (2019–2024) antud poliitilistes suunistes „Liit, mis seab kõrgemad sihid“[1] võetud poliitiline kohustus, mille kohaselt komisjon teeb ettepaneku võtta vastu õigusakt, mis tagab kooskõlastatud Euroopa käsitluse tehisintellekti mõjust inimesele ja eetikale. Selle teadaande järel avaldas komisjon 19. veebruaril 2020 valge raamatu „Tehisintellekt: Euroopa käsitus tipptasemel ja usaldusväärsest tehnoloogiast“[2]. Valges raamatus on esitatud poliitikavariandid selle kohta, kuidas täita kaks võrdset eesmärki: soodustada tehisintellekti kasutuselevõttu ja tegeleda selle tehnoloogia teatavate kasutusviisidega seotud riskidega. Käesoleva ettepanekuga taotletakse teist eesmärki, milleks esitatakse ettepanek usaldusväärse tehisintellekti õigusraamistiku loomise kohta, et luua usaldusväärne ökosüsteem. Ettepanek põhineb ELi väärtustel ja põhiõigustel ning sellega soovitakse anda inimestele ja muudele kasutajatele kindlustunnet tehisintellektipõhiste lahenduste kasutamisel, julgustades samas ettevõtjaid neid välja arendama. Tehisintellekt peaks olema inimeste abivahend ja ühiskonda edasiviiv jõud, mille lõppeesmärk on suurendada inimeste heaolu. Seepärast peaksid liidu turul olemasolevat või liidu kodanikke muul viisil mõjutavat tehisintellekti käsitlevad eeskirjad olema inimesekesksed, et inimesed saaksid olla kindlad, et tehnoloogiat kasutatakse ohutul ja õiguspärasel viisil, sealhulgas austades põhiõigusi. Pärast valge raamatu avaldamist alustas komisjon ulatuslikku konsulteerimist sidusrühmadega. Suur hulk sidusrühmi oli väga huvitatud ja toetas valdavalt regulatiivset sekkumist, et tegeleda tehisintellekti suurenevast kasutamisest tulenevate probleemide ja muredega.

Ettepanek on ühtlasi vastus Euroopa Parlamendi ja Euroopa Ülemkogu sõnaselgetele korduvatele nõudmistele võtta õiguslikud meetmed, et tagada hästi toimiv tehisintellektisüsteemide siseturg, kus liidu tasandil käsitletakse asjakohaselt nii tehisintellekti

[1] https://ec.europa.eu/info/sites/default/files/political-guidelines-next-commission_et.pdf.

[2] Euroopa Komisjoni 2020. aasta valge raamat „Tehisintellekt: Euroopa käsitus tipptasemel ja usaldusväärsest tehnoloogiast“, COM(2020) 65 final.

kasulikkust kui ka riske. See toetab Euroopa Ülemkogu[3] püstitatud liidu eesmärki võtta ülemaailmne juhtroll turvalise, usaldusväärse ja eetilise tehisintellekti arendamises ning tagab eetikapõhimõtete kaitse, mida on konkreetselt nõudnud Euroopa Parlament[4].

Euroopa Ülemkogu nõudis 2017. aastal esilekerkivate suundumuste kiiret käsitlemist, mis „hõlmab selliseid küsimusi nagu tehisintellekt [...], tagades samal ajal andmekaitse, digitaalõiguste ja eetiliste standardite kõrge taseme“[5]. Nõukogu rõhutas 2019. aasta järeldustes, milles käsitletakse kooskõlastatud kava Euroopas loodud tehisintellekti arendamise ja kasutamise kohta,[6] kui tähtis on tagada Euroopa kodanike õiguste täielik järgimine, ja kutsus üles läbi vaatama olemasolevad asjakohased õigusaktid, et need vastaksid tehisintellektiga seotud uutele võimalustele ja väljakutsetele. Euroopa Ülemkogu on nõudnud ka suure riskiga tehisintellektirakenduste selget määratlemist[7].

Viimastes, 21. oktoobril 2020 avaldatud järeldustes nõuti ka teatavate tehisintellektisüsteemide musta kasti efekti, keerukuse, kallutatuse, teatava ettearvamatuse ja osaliselt autonoomse käitumise probleemiga tegelemist, et tagada nende kokkusobivus põhiõigustega ja hõlbustada õigusnormide jõustamist[8].

Ka Euroopa Parlament on teinud tehisintellekti valdkonnas märkimisväärselt palju. Parlament võttis 2020. aasta oktoobris vastu mitu tehisintellektiga seotud resolutsiooni, sealhulgas eetika,[9] vastutuse[10] ja autoriõiguse[11] teemal. Nendele järgnesid 2021. aastal resolutsioonid tehisintellekti kohta kriminaalasjades[12] ning haridus-, kultuuri- ja audiovisuaalsektoris[13]. Parlamendi resolutsioonis tehisintellekti, robotitehnoloogia ja seonduva tehnoloogia eetiliste aspektide raamistiku kohta soovitatakse komisjonil välja pakkuda õiguslikud meetmed, et kasutada ära tehisintellekti pakutavaid võimalusi ja hüvesid, kuid ühtlasi tagada eetikapõhimõtete kaitse. Resolutsioon hõlmab tehisintellekti, robotitehnoloogia ja seonduva tehnoloogia arendamise, juurutamise ja kasutamise eetikapõhimõtteid käsitleva määruse seadusandliku ettepaneku teksti. Kooskõlas president von der Leyeni poliitilistes suunistes võetud poliitilise kohustusega seoses ELi toimimise lepingu artikli 225 alusel Euroopa Parlamendi vastuvõetavate resolutsioonidega, võetakse käesolevas ettepanekus arvesse

---

3 Euroopa Ülemkogu, Euroopa Ülemkogu erakorraline kohtumine (1. ja 2. oktoober 2020) – Järeldused, EUCO 13/20, 2020, lk 6.

4 Euroopa Parlamendi 20. oktoobri 2020. aasta resolutsioon soovitustega komisjonile tehisintellekti, robotitehnoloogia ja seonduva tehnoloogia eetiliste aspektide raamistiku kohta, 2020/2012(INL).

5 Euroopa Ülemkogu, *Euroopa Ülemkogu erakorraline kohtumine (19. oktoober 2017) – Järeldused*, EUCO 14/17, 2017, lk 8.

6 Euroopa Liidu Nõukogu, *Tehisintellekt b) Järeldused tehisintellekti käsitleva kooskõlastatud kava kohta – Vastuvõtmine* 6177/19, 2019.

7 Euroopa Ülemkogu, *Euroopa Ülemkogu erakorraline kohtumine (1. ja 2. oktoober 2020) – Järeldused*, EUCO 13/20, 2020.

8 Euroopa Liidu Nõukogu, *Eesistujariigi järeldused – Põhiõiguste harta seoses tehisintellekti ja digitaalsete muutustega*, 11481/20, 2020.

9 Euroopa Parlamendi 20. oktoobri 2020. aasta resolutsioon tehisintellekti, robotitehnoloogia ja seonduva tehnoloogia eetiliste aspektide raamistiku kohta, 2020/2012(INL).

10 Euroopa Parlamendi 20. oktoobri 2020. aasta resolutsioon tehisintellekti tsiviilvastutuse korra kohta, 2020/2014(INL).

11 Euroopa Parlamendi 20. oktoobri 2020. aasta resolutsioon intellektuaalomandi õiguste kohta tehisintellekti tehnoloogiate arendamisel, 2020/2015(INI).

12 Euroopa Parlamendi raporti projekt tehisintellekti kohta kriminaalõiguses ning tehisintellekti politsei ja kohtuasutuste poolt kriminaalasjades kasutamise kohta, 2020/2016(INI).

13 Euroopa Parlamendi raporti projekt tehisintellekti kohta haridus-, kultuuri- ja audiovisuaalsektoris, 2020/2017(INI). Sellel teemal on komisjon vastu võtnud teatise „Digiõppe tegevuskava 2021–2027: hariduse ja koolituse ümberkujundamine digiajastu jaoks“, milles on ette nähtud välja töötada eetikasuunised seoses tehisintellekti ja andmete kasutamisega hariduses, COM(2020) 624 final.

eespool nimetatud Euroopa Parlamendi resolutsiooni, austades täiel määral proportsionaalsuse, subsidiaarsuse ja parema õigusloome põhimõtteid.

Sellises poliitilises kontekstis pakub komisjon välja tehisintellekti reguleeriva raamistiku järgmiste **erieesmärkidega**:

- tagada, et turule lastavad ja kasutatavad tehisintellektisüsteemid on ohutud ja kooskõlas kehtiva põhiõigusi käsitleva õigusega ning liidu väärtustega;
- tagada õiguskindlus tehisintellekti tehtavate investeeringute ja innovatsiooni soodustamiseks;
- tugevdada juhtimist ja tõhustada põhiõigusi käsitleva kehtiva õiguse ja tehisintellektisüsteemidele kohalduvate ohutusnõuete täitmise tagamist;
- hõlbustada seaduslike, ohutute ja usaldusväärsete tehisintellektirakenduste ühtse turu väljatöötamist ja vältida turu killustumist.

Nende eesmärkide täitmiseks esitatakse käesolevas ettepanekus tehisintellekti reguleerimise tasakaalustatud ja proportsionaalne horisontaalne käsitus, milles piirdutakse tehisintellektiga seotud riskide ja probleemidega tegelemiseks vajalike vähimate nõuetega, ilma, et põhjendamatult pärsitaks või takistataks tehnoloogia arengut või suurendataks muul viisil ebaproportsionaalselt tehisintellektilahenduste turule laskmise kulu. Ettepanekus sätestatakse põhjalik ja paindlik õigusraamistik. Ühest küljest on selle reguleerimisalased põhivalikud, sealhulgas tehisintellektisüsteemidele kohaldatavad ja põhimõtetel rajanevad nõuded, terviklikud ja tulevikukindlad. Teisest küljest kehtestatakse sellega proportsionaalne reguleeriv raamistik, mille keskmes on hästi määratletud riskipõhine regulatiivne lähenemisviis, mis ei tekita kaubandusele ebavajalikke piiranguid ja mille puhul reguleeriv sekkumine on kohandatud nendele konkreetsetele olukordadele, kus on või võib mõistlikult eeldada lähitulevikus tekkivat põhjust muretsemiseks. Samas hõlmab õigusraamistik paindlikke mehhanisme, mis võimaldavad sellel tehnoloogia arenedes ja uute muret tekitavate olukordade tekkides dünaamiliselt kohanduda.

Ettepanekus sätestatakse harmoneeritud eeskirjad tehisintellektisüsteemide arendamiseks, turule laskmiseks ja kasutamiseks liidus, järgides proportsionaalset riskipõhist lähenemisviisi. Selles esitatakse ühtne tulevikukindel tehisintellekti määratlus. Teatavad eriti kahjulikud tehisintellektiga seotud tavad keelustatakse, sest on vastuolus liidu väärtustega, ning pakutakse välja eripiirangud ja -kaitsemeetmed seoses biomeetrilise kaugtuvastamise süsteemide teatavate kasutusviisidega õiguskaitse eesmärgil. Ettepanekus sätestatakse kindel riskimetoodika, et määratleda suure riskiga tehisintellektisüsteemid, mis põhjustavad märkimisväärseid riske inimeste tervisele ja ohutusele või põhiõigustele. Need tehisintellektisüsteemid peavad vastama usaldusväärse tehisintellekti suhtes kohaldatavatele horisontaalsetele kohustuslikele nõuetele ja enne nende laskmist liidu turule tuleb nende kohta ellu viia vastavushindamismenetlused. Samuti kehtestatakse nende süsteemide pakkujatele ja kasutajatele prognoositavad, proportsionaalsed ja selged kohustused, et tagada ohutus ja selliste olemasolevate õigusaktide järgimine, mis kaitsevad põhiõigusi kogu tehisintellektisüsteemide olelusringi jooksul. Teatavatele konkreetsetele tehisintellektisüsteemidele pakutakse välja ainult minimaalsed läbipaistvuskohustused, eriti kui kasutatakse juturoboteid või nn süvavõltsinguid.

Pakutud eeskirju jõustatakse liikmesriigi tasandi juhtimissüsteemiga, võttes aluseks juba olemasolevad struktuurid, ning liidu tasandil koostööks loodava Euroopa tehisintellekti nõukoja kaudu. Ette nähakse lisameetmed innovatsiooni toetamiseks, eelkõige tehisintellekti regulatsiooni testkeskkondade ja muude meetmete kaudu, millega vähendatakse regulatiivset

koormust ning toetatakse väikeseid ja keskmise suurusega ettevõtjaid (edaspidi „VKEd“) ja idufirmasid.

1.2. Kooskõla poliitikavaldkonnas praegu kehtivate õigusnormidega

Ettepaneku horisontaalsus eeldab täielikku järjepidevust olemasolevate liidu õigusaktidega, mida kohaldatakse sektorites, kus juba kasutatakse või tõenäoliselt hakatakse lähitulevikus kasutama suure riskiga tehisintellektisüsteeme.

Tagatakse ka järjepidevus ELi põhiõiguste harta ja olemasolevate liidu teiseste õigusaktidega andmekaitse, tarbijakaitse, diskrimineerimiskeelu ja soolise võrdõiguslikkuse valdkonnas. Ettepanek ei piira isikuandmete kaitse üldmääruse (määrus (EL) 2016/679) ega õiguskaitsedirektiivi (direktiiv (EL) 2016/680) kohaldamist ja täiendab neid harmoneeritud eeskirjadega, mida kohaldatakse teatavate suure riskiga tehisintellektisüsteemide projekteerimisele, arendamisele ja kasutamisele, ning biomeetrilise kaugtuvastamise süsteemide teatavatele kasutusviisidele kohaldatavate piirangutega. Ettepanek täiendab ka diskrimineerimiskeeluga seotud olemasolevat liidu õigust erinõuetega, mille eesmärk on viia miinimumini algoritmilise diskrimineerimise risk, eelkõige seoses tehisintellektisüsteemide arendamiseks kasutatavate andmekogumite ülesehituse ja kvaliteediga. Lisaks võetakse tehisintellektisüsteemide kogu olelusringi jooksul kasutusele testimis-, riskijuhtimis-, dokumenteerimis- ja inimjärelevalve kohustused. Ettepaneku kohaldamine ei piira liidu konkurentsiõiguse kohaldamist.

Toodetes turvakomponentidena kasutatavate suure riskiga tehisintellektisüsteemide valdkonnas kaasatakse käesolev ettepanek olemasolevasse valdkondlikku ohutusõigusesse, et tagada järjepidevus, vältida dubleerimist ja viia miinimumini lisakoormus. Uue õigusraamistiku õigusaktides käsitletavate toodetega (näiteks masinad, meditsiiniseadmed, mänguasjad) seotud suure riskiga tehisintellektisüsteemidele käesolevas ettepanekus esitatud nõudeid kontrollitakse olemasolevate vastavushindamismenetluste raames uue õigusraamistiku asjakohaste õigusaktide alusel. Seoses nõuete vastastikuse mõjuga võib öelda, et kui käesolevas ettepanekus esitatud nõuetega soovitakse käsitleda tehisintellektisüsteemidele eriomaseid ohutusriske, siis uue õigusraamistiku õigusaktide eesmärk on tagada lõpptoote üldine ohutus ja seega võivad need sisaldada erinõudeid tehisintellektisüsteemi ohutu integreerimise kohta lõpptootesse. Ilmne näide sellisest lähenemisest on ettepanek masinaid käsitleva määruse kohta, mis võetakse vastu käesoleva ettepanekuga samal päeval. Käesolevat ettepanekut ei kohaldataks otseselt suure riskiga tehisintellektisüsteemidele, mis on seotud vana lähenemisviisi asjakohastes õigusaktides käsitletud toodetega (näiteks lennundus, autod). Küll aga tuleb suure riskiga tehisintellektisüsteemidele kohaldatavaid ja käesolevas ettepanekus sätestatud hädavajalikke eeltingimusi arvesse võtta nende õigusaktide alusel asjakohaste rakendus- või delegeeritud aktide vastuvõtmisel.

Seoses reguleeritud krediidiasutuste pakutavate või kasutatavate tehisintellektisüsteemidega tuleks liidu finantsteenuseid käsitlevate õigusaktide järelevalve eest vastutavad asutused nimetada pädevateks asutusteks, kes peavad jälgima käesoleva ettepaneku nõuete täitmist, et järjepidevalt oleks tagatud käesolevast ettepanekust tulenevate kohustuste ja liidu finantsteenuseid käsitlevate selliste õigusaktide täitmine, millega tehisintellektisüsteeme reguleeritakse teatavas ulatuses kaudselt seoses krediidiasutuste sisemise juhtimissüsteemiga. Järjepidevuse suurendamiseks integreeritakse vastavushindamine ja käesolevast ettepanekust pakkujatele tulenevad teatavad menetluskohustused krediidiasutuste tegevuse alustamise

tingimusi ning usaldatavusnõuete täitmise järelevalvet käsitleva direktiivi 2013/36/EL[14] kohastesse menetlustesse.

Käesolev ettepanek on ühtlasi kooskõlas teenuste, sealhulgas e-kaubanduse direktiiviga 2000/31/EÜ[15] reguleeritavate vahendusteenuste valdkonnas kohaldatavate liidu õigusaktidega ja komisjoni hiljutise ettepanekuga digiteenuste õigusakti kohta[16].

Ettepanekut ei kohaldata tehisintellektisüsteemidele, mis on Suuremahuliste IT-süsteemide Operatiivjuhtimise Euroopa Liidu Ameti (eu-LISA) juhitavas vabadusel, turvalisusel ja õigusel rajanevas alas suuremahuliste IT-süsteemide komponendid ja turule lastud või kasutusele võetud enne ühe aasta möödumist käesoleva määruse kohaldamise kuupäevast, välja arvatud juhul kui nende õigusaktide asendamine või muutmine toob kaasa asjakohase tehisintellektisüsteemi või -süsteemide projekteerimise või sihtotstarbe märkimisväärse muutmise.

1.3. Kooskõla muude liidu tegevuspõhimõtetega

Ettepanek on osa laiemast terviklikust meetmepaketist, mille eesmärk on lahendada tehisintellekti arendamisest ja kasutamisest tingitud probleeme, nagu on vaadeldud tehisintellekti käsitlevas valges raamatus. Seetõttu tagatakse järjepidevus ja täiendavus komisjoni teiste käimasolevate või kavandatud algatustega, mille eesmärk on samuti tegeleda nende probleemidega, sealhulgas vaadata läbi tooteid käsitlevad valdkondlikud õigusaktid (näiteks masinadirektiiv, üldise tooteohutuse direktiiv), ning algatustega, mille raames tegeletakse uue tehnoloogiaga, sealhulgas tehisintellektisüsteemidega seotud vastutuse küsimustega. Need algatused tuginevad käesolevale ettepanekule ja täiendavad seda, et luua õiguskindlust ja soodustada usaldusväärse tehisintellekti ökosüsteemi loomist Euroopas.

Ettepanek on kooskõlas ka komisjoni kogu digistrateegiaga, sest see toetab inimeste heaks toimivat tehnoloogiat, mis on üks kolmest teatises „Euroopa digituleviku kujundamine“[17] välja toodud poliitikasuuna tugisambast ja põhieesmärgist. Selles sätestatakse sidus, tõhus ja proportsionaalne raamistik, et tehisintellekti arendamisel austataks inimeste õigusi ja teenitaks ära nende usaldus, kujundades Euroopa digiajastule vastavaks ja muutes järgmised kümme aastat **Euroopa digikümnendiks**[18].

Tehisintellektipõhine innovatsioon on tihedalt seotud ka **andmehaldust käsitleva õigusakti**,[19] **avaandmete direktiivi**[20] ja **ELi andmestrateegia**[21] kohaste muude algatustega,

---

14 Euroopa Parlamendi ja nõukogu 26. juuni 2013. aasta direktiiv 2013/36/EL, mis käsitleb krediidiasutuste tegevuse alustamise tingimusi ning krediidiasutuste ja investeerimisühingute usaldatavusnõuete täitmise järelevalvet, millega muudetakse direktiivi 2002/87/EÜ ning millega tunnistatakse kehtetuks direktiivid 2006/48/EÜ ja 2006/49/EÜ, EMPs kohaldatav tekst, ELT L 176, 27.6.2013, lk 338–436.

15 Euroopa Parlamendi ja nõukogu 8. juuni 2000. aasta direktiiv 2000/31/EÜ infoühiskonna teenuste teatavate õiguslike aspektide, eriti elektroonilise kaubanduse kohta siseturul (direktiiv elektroonilise kaubanduse kohta), EÜT L 178, 17.7.2000, lk 1–16.

16 Vt Ettepanek: Euroopa Parlamendi ja nõukogu määrus, mis käsitleb digiteenuste ühtset turgu (digiteenuste õigusakt) ja millega muudetakse direktiivi 2000/31/EÜ, COM(2020) 825 final.

17 Komisjoni teatis „Euroopa digituleviku kujundamine“, COM(2020) 67 final.

18 Digikompass 2030: Euroopa tee digikümnendil.

19 Ettepanek võtta vastu määrus Euroopa andmehalduse kohta (andmehaldust käsitlev õigusakt) COM(2020) 767.

20 Euroopa Parlamendi ja nõukogu 20. juuni 2019. aasta direktiiv (EL) 2019/1024 avaandmete ja avaliku sektori valduses oleva teabe taaskasutamise kohta, PE/28/2019/REV/1, ELT L 172, 26.6.2019, lk 56–83.

21 Komisjoni teatis „Euroopa andmestrateegia“, COM(2020) 66 final.

millega luuakse usaldusväärsed mehhanismid ja teenused selliste andmete taaskasutamiseks, jagamiseks ja koondamiseks, mis on hädavajalikud kvaliteetsete andmepõhiste tehisintellektimudelite arendamiseks.

Ettepanek tugevdab märkimisväärselt liidu rolli, et aidata kujundada ülemaailmseid norme ja standardeid ning soodustada usaldusväärset tehisintellekti, mis on kooskõlas liidu väärtuste ja huvidega. See annab liidule kindla lähtekoha, et suhelda rohkem oma välispartneritega, sealhulgas kolmandate riikidega, ja osaleda rohkem tehisintellektiga seotud küsimusi käsitlevatel rahvusvahelistel foorumitel.

2. ÕIGUSLIK ALUS, SUBSIDIAARSUS JA PROPORTSIONAALSUS

2.1. Õiguslik alus

Ettepaneku õiguslik alus on Euroopa Liidu toimimise lepingu artikkel 114, milles on ette nähtud meetmete võtmine, et tagada siseturu loomine ja toimimine.

Käesolev ettepanek on ELi digitaalse ühtse turu strateegia keskne osa. Ettepaneku peamine eesmärk on tagada siseturu nõuetekohane toimimine, sätestades harmoneeritud eeskirjad eelkõige tehisintellektitehnoloogiat kasutavate või eraldiseisvate tehisintellektisüsteemidena pakutavate toodete ja teenuste arendamise, liidu turule laskmise ja kasutamise kohta. Mõned liikmesriigid kaaluvad juba riiklike eeskirjade kehtestamist, et tagada tehisintellekti ohutus ning arendamine ja kasutamine kooskõlas põhiõigustega seotud kohustustega. See toob tõenäoliselt kaasa kaks peamist probleemi: i) siseturg killustub olemuslikes aspektides, eelkõige seoses tehisintellektitoodetele ja -teenustele esitatavate nõuete, nende turundamise, kasutamise, vastutuse ja ametiasutuste poolse järelevalvega, ning ii) märkimisväärselt väheneb nii tehisintellektisüsteemide pakkujate kui ka kasutajate õiguskindlus seoses sellega, kuidas kohaldatakse liidus nende süsteemide suhtes olemasolevaid ja uusi eeskirju. Arvestades toodete ja teenuste laialdast piiriülest ringlust, saab need kaks probleemi kõige paremini lahendada ühtlustavate ELi õigusaktidega.

Selleks määratletakse ettepanekus ühised kohustuslikud nõuded, mida kohaldatakse teatavate tehisintellektisüsteemide projekteerimisele ja arendamisele enne nende turule laskmist ning mille toimivust suurendatakse veelgi harmoneeritud tehniliste standarditega. Ettepanekus käsitletakse ka tehisintellektisüsteemide turule laskmise järgset olukorda, harmoneerides järelkontrolli tegemise viisid.

Arvestades, et käesolevas ettepanekus on teatavaid erieeskirju üksikisikute kaitse kohta isikuandmete töötlemisel, nimelt piirangud tehisintellektisüsteemide kasutamisele õiguskaitse eesmärgil reaalajas toimuvaks biomeetriliseks kaugtuvastamiseks avalikult juurdepääsetavates ruumides, on asjakohane võtta seoses nende erieeskirjadega määruse aluseks ka ELi toimimise lepingu artikkel 16.

2.2. Subsidiaarsus (ainupädevusse mittekuuluva valdkonna puhul)

Tehisintellekt tugineb sageli suurtele ja mitmekesistele andmekogumitele ning selle võib sisse ehitada siseturul vabalt ringlevasse mis tahes tootesse või teenusesse, mistõttu liikmesriigid üksi ei saa käesoleva ettepaneku eesmärke tõhusalt täita. Lisaks takistab lahkneda võivate riiklike eeskirjade segu tehisintellektisüsteemidega seotud toodete ja teenuste vaba ringlust ELis ega suuda eri liikmesriikides tõhusalt tagada ohutust ega põhiõiguste ja liidu väärtuste kaitset. Probleemide riiklik lahendamine tekitaks ainult täiendavat õiguskindlusetust ja takistusi ning aeglustaks tehisintellekti levikut turul.

Käesoleva ettepaneku eesmärke on parem täita liidu tasandil, et vältida ühtse turu edasist killustumist potentsiaalselt vastuolulisteks riiklikeks raamistikeks, mis takistavad sisse

ehitatud tehisintellektiga toodete ja teenuste vaba ringlust. Usaldusväärset tehisintellekti reguleeriv kindel Euroopa raamistik tagab ka võrdsed võimalused ja kaitseb kõiki inimesi, tugevdades ühtlasi Euroopa tehisintellekti valdkonna konkurentsivõimet ja tööstusbaasi. Vaid liidu tasandi ühismeetmetega on võimalik kaitsta liidu digitaalset suveräänsust ning kasutada ära selle vahendeid ja regulatiivvolitusi ülemaailmsete eeskirjade ja standardite kujundamiseks.

2.3. Proportsionaalsus

Ettepanek tugineb olemasolevatele õigusraamistikele ja on proportsionaalne ja vajalik eesmärkide täitmiseks, sest järgib riskipõhist lähenemisviisi ning sellega kehtestatakse regulatiivne koormus vaid siis, kui tehisintellektisüsteem põhjustab tõenäoliselt suuri riske põhiõigustele ja ohutusele. Muudele kui suure riskiga tehisintellektisüsteemidele kehtestatakse ainult väga piiratud läbipaistvuskohustused, näiteks kohustus jagada teavet, et märgistada tehisintellektisüsteemi kasutamine inimestega suhtlemisel. Suure riskiga tehisintellektisüsteemide puhul on nõuded kvaliteetsete andmete, dokumentatsiooni, jälgitavuse, läbipaistvuse, inimjärelevalve, täpsuse ja stabiilsuse kohta rangelt vajalikud, et viia miinimumini tehisintellektist tingitud riskid põhiõigustele ja ohutusele ning riskid, mida ei kata muud olemasolevad õigusraamistikud. Harmoneeritud standardid, lisasuunised ja nõuete täitmise abivahendid aitavad pakkujatel ja kasutajatel järgida ettepanekuga sätestatud nõudeid ja vähendada kulusid. Operaatoritele tekkivad kulud vastavad täidetavatele eesmärkidele ning majanduslikule ja mainega seotud kasule, mida operaatorid võivad sellest ettepanekust eeldada.

2.4. Vahendi valik

Määruse valimist õiguslikuks vahendiks põhjendab uute eeskirjade ühetaolise kohaldamise vajalikkus, näiteks seoses tehisintellekti määratluse, teatavate kahjulike tehisintellekti võimaldatavate tavade keelu ja teatavate tehisintellektisüsteemide liigitamisega. ELi toimimise lepingu artiklist 288 tulenev määruse vahetu kohaldatavus vähendab õiguslikku killustatust ja soodustab seaduslike, ohutute ja usaldusväärsete tehisintellektisüsteemide ühtse turu väljatöötamist. Selleks kehtestatakse eelkõige harmoneeritud põhinõuded suure riskiga tehisintellektisüsteemidele ja kohustused nende süsteemide pakkujatele ja kasutajatele, et suurendada põhiõiguste kaitset ning tagada nii operaatoritele kui ka tarbijatele õiguskindlus.

Samal ajal ei ole määruse sätted liiga piiravad ja jätavad liikmesriikidele ruumi võtta eri tasandi meetmeid elementide puhul, mis ei kahjusta algatuse eesmärke, näiteks turujärelevalve süsteemi sisekorraldus ja innovatsiooni soodustavate meetmete kasutuselevõtt.

3. JÄRELHINDAMISE, SIDUSRÜHMADEGA KONSULTEERIMISE JA MÕJU HINDAMISE TULEMUSED

3.1. Konsulteerimine sidusrühmadega

Käesoleva ettepaneku koostamiseks konsulteeriti ulatuslikult kõigi peamiste sidusrühmadega ja selles kohaldas komisjon huvitatud pooltega konsulteerimise üldisi põhimõtteid ja miinimumnõudeid.

Koos tehisintellekti käsitleva valge raamatu avaldamisega algatati 19. veebruaril 2020 **avalik veebikonsultatsioon**, mis kestis kuni 14. juunini 2020. Konsultatsiooni eesmärk oli koguda valge raamatu kohta seisukohti ja arvamusi. Konsultatsioon oli mõeldud kõigile avaliku ja erasektori huvitatud sidusrühmadele, sealhulgas valitsused, kohalikud ametiasutused, kaubanduslikud ja mittekaubanduslikud organisatsioonid, sotsiaalpartnerid, eksperdid,

akadeemikud ja kodanikud. Pärast kõikide saadud vastuste analüüsimist avaldas komisjon tulemuste kokkuvõtte ja individuaalsed vastused oma veebisaidil[22].

Kokku saadi 1215 vastust, millest 352 esitasid ettevõtjad või äriorganisatsioonid / ettevõtjate ühendused, 406 üksikisikud (92 % ELi üksikisikud), 152 esitati akadeemiliste/teadusasutuste nimel ja 73 esitasid avalikud asutused. Kodanikuühiskonna häält esindas 160 vastajat (kellest 9 olid tarbijaorganisatsioonid, 129 valitsusvälised organisatsioonid ja 22 ametiühingud); 72 olid „muud“ vastajad. 352 ettevõtluse ja tööstuse esindajast olid 222 ettevõtete ja äriringkondade esindajad, kellest 41,5 % olid mikro-, väikesed ja keskmise suurusega ettevõtjad. Ülejäänud olid ettevõtjate ühendused. ELi 27 riigist saadi kokku 84 % ettevõtjate ja tööstuse vastustest. Olenevalt küsimusest kasutas 81–598 vastajat märkuste sisestamiseks vaba teksti võimalust. EU Survey veebisaidi kaudu esitati üle 450 seisukohti käsitleva dokumendi kas lisaks küsimustiku vastustele (üle 400) või eraldiseisva panusena (üle 50).

Sidusrühmad on üldiselt ühel nõul meetmete vajalikkuses. Valdav enamus sidusrühmi nõustub, et esineb seaduslünki või et vaja on uusi õigusakte. Samas hoiatavad mitu sidusrühma komisjoni, et vältida tuleb dubleerimist, vastuolus olevaid kohustusi ja ülereguleerimist. Paljudes märkustes rõhutati, et tähtis on tehnoloogianeutraalne ja proportsionaalne reguleeriv raamistik.

Sidusrühmad nõudsid enamasti kitsast, selget ja täpset tehisintellekti määratlust. Sidusrühmad rõhutasid ka, et peale termini „tehisintellekt“ täpsustamist on tähtis määratleda „risk“, „suure riskiga“, „väikese riskiga“, „biomeetriline kaugtuvastus“ ja „kahju“.

Enamik vastajaid pooldab sõnaselgelt riskipõhist lähenemisviisi. Riskipõhise raamistiku kasutamist peeti paremaks variandiks kui kõigi tehisintellektisüsteemide üldist reguleerimist. Riskide ja ohtude liigid peaksid põhinema sektori- ja üksikjuhtumipõhisel lähenemisviisil. Riskide arvutamisel tuleks samuti arvesse võtta mõju õigustele ja ohutusele.

Regulatsiooni testkeskkonnad võivad olla tehisintellekti soodustamiseks väga kasulikud ja teatavad sidusrühmad, eriti ettevõtjate ühendused on väljendanud nende üle heameelt.

Nende hulgas, kes sõnastasid oma arvamuse täitmise tagamise mudelite kohta, pooldas enam kui 50 % suure riskiga tehisintellektisüsteemide puhul riskide eelhindamise ja hilisema täitmise tagamise kombinatsiooni, eriti ettevõtjate ühenduste liikmed.

3.2. Eksperdiarvamuste kogumine ja kasutamine

Ettepanek tugineb kahe aasta jooksul tehtud analüüsidele ja selle koostamisel on tihedat koostööd tehtud sidusrühmade, sealhulgas akadeemikute, ettevõtjate, sotsiaalpartnerite, valitsusväliste organisatsioonide, liikmesriikide ja kodanikega. Ettevalmistustöö algas 2018. aastal, kui loodi **tehisintellekti kõrgetasemeline eksperdirühm**, millel oli kaasav ja mitmekesine koosseis, s.o 52 hästi tuntud eksperti, kelle ülesanne oli anda komisjonile nõu tema tehisintellekti strateegia rakendamise kohta. Komisjon toetas[23] 2019. aasta aprillis eksperdirühma usaldusväärset tehisintellekti käsitlevates eetikasuunistes[24] sätestatud põhinõudeid, mida oli muudetud, et võtta arvesse sidusrühmade enam kui 500 vastust. Põhinõuetes kajastub laialt levinud ja tavaline lähenemisviis, et tehisintellekti arendamisel ja kasutamisel tuleks lähtuda teatavatest väärtustest kantud olulistest põhimõtetest. Selline lähenemisviis ilmneb paljude Euroopa ja muu maailma era- ja avaliku sektori organisatsioonide väljatöötatud paljudest eetikakoodeksitest ja -põhimõtetest. Need nõuded

22 Kõik konsultatsiooni tulemused asuvad siin.

23 Euroopa Komisjon, *„Usalduse loomine inimkeskse tehisintellekti vastu“*, COM(2019) 168.

24 Kõrgetasemeline eksperdirühm, *„Ethics Guidelines for Trustworthy AI“* (Eetikasuunised usaldusväärse tehisintellekti arendamiseks), 2019.

muudeti toimivaks usaldusväärse tehisintellekti kontrollnimekirjaga[25] katseprotsessis, milles osales üle 350 organisatsiooni.

Lisaks loodi **tehisintellekti allianss**[26] kui platvorm, kus ligikaudu 4000 sidusrühma saavad arutada tehisintellekti tehnoloogilise ja sotsiaalse mõju üle ning mille haripunkt igal aastal on tehisintellekti käsitlev assamblee.

Seda kaasavat lähenemisviisi arendati edasi tehisintellekti käsitlevas **valges raamatus**, mis ajendas enam kui 1250 sidusrühma esitama märkusi, sealhulgas üle 450 täiendava seisukohti käsitleva dokumendi. Selle tulemusel avaldas komisjon esialgse mõjuhinnangu, mille kohta esitati omakorda üle 130 märkuse[27]. Korraldati **täiendavaid sidusrühmade seminare ja muid üritusi**, mille tulemused toetavad mõjuhinnangu analüüsi ja käesolevas ettepanekus valitud poliitikavariante[28]. Telliti ka **välisuuring**, mille tulemused kaasati mõjuhinnangusse.

3.3. Mõjuhinnang

Komisjon korraldas kooskõlas parema õigusloome poliitikaga käesoleva ettepaneku mõju hindamise, mille vaatas läbi komisjoni õiguskontrollikomitee. Õiguskontrollikomiteega kohtuti 16. detsembril 2020 ja sellele järgnes negatiivne arvamus. Kui mõjuhinnangut oli märkuste arvesse võtmiseks põhjalikult muudetud ja see uuesti esitatud, andis õiguskontrollikomitee 21. märtsil 2021 positiivse arvamuse. Õiguskontrollikomitee arvamused, soovitused ja selgitused selle kohta, kuidas soovitusi on arvesse võetud, on esitatud mõjuhinnangu 1. lisas.

Komisjon vaatas läbi erinevad poliitikavariandid, et täita ettepaneku üldine eesmärk, mis on **tagada ühtse turu nõuetekohane toimimine**, luues tingimused usaldusväärse tehisintellekti arendamiseks ja kasutamiseks liidus.

Hinnati nelja erineval tasemel regulatiivse sekkumisega poliitikavarianti:

- **variant 1**: ELi õigusakt, millega luuakse vabatahtlik märgistuskord;
- **variant 2**: ajutine valdkondlik lähenemisviis;
- **variant 3**: proportsionaalse riskipõhise lähenemisviisiga horisontaalne ELi õigusakt;
- **variant 3+**: proportsionaalse riskipõhise lähenemisviisiga horisontaalne ELi õigusakt + tegevusjuhendid muu kui suure riskiga tehisintellektisüsteemide kohta;
- **variant 4**: horisontaalne ELi õigusakt, millega kehtestatakse kohustuslikud nõuded kõigile tehisintellektisüsteemidele, olenemata nende riskitasemest.

Komisjoni kehtestatud metoodika järgi hinnati iga poliitikavarianti, lähtudes majanduslikust ja sotsiaalsest mõjust ning keskendudes eelkõige põhiõigustele avaldatavale mõjule. Eelistatud on variant 3+ ehk ainult suure riskiga tehisintellektisüsteeme reguleeriv raamistik koos kõigi muu kui suure riskiga tehisintellektisüsteemide pakkujate võimalusega järgida tegevusjuhendeid. Nõuded puudutavad andmeid, dokumentatsiooni ja jälgitavust, teabe

---

25 Kõrgetasemeline eksperdirühm, *„Assessment List for Trustworthy Artificial Intelligence (ALTAI) for self-assessment“* (Usaldusväärse tehisintellekti hindamise kontrollnimekiri), 2020.

26 Tehisintellekti allianss on 2018. aasta juunis loodud mitut sidusrühma hõlmav foorum, https://ec.europa.eu/digital-single-market/en/european-ai-alliance.

27 Euroopa Komisjon, *Esialgne mõjuhinnang ettepaneku kohta võtta vastu Euroopa Parlamendi ja nõukogu õigusakt, millega kehtestatakse nõuded tehisintellektile.*

28 Kõigi toimunud konsultatsioonide üksikasjad on esitatud mõjuhinnangu 2. lisas.

jagamist ja läbipaistvust, inimjärelevalvet ning stabiilsust ja täpsust ja need oleksid kohustuslikud suure riskiga tehisintellektisüsteemide puhul. Teiste tehisintellektisüsteemidega seotud tegevusjuhendeid kehtestavad ettevõtjad teeksid seda vabatahtlikult.

Eelistatud varianti peeti kõige tõhusamaks käesoleva ettepaneku eesmärkide täitmiseks. Eelistatud variant eeldab tehisintellekti arendajatelt ja kasutajatelt piiratud, kuid tõhusaid meetmeid ja vähendab seega inimeste põhiõiguste ja ohutuse rikkumise riske ning soodustab tõhusat järelevalvet ja täitmise tagamist, sest nõudeid peavad täitma vaid süsteemid, mille puhul on selliste rikkumiste esinemise oht suur. Nii hoitakse selle variandiga vastavuskulud võimalikult väikesed ja välditakse kõrgematest hindadest ja vastavuskuludest tulenevat kasutuselevõtu ebavajalikku aeglustumist. Selleks et see variant ei oleks VKEdele ebasoodne, hõlmab see mitut vahendit nende nõuetele vastavuse toetamiseks ja kulude vähendamiseks, sealhulgas regulatsiooni testkeskkondade loomine ja kohustus võtta arvesse VKEde huve vastavushindamisega seotud tasude määramisel.

Eelistatud variant suurendab inimeste usaldust tehisintellekti vastu, suureneb ettevõtjate õiguskindlus ja liikmesriigid ei pea põhjendatuks ühepoolseid meetmeid, mis võivad killustada ühtset turgu. Tehisintellekti ühtne turg kasvab tõenäoliselt jõudsalt, sest tänu usaldusväärsuse kasvule suureneb nõudlus, tänu õiguskindlusele on rohkem pakkumisi ja puuduvad takistused tehisintellektisüsteemide piiriülesele liikuvusele. Euroopa Liit jätkab tehisintellektitehnoloogiat või eraldiseisvaid tehisintellektisüsteeme sisaldavate uuenduslike teenuste ja toodete kiiresti kasvava ökosüsteemi arendamist, mis suurendab digitaalset sõltumatust.

Ettevõtjad või ametiasutused, kes arendavad või kasutavad tehisintellektirakendusi, mis hõlmavad suurt riski kodanike ohutusele või põhiõigustele, peaksid järgima erinõudeid ja -kohustusi. Nende nõuete täitmine tähendaks ligikaudu 6 000–7 000 euro suuruseid kulusid umbes 170 000 eurose keskmise suure riskiga tehisintellektisüsteemi pakkumiseks 2025. aastaks. Tehisintellekti kasutajatele tekiks asjakohasel juhul ka iga-aastane kulu inimjärelevalve tagamiseks kulutatud aja eest, olenevalt kasutusmallist. See on hinnanguliselt ligikaudu 5 000–8 000 eurot aastas. Suure riskiga tehisintellekti pakkujate vastavuskulud võivad olla veel täiendavad 3 000–7 500 eurot. Ettevõtjatel või ametiasutustel, kes arendavad või kasutavad tehisintellektirakendusi, mis ei ole liigitatud suure riskiga rakendusteks, oleksid ainult minimaalsed teavitamiskohustused. Küll aga võivad nad teistega liituda ja võtta ühiselt vastu tegevusjuhendi, et täita sobivad nõuded ja tagada, et nende tehisintellektisüsteemid on usaldusväärsed. Sellisel juhul oleksid kulud kuni sama suured kui suure riskiga tehisintellektisüsteemide puhul, kuid tõenäoliselt väiksemad.

Poliitikavariantide mõju eri sidusrühmade kategooriatele (majandustegevuses osalejad / ettevõtjad; vastavushindamisasutused, standardiorganisatsioonid ja muud avalik-õiguslikud organid; üksikisikud/kodanikud; teadurid) selgitatakse üksikasjalikult käesolevat ettepanekut toetava mõjuhinnangu 3. lisas.

3.4. Õigusnormide toimivus ja lihtsustamine

Käesolevas ettepanekus on sätestatud suure riskiga tehisintellektisüsteemide pakkujatele ja kasutajatele kohaldatavad kohustused. Selliseid süsteeme arendavatele ja liidu turule laskvatele pakkujatele tekitab see õiguskindluse ja tagab, et tehisintellektiga seotud teenuste ja toodete piiriülesel pakkumisel ei esine takistusi. See suurendab tehisintellekti kasutavate ettevõtjate usaldusväärsust nende klientide silmis. Riikide haldusasutuste seisukohast suurendab see üldsuse usaldust tehisintellekti kasutamise vastu ja tugevdab jõustamismehhanisme (kehtestades Euroopa koordineerimismehhanismi, tagades asjakohase suutlikkuse ja hõlbustades tehisintellektisüsteemide auditeerimist uute dokumenteerimis-, jälgitavus- ja läbipaistvusnõuete alusel). Raamistikus nähakse ette ka konkreetsed

innovatsiooni toetavad meetmed, sealhulgas regulatsiooni testkeskkonnad ja erimeetmed, mis aitavad suure riskiga tehisintellektisüsteemide väikekasutajatel ja pakkujatel järgida uusi eeskirju.

Ettepaneku üks eesmärke on tugevdada Euroopa tehisintellekti valdkonna konkurentsivõimet ja tööstusbaasi. Tagatakse täielik järjepidevus olemasolevate tehisintellektisüsteemidele (näiteks toodetele ja teenustele) kohaldatavate valdkondlike liidu õigusaktidega, mis suurendab selgust ja lihtsustab uute eeskirjade täitmise tagamist.

3.5. Põhiõigused

Eriomadustega (näiteks läbipaistmatus, keerukus, sõltuvus andmetest, autonoomne tegutsemine) tehisintellekti kasutamine võib negatiivselt mõjutada ELi põhiõiguste hartas (edaspidi „harta“) sätestatud mitme põhiõiguse kasutamist. Käesoleva ettepanekuga püütakse tagada nende põhiõiguste kaitse kõrge tase ja käsitleda mitut riskiallikat selgesti määratletud riskipõhise lähenemisviisi abil. Kõigile väärtusahela osalejatele kohaldatavate usaldusväärset tehisintellekti käsitlevate nõuete ja proportsionaalsete kohustustega suurendab ettepanek hartaga kaitstavate õiguste kaitset: õigus inimväärikusele (artikkel 1), eraelu austamisele ja isikuandmete kaitsele (artiklid 7 ja 8), diskrimineerimiskeeld (artikkel 21) ning naiste ja meeste võrdõiguslikkus (artikkel 23). Selle eesmärk on vältida heidutavat mõju sõnavabadusele (artikkel 11) ja kogunemisvabadusele (artikkel 12), tagada õigus tõhusale õiguskaitsevahendile ja õiglasele kohtulikule arutamisele, kaitseõigus ja süütuse presumptsioon (artiklid 47 ja 48) ning üldine hea halduse põhimõte. Teatavates valdkondades kohaldatavana mõjutab ettepanek positiivselt mitme rühma õigusi, nagu töötajate õigused headele ja õiglastele töötingimustele (artikkel 31), tarbijakaitse kõrge tase (artikkel 28), lapse õigused (artikkel 24) ning puuetega inimeste integreerimine ühiskonda (artikkel 26). Tähtis on ka õigus kõrgetasemelisele keskkonnakaitsele ja keskkonna kvaliteedi parandamisele (artikkel 37), sealhulgas seoses inimeste tervise ja ohutusega. Teiste põhiõiguste austamisele aitavad kaasa eelkontrolli, riskijuhtimise ja inimjärelevalve kohustused, millega viiakse miinimumini ekslike või erapoolikute tehisintellektipõhiste otsuste tegemise risk elutähtsates valdkondades, nagu haridus ja koolitus, tööhõive, tähtsad teenused, õiguskaitse ja kohtuvõim. Kui põhiõiguste rikkumisi ikkagi esineb, tehakse kahju kandnud isikutele kättesaadavaks tõhus õiguskaitse, tagades tehisintellektisüsteemide läbipaistvuse ja jälgitavuse koos range järelkontrolliga.

Ettepanekuga kehtestatakse teatavad piirangud ettevõtlusvabadusele (artikkel 16) ja kunsti ja teaduse vabadusele (artikkel 13), et tagada suure riskiga tehisintellektitehnoloogia arendamisel ja kasutamisel kooskõla ülekaaluka avaliku huviga seotud põhjustega, nagu tervis, ohutus, tarbijakaitse ja muude põhiõiguste kaitse (vastutustundlik innovatsioon). Tegemist on proportsionaalsete ja minimaalselt vajalike piirangutega, et takistada ja leevendada suuri ohutusriske ning põhiõiguste tõenäolisi rikkumisi.

Suurendatud läbipaistvuskohustused ei mõjuta ebaproportsionaalselt õigust intellektuaalomandi kaitsele (artikli 17 lõige 2), sest piirdutakse ainult minimaalselt vajaliku teabega, et üksikisikud saaksid kasutada tõhusa õiguskaitse õigust, ning järelevalve- ja täitevasutuste vajaliku läbipaistvusega kooskõlas nende volitustega. Teavet avalikustatakse kooskõlas valdkonna asjakohaste õigusaktidega, sealhulgas direktiiviga (EL) 2016/943, milles käsitletakse avalikustamata oskusteabe ja äriteabe (ärisaladuste) ebaseadusliku omandamise, kasutamise ja avalikustamise vastast kaitset. Kui ametiasutustele ja teavitatud asutustele tuleb anda juurdepääs konfidentsiaalsele teabele või lähtekoodile, et uurida oluliste kohustuste järgimist, kehtestatakse neile siduvad konfidentsiaalsuskohustused.

4. MÕJU EELARVELE

Liikmesriigid peavad määrama järelevalveasutused, mis juhivad õigusnõuete rakendamist. Järelevalvefunktsiooni täites võiksid nad tugineda olemasolevale korrale, näiteks vastavushindamisasutuste või turujärelevalve korrale, kuid vajaksid piisavat tehnoloogilist oskusteavet, inimressursse ja rahalisi vahendeid. Olenevalt igas liikmesriigis eelnevalt olemasolevast struktuurist võiks see olla 1–25 täistööaja ekvivalenti liikmesriigi kohta.

Üksikasjalik ülevaade kaasnevatest kuludest on esitatud käesoleva ettepanekuga seotud finantsselgituses.

5. MUU TEAVE

5.1. Rakenduskavad ning järelevalve, hindamise ja aruandluse kord

Selleks et ettepanekuga selle erieesmärgid tõhusalt täita, on hädavajalik ette näha kindel seire- ja hindamismehhanism. Ettepaneku mõju jälgimise eest vastutab komisjon. Komisjon loob süsteemi suure riskiga eraldiseisvate tehisintellektirakenduste registreerimiseks avalikku ELi andmebaasi. Registreerimine võimaldab pädevatel asutustel, kasutajatel ja teistel huvitatud isikutel kontrollida, kas suure riskiga tehisintellektisüsteem vastab ettepanekus sätestatud nõuetele, ning neid põhiõigustele suurt riski kujutavaid tehisintellektisüsteeme paremini jälgida. Andmebaasi täitmiseks peavad tehisintellekti pakkujad esitama olulist teavet oma süsteemide kohta ja nende süsteemide puhul tehtud vastavushindamise kohta.

Lisaks peavad tehisintellekti pakkujad teavitama riikide pädevaid asutusi põhiõigustega seotud kohustuste rikkumist tähendavatest tõsistest intsidentidest või riketest niipea, kui nad saavad nendest teadlikuks, ning tehisintellektisüsteemide tagasikutsumisest või turult kõrvaldamisest. Seejärel uurivad riikide pädevad asutused intsidenti või riket, koguvad kogu vajaliku teabe ja edastavad selle korrapäraselt komisjonile koos asjakohaste metaandmetega. Komisjon täiendab seda intsidenditeavet tehisintellektituru põhjaliku analüüsiga.

Komisjon avaldab aruande, milles hinnatakse välja pakutud tehisintellektiraamistikku ja vaadatakse see läbi viis aastat pärast selle kohaldumiskuupäeva.

5.2. Ettepaneku sätete üksikasjalik selgitus

5.2.1. KOHALDAMISALA JA MÕISTED (I JAOTIS)

I jaotises määratletakse määruse reguleerimisese ja tehisintellektisüsteemide turule laskmist, kasutuselevõttu ja kasutamist käsitlevate uute eeskirjade kohaldamisala. Selles esitatakse ka õigusaktis kasutatavad mõisted. Tehisintellektisüsteem tuleks õigusraamistikus määratleda võimalikult tehnoloogianeutraalselt ja tulevikukindlalt, võttes arvesse tehisintellektiga seotud kiireid tehnoloogiaalaseid ja turusuundumusi. Vajaliku õiguskindluse tagamiseks täiendatakse I jaotist I lisaga, milles esitatakse tehisintellekti arendamise lähenemisviiside ja meetodite üksikasjalik loetelu, mida komisjon kohandab kooskõlas uute tehnoloogiaalaste suundumustega. Selgesti määratletakse kogu tehisintellekti väärtusahela peamised osalejad, nagu tehisintellektisüsteemide pakkujad ja kasutajad, s.o võrdsete võimaluste tagamiseks nii avaliku kui ka erasektori ettevõtjad.

5.2.2. TEHISINTELLEKTIGA SEOTUD KEELATUD TAVAD (II JAOTIS)

II jaotises esitatakse keelatud tehisintellekti loetelu. Määruses järgitakse riskipõhist lähenemisviisi, eristades tehisintellekti kasutusviise, mis tekitavad i) vastuvõetamatu riski, ii) suure riski ja iii) väikese või minimaalse riski. II jaotises esitatud keelatud tavade loetelu hõlmab kõiki neid tehisintellektisüsteeme, mille kasutamist peetakse vastuvõetamatuks, sest see on vastuolus liidu väärtustega, näiteks põhiõiguste rikkumise tõttu. Keelatud on tavad,

mille abil on võimalik inimestega märkimisväärselt manipuleerida, kasutades alalävisele tajule suunatud võtteid, või ära kasutada konkreetsete haavatavate rühmade, näiteks laste või puuetega inimeste nõrkusi, et mõjutada oluliselt nende käitumist nii, et see põhjustab tõenäoliselt neile või teistele isikutele vaimset või füüsilist kahju. Muid täiskasvanutega manipuleerivaid või neid ekspluateerivaid tavu, mida tehisintellektisüsteemid võivad soodustada, võib reguleerida olemasolevate andmekaitse-, tarbijakaitse- ja digiteenustealaste õigusaktidega, mis tagavad, et füüsilisi isikuid teavitatakse nõuetekohaselt nende kohta tehtavast profiilianalüüsist või nende käitumist mõjutada võivatest muudest tavadest ning neil on võimalus keelduda nende kasutamisest. Ettepanekuga keelustatakse ametiasutuste kasutatav tehisintellektipõhine sotsiaalne hindamine üldistel eesmärkidel. Keelustatakse ka reaalajas toimuva biomeetrilise kaugtuvastamise süsteemide kasutamine õiguskaitse eesmärgil avalikult juurdepääsetavates ruumides, välja arvatud juhul, kui kohaldatakse teatavaid piiratud erandeid.

5.2.3. SUURE RISKIGA TEHISINTELLEKTISÜSTEEMID (III JAOTIS)

III jaotises esitatakse erieeskirjad tehisintellektisüsteemide kohta, mis põhjustavad suurt riski füüsiliste isikute tervisele ja ohutusele või põhiõigustele. Kooskõlas riskipõhise lähenemisviisiga lubatakse nende suure riskiga tehisintellektisüsteemide kasutamist Euroopa turul, kui on täidetud teatavad kohustuslikud nõuded ja tehtud vastavuse eelhindamine. Suure riskiga tehisintellektisüsteemiks liigitamisel lähtutakse tehisintellektisüsteemi sihtotstarbest kooskõlas olemasolevate tooteohutusalaste õigusaktidega. Seega ei olene suure riskiga süsteemiks liigitamine ainult tehisintellektisüsteemi täidetavast funktsioonist, vaid ka selle süsteemi konkreetsest kasutuseesmärgist ja kasutusviisidest.

III jaotise 1. peatükis sätestatakse liigitamiseeskirjad ja tehakse kindlaks suure riskiga tehisintellektisüsteemide kaks peamist kategooriat:

- tehisintellektisüsteemid, mis on mõeldud kasutamiseks selliste toodete turvakomponendina, mille kohta teeb kolmas isik vastavuse eelhindamise;
- III lisas sõnaselgelt loetletud muud eraldiseisvad tehisintellektisüsteemid, mis mõjutavad peamiselt põhiõigusi.

See III lisas esitatud suure riskiga tehisintellektisüsteemide loetelu sisaldab piiratud arvu tehisintellektisüsteeme, mille riskid on juba ilmnenud või tõenäoliselt ilmnevad lähitulevikus. Selleks et määrust oleks võimalik kohandada uute tehisintellekti kasutusviiside ja tehisintellektirakendustega, võib komisjon pikendada teatavates eelnevalt kindlaks määratud valdkondades kasutatavate suure riskiga tehisintellektisüsteemide loetelu, kohaldades kriteeriumeid ja riskihindamise metoodikat.

2. peatükis sätestatakse suure riskiga tehisintellektisüsteemide suhtes kohaldatavad õiguslikud nõuded seoses andmete ja andmehalduse, andmete dokumenteerimise ja säilitamise, läbipaistvuse ja kasutajatele teabe jagamise, inimjärelevalve, stabiilsuse, täpsuse ja turvalisusega. Paljud hoolsad ettevõtjad juba kasutavad väljapakutud miinimumnõudeid, mis tulenevad kaks aastat kestnud ettevalmistustööst ja kõrgetasemelise eksperdirühma koostatud eetikasuunistest,[29] mille on kasutusele võtnud enam kui 350 organisatsiooni[30]. Need on valdavalt kooskõlas muude rahvusvaheliste soovituste ja põhimõtetega, mis tagab, et väljapakutud tehisintellekti raamistik sobib kokku ELi rahvusvaheliste kaubanduspartnerite vastu võetud raamistikega. Nende nõuete täitmist tagavad täpsed tehnilised lahendused võib

[29] Tehisintellekti kõrgetasemeline eksperdirühm, *„Ethics Guidelines for Trustworthy AI“* (Eetikasuunised usaldusväärse tehisintellekti arendamiseks), 2019.

[30] Need kiitis heaks ka komisjon 2019. aasta teatises inimkeskse tehisintellektikäsituse kohta.

esitada standardites või muudes tehnilistes kirjeldustes või need välja töötada vastavalt tehisintellektisüsteemi pakkuja käsutuses olevatele üldistele tehnika- või teadusalastele teadmistele. Selline paindlikkus on eriti tähtis, sest võimaldab tehisintellektisüsteemide pakkujatel valida neile sobiv nõuete täitmise viis, arvestades valdkonna tipptehnoloogiat ning tehnoloogia ja teaduse arengut.

3. peatükis kehtestatakse suure riskiga tehisintellektisüsteemide pakkujatele selged horisontaalsed kohustused. Proportsionaalsed kohustused kehtestatakse ka kasutajatele ja teistele tehisintellekti väärtusahela osalejatele (näiteks importijad, turustajad, volitatud esindajad).

4. peatükis sätestatakse raamistik teavitatud asutuste kui sõltumatute kolmandate isikute osalemise kohta vastavushindamises ja 5. peatükis selgitatakse üksikasjalikult iga liiki suure riskiga tehisintellektisüsteemi puhul kasutatavat vastavushindamist. Vastavushindamisega soovitakse viia miinimumini majandustegevuses osalejate ja samuti teavitatud asutuste koormus, kelle suutlikkust tuleb aja jooksul järk-järgult suurendada. Uue õigusraamistiku õigusaktidega reguleeritavate toodete (näiteks masinad, mänguasjad, meditsiiniseadmed jne) turvakomponentideks mõeldud tehisintellektisüsteemide suhtes kohalduvad samad vastavuse eel- ja järelhindamise ning täitmise tagamise mehhanismid nagu toodetele, mille osad need on. Peamine erinevus seisneb selles, et eel- ja järelmehhanismid ei taga vastavust üksnes valdkonna õigusaktidega kehtestatud nõuetele, vaid ka käesoleva määrusega kehtestatavatele nõuetele.

III lisas osutatud eraldiseisvatele suure riskiga tehisintellektisüsteemidele kehtestatakse uus vastavus- ja täitmise tagamise süsteem. Sellega järgitakse uue õigusraamistiku õigusaktide mudelit, mida rakendatakse pakkujate sisekontrolli kaudu. Erand on biomeetrilise kaugtuvastamise süsteemid, mille vastavushindamise teeb kolmas isik. Põhjalik vastavuse eelhindamine sisekontrolli kaudu kombineerituna hilisema tugeva täitmise tagamisega võib olla nende süsteemide korral tõhus ja mõistlik lahendus, arvestades varast regulatiivset sekkumist ja asjaolu, et tehisintellektisektor on väga uuenduslik ja auditeerimise oskusteavet kogutakse alles praegu. Eraldiseisvate suure riskiga tehisintellektisüsteemide hindamine sisekontrolli raames eeldaks täieliku, tõhusa ja nõuetekohaselt dokumenteeritud eelhindamisega kinnitatud vastavust kõigile määruse nõuetele koos töökindlate kvaliteedi- ja riskijuhtimissüsteemide ning turustamisjärgse seirega. Kui pakkuja on teinud asjakohase vastavushindamise, peaks ta need eraldiseisvad suure riskiga tehisintellektisüsteemid registreerima komisjoni hallatavas ELi andmebaasis, et suurendada läbipaistvust avalikkuse jaoks ja järelevalvet ning tugevdada pädevate asutuste poolset järelevalvet. Seevastu toodete turvakomponentidena kasutatavate tehisintellektisüsteemide vastavushindamise korral järgitakse kolmanda isiku tehtava vastavushindamise süsteemi, mis on juba kehtestatud asjakohastes tooteohutust käsitlevates valdkondlikes õigusaktides, et tagada järjepidevus nende olemasolevate õigusaktidega. Kui tehisintellektisüsteemides tehakse olulisi muudatusi (ja eelkõige muudatusi, mis lähevad kaugemale pakkuja tehnilises dokumentatsioonis määratust ja vastavuse eelhindamise hetkel kontrollitust), tuleb teha uued vastavuse eelhindamised.

5.2.4. TEATAVATE TEHISINTELLEKTISÜSTEEMIDE KORRAL KOHALDATAVAD LÄBIPAISTVUSKOHUSTUSED (IV JAOTIS)

IV jaotises käsitletakse teatavaid tehisintellektisüsteeme, millega kaasnevad konkreetsed manipuleerimisriskid. Läbipaistvuskohustusi kohaldatakse süsteemidele, i) mis suhtlevad inimestega, ii) mida kasutatakse biomeetriliste andmete põhjal tunnete tuvastamiseks või (sotsiaalsete) kategooriatega seoste kindlaks tegemiseks või iii) mis loovad või muudavad sisu (süvavõltsingud). Inimesi tuleb teavitada sellest, kui nad suhtlevad tehisintellektisüsteemiga

või nende tundeid või omadusi tuvastatakse automatiseeritud vahendite abil. Tuleks kehtestada kohustus, et kui tehisintellektisüsteemi kasutatakse autentse sisuna näiva pildi-, audio- või videosisu loomiseks või muutmiseks, peab teavitama, et sisu on loodud automatiseeritud vahendite abil, kuigi õiguspärastel eesmärkidel võib esineda erandeid (õiguskaitse, väljendusvabadus). See võimaldab inimestel teha teadlikke valikuid või olukorrast väljuda.

5.2.5. INNOVATSIOONI TOETAVAD MEETMED (V JAOTIS)

V jaotis aitab täita eesmärki luua innovatsiooni soodustav, tulevikukindel ja häiretele vastupidav õigusraamistik. Selleks soovitatakse riikide pädevatel asutustel luua regulatsiooni testkeskkonnad ja sätestatakse juhtimise, järelevalve ja vastutuse põhiraamistik. Tehisintellekti regulatsiooni testkeskkonnad on kontrollitud keskkonnad, milles katsetada pädevate asutustega kokku lepitud katseplaani järgi piiratud aja jooksul uuenduslikku tehnoloogiat. V jaotises esitatakse ka VKEde ja idufirmade regulatiivse koormuse vähendamise meetmed.

5.2.6. JUHTIMINE JA RAKENDAMINE (VI, VII JA VIII JAOTIS)

VI jaotises sätestatakse liidu ja riigi tasandi juhtimissüsteemid. Liidu tasandil kehtestatakse ettepanekuga liikmesriikide ja komisjoni esindajatest koosnev Euroopa tehisintellekti nõukoda (edaspidi „nõukoda“). Nõukoda aitab tõhustada riikide järelevalveasutuste ja komisjoni koostööd ning annab komisjonile nõu ja oskusteavet, soodustades sellega käesoleva määruse sujuvat, tõhusat ja harmoneeritud rakendamist. Nõukoda ühtlasi kogub ja jagab liikmesriikidega parimaid tavasid.

Riigi tasandil peavad liikmesriigid määruse kohaldamise ja rakendamise jälgimise eesmärgil nimetama ühe või mitu riiklikku pädevat asutust ning nende hulgast riikliku järelevalveasutuse. Euroopa andmekaitseinspektor tegutseb liidu asutuste, ametite ja organite üle järelevalvet teostava pädeva asutusena, kui need kuuluvad käesoleva määruse kohaldamisalasse.

VII jaotise eesmärk on hõlbustada komisjoni ja riikide ametiasutuste seiretööd, kehtestades peamiselt põhiõigusi mõjutavate eraldiseisvate suure riskiga tehisintellektisüsteemide ELi andmebaasi. Andmebaasi haldab komisjon ja selle andmed pärinevad tehisintellektisüsteemide pakkujatelt, kellelt nõutakse oma süsteemide registreerimist enne nende turule laskmist või muul viisil kasutusele võtmist.

VIII jaotises sätestatakse tehisintellektisüsteemide pakkujate seire- ja aruandekohustused seoses turustamisjärgse seire ja aruandluse ning tehisintellektiga seotud intsidentide ja rikete uurimisega. Turujärelevalveasutused kontrollivad turgu ja uurivad kõigile juba turule lastud suure riskiga tehisintellektisüsteemidele kehtestatud kohustuste ja nõuete täitmist. Turujärelevalveasutustel on kõik turujärelevalvet käsitlevast määrusest (EL) 2019/1020 tulenevad volitused. Hilisema täitmise tagamisega tuleks kindlustada, et kui tehisintellektisüsteem on turule lastud, on ametiasutustel olemas sekkumiseks vajalikud volitused ja vahendid, juhuks kui tehisintellektisüsteemid tekitavad kiiret tegutsemist nõudvaid ootamatuid riske. Nad jälgivad ka seda, kas operaatorid täidavad neile määrusega kehtestatud asjakohaseid kohustusi. Ettepanekus ei nähta ette liikmesriigi tasandi täiendavate organite ega asutuste automaatset loomist. Seepärast võivad liikmesriigid nimetada olemasolevaid valdkonna ametiasutusi (ja kasutada nende oskusteavet), usaldades neile ka määruse täitmise järelevalve ja tagamise volitused.

Miski eespool kirjeldatust ei piira kehtiva süsteemi kohaldamist ega liikmesriikides kehtivate põhiõigustega seotud kohustuste hilisema täitmise tagamise volituste jaotamist. Kui see on tähtis olemasolevate järelevalve- ja täitevasutuste volituste täitmiseks, on neil ka volitus

taotleda käesoleva määruse alusel säilitatavat dokumentatsiooni ja sellega tutvuda ning vajaduse korral taotleda turujärelevalveasutustelt suure riskiga tehisintellektisüsteemi katsetamise korraldamist tehniliste vahendite abil.

5.2.7. TEGEVUSJUHENDID (IX JAOTIS)

IX jaotises luuakse tegevusjuhendite koostamise raamistik. Tegevusjuhendite eesmärk on julgustada muu kui suure riskiga tehisintellektisüsteemide pakkujaid vabatahtlikult kohaldama suure riskiga tehisintellektisüsteemidele kohustuslikke nõudeid (vastavalt III jaotisele). Muu kui suure riskiga tehisintellektisüsteemide pakkujad võivad tegevusjuhendeid ise koostada ja rakendada. Need juhendid võivad hõlmata ka vabatahtlikult võetavaid kohustusi, mis võivad olla seotud näiteks keskkonnasäästlikkusega, puuetega inimeste juurdepääsuga, sidusrühmade osalemisega tehisintellektisüsteemide projekteerimises ja arendamises ning arendustiimide mitmekesisusega.

5.2.8. LÕPPSÄTTED (X, XI ja XII JAOTIS)

X jaotises toonitatakse kõigi poolte kohustust austada teabe ja andmete konfidentsiaalsust ning sätestatakse eeskirjad määruse rakendamisel hangitava teabe vahetamiseks. X jaotis sisaldab ka meetmeid, millega tagada määruse tõhus rakendamine selle normide rikkumise eest määratavate tõhusate, proportsionaalsete ja heidutavate karistustega.

XI jaotises sätestatakse delegeerimis- ja rakendusvolituste kasutamise eeskirjad. Ettepanek annab komisjonile õiguse võtta asjakohasel juhul vastu rakendusakte määruse ühetaolise kohaldamise tagamiseks või delegeeritud õigusakte I–VII lisa loetelude ajakohastamiseks või täiendamiseks.

XII jaotises kehtestatakse komisjonile kohustus hinnata korrapäraselt III lisa ajakohastamise vajadust ja koostada korrapäraselt määruse hindamise ja läbivaatamise aruandeid. Lisaks esitatakse selles lõppsätted, sealhulgas diferentseeritud üleminekuperiood määruse esialgse kohaldamise kuupäevani, et hõlbustada kõigi asjaomaste poolte jaoks sujuvat rakendamist.

2021/0106 (COD)

Ettepanek:

EUROOPA PARLAMENDI JA NÕUKOGU MÄÄRUS,

MILLEGA NÄHAKSE ETTE TEHISINTELLEKTI KÄSITLEVAD ÜHTLUSTATUD ÕIGUSNORMID (TEHISINTELLEKTI KÄSITLEV ÕIGUSAKT) JA MUUDETAKSE TEATAVAID LIIDU ÕIGUSAKTE

EUROOPA PARLAMENT JA EUROOPA LIIDU NÕUKOGU,

võttes arvesse Euroopa Liidu toimimise lepingut, eriti selle artikleid 16 ja 114,

võttes arvesse Euroopa Komisjoni ettepanekut,

olles edastanud seadusandliku akti eelnõu riikide parlamentidele,

võttes arvesse Euroopa Majandus- ja Sotsiaalkomitee arvamust[31],

võttes arvesse Regioonide Komitee arvamust[32],

toimides seadusandliku tavamenetluse kohaselt

ning arvestades järgmist:

(1) Käesoleva määruse eesmärk on parandada siseturu toimimist ühtse õigusraamistiku kehtestamisega eeskätt tehisintellekti arendamise, turustamise ja kasutamise jaoks kooskõlas liidu väärtustega. Käesolev määrus on ajendatud mitmest kaaluka üldise huvi eesmärgist, nagu kõrgetasemeline tervise, ohutuse ja põhiõiguste kaitse, ning sellega tahetakse tagada tehisintellektil põhinevate kaupade ja teenuste vaba piiriülene liikumine, vältides seega liikmesriikide kehtestatavaid piiranguid tehisintellektisüsteemide arendamisele, turustamisele ja kasutamisele, kui selleks pole just käesoleva määrusega antud selget luba.

(2) Tehisintellektisüsteeme on lihtne mitmesugustes majanduse ja ühiskonna sektorites kasutusele võtta, sh piiriüleselt, ning need võivad levida kogu liidus. Teatavad liikmesriigid on juba uurinud võimalust võtta vastu siseriiklikke õigusnorme, et tagada tehisintellekti ohutus ning selle arendamine ja kasutamine koostkõlas põhiõigustega seotud kohustustega. Siseriiklike õigusnormide vahelised erinevused võivad tuua kaasa siseturu killustumise ja vähendada tehisintellektisüsteemide arendamise ja kasutamisega tegelevate operaatorite õiguskindlust. Seepärast tuleks kõikjal liidus tagada kaitse järjekindlus ja kõrge tase ning ühtlasi vältida erinevusi, mis kahjustavad tehisintellektisüsteemide ja nendega seotud toodete ja teenuste vaba ringlust siseturul; selleks tuleks operaatoritele kehtestada ühetaolised kohustused ja kindlustada kaalukate üldiste huvide ja isikute õiguste ühtne kaitse siseturul, lähtudes Euroopa Liidu toimimise lepingu (edaspidi „ELi toimimise leping“) artiklist 114. Kuivõrd käesolev määrus sisaldab konkreetseid õigusnorme, mis puudutavad üksikisikute kaitset seoses isikuandmete töötlemisega ja millega piiratakse tehisintellektisüsteemide kasutamist avalikult juurdepääsetavas ruumis õiguskaitse

[31] ELT C […], […], lk […].
[32] ELT C […], […], lk […].

eesmärgil reaalajas toimuva biomeetrilise kaugtuvastamise jaoks, on asjakohane võtta nende konkreetsete normide puhul käesoleva määruse aluseks ELi toimimise lepingu artikkel 16. Neid konkreetseid õigusnorme ja ELi toimimise lepingu artiklile 16 tuginemist silmas pidades on asjakohane konsulteerida Euroopa Andmekaitsenõukoguga.

(3) Tehisintellekt on kiirelt arenev tehnoloogiaharu, mis võib aidata saavutada mitmesuguseid majanduslikke ja ühiskondlikke hüvesid kõigis tööstusharudes ja ühiskondlikes tegevustes. Tänu täpsemale prognoosimisele, tegevuse ja ressursijaotuse optimeerimisele ning üksikisikutele ja organisatsioonidele kättesaadavate digilahenduste personaliseerimisele võib tehisintellekti kasutamine anda ettevõtjatele olulise konkurentsieelise ning toetada ühiskonna ja keskkonna jaoks positiivsete tulemuste saavutamist näiteks sellistes valdkondades nagu tervishoid, põllumajandus, haridus ja koolitus, taristuhaldus, energeetika, transport ja logistika, avalikud teenused, turvalisus, õigus, ressursi- ja energiatõhusus ning kliimamuutuste leevendamine ja nendega kohanemine.

(4) Samas võib tehisintellekt olenevalt konkreetse rakenduse ja kasutuse asjaoludest tekitada ka riske ning kahjustada avalikke huve ja liidu õigusega kaitstud õigusi. Selline kahju võib olla varaline või mittevaraline.

(5) Seepärast on vaja liidu õigusraamistikku, millega nähtaks ette tehisintellekti käsitlevad ühtlustatud õigusnormid, et edendada siseturul tehisintellekti arendamist, kasutamist ja levikut, mille puhul oleks ühtlasi tagatud liidu õigusega tunnustatud ja kaitstud üldiste huvide, näiteks tervise ja ohutuse ning põhiõiguste kõrgetasemeline kaitse. Selle eesmärgi saavutamiseks tuleks kehtestada teatavate tehisintellektisüsteemide turule laskmist ja kasutusele võtmist reguleerivad õigusnormid, et seeläbi tagada siseturu sujuv toimimine ja võimaldada neil süsteemidel saada kasu kaupade ja teenuste vaba liikumise põhimõttest. Kõnealuste õigusnormide kehtestamisega toetab käesolev määrus Euroopa Ülemkogu sõnastatud liidu eesmärki olla maailmas turvalise, usaldusväärse ja eetilise tehisintellekti arendamisel liidripositsioonil[33] ning samas aitab see tagada eetiliste põhimõtete kaitse, mida on eraldi nõudnud Euroopa Parlament[34].

(6) Õiguskindluse tagamiseks tuleks tehisintellektisüsteemi mõiste selgelt määratleda, kuid samas tuleks säilitada paindlikkus, et jääks ruumi tehnika edasiseks arenguks. Määratlus peaks põhinema tarkvara peamistel funktsionaalsetel omadustel, eeskätt võimel genereerida teatavate inimese poolt kindlaks määratud eesmärkide jaoks väljundeid, näiteks sisu, prognoose, soovitusi või otsuseid, mis mõjutavad keskkonda, millega süsteem suhtleb kas füüsilises või digitaalses plaanis. Tehisintellektisüsteeme saab projekteerida töötama erineval autonoomsuse tasemel ning neid võib kasutada eraldiseisvatena või mõne teise toote komponentidena, olenemata sellest, kas süsteem on füüsiliselt tootesse integreeritud (sisseehitatud) või teenib toote funktsionaalsust ilma, et oleks sellesse integreeritud (sisseehitamata). Tehisintellektisüsteemi määratlust tuleks täiendada selle arendamiseks kasutatavate konkreetsete meetodite ja lähenemisviiside loeteluga, mida tuleks hoida turu ja tehnika arengu seisukohast ajakohasena delegeeritud õigusaktidega, mida komisjon selle loetelu muutmiseks vastu võtab.

---

33 Euroopa Ülemkogu erakorraline kohtumine, 1. ja 2. oktoober 2020, järeldused, EUCO 13/20, 2020, lk 6.

34 Euroopa Parlamendi 20. oktoobri 2020. aasta resolutsioon soovitustega komisjonile tehisintellekti, robootika ja seonduva tehnoloogia eetiliste aspektide raamistiku kohta, 2020/2012(INL).

(7) Käesolevas määruses kasutatav biomeetriliste andmete mõiste on vastavuses biomeetriliste andmete mõistega, mis on määratletud Euroopa Parlamendi ja nõukogu määruse (EL) 2016/679[35] artikli 4 punktis 14, Euroopa Parlamendi ja nõukogu määruse (EL) 2018/1725[36] artikli 3 punktis 18 ja Euroopa Parlamendi ja nõukogu direktiivi (EL) 2016/680[37] artikli 3 punktis 13, ning seda tuleks tõlgendada kooskõlas nende õigusaktidega.

(8) Käesolevas määruses kasutatav biomeetrilise kaugtuvastamise süsteemi mõiste tuleks määratleda funktsioonidest lähtuvalt kui tehisintellektisüsteem, mis on mõeldud füüsiliste isikute eemalt tuvastamiseks, võrreldes isiku biomeetrilisi andmeid võrdlusbaasis sisalduvate biomeetriliste andmetega ning ilma, et oleks ette teada, kas asjaomane isik viibib seal ja kas teda on võimalik tuvastada, olenemata sellest, milliseid konkreetseid tehnoloogiaid ja protseduure või mis liiki biomeetrilisi andmeid selleks kasutatakse. Eristada tuleks nn reaalajas toimuva ja tagantjärele toimuva biomeetrilise kaugtuvastamise süsteeme, sest nende omadused ja kasutusviisid on erinevad ning nendega kaasnevad erinevad riskid. Reaalajas kasutatavate süsteemide puhul toimub biomeetriliste andmete hõive, võrdlemine ja isiku identifitseerimine kõik hetkega, peaaegu hetkega või igal juhul ilma märkimisväärse viivituseta. Siinjuures ei tohiks jääda võimalust hoida väikeste viivituste kasutamisega kõrvale käesoleva määruse sätetest, mis käsitlevad tehisintellektisüsteemi kasutamist reaalajas. Reaalajalistes süsteemides kasutatakse kaamera või muu sarnase funktsiooniga seadmega tehtud otse edastatavat või peaaegu otse edastatavat materjali, näiteks videosalvestisi. Tagantjärele kasutatavate süsteemide puhul on aga biomeetriliste andmete hõive juba toimunud ning võrdlemine ja isikute identifitseerimine toimub alles pärast olulist viivitust. Sealjuures kasutatakse selliseid materjale nagu videovalvesüsteemi või isikliku seadmega tehtud pildid või videosalvestised, mis on tehtud enne, kui süsteemi kasutatakse konkreetse füüsilise isiku puhul.

(9) Käesoleva määruse kohaldamisel tuleks avalikult juurdepääsetava ruumina käsitada mis tahes füüsilist kohta, mis on üldsusele juurdepääsetav, olenemata sellest, kas kõnealune koht on era- või avalik-õiguslikus omandis. Seega ei hõlma see mõiste olemuselt privaatseid kohti, mis ei ole kolmandatele isikutele, sh õiguskaitseasutustele tavaliselt ilma konkreetse kutse või loata vabalt juurdepääsetavad, näiteks inimeste kodusid, eraklubisid, kontoreid, ladusid ja tehaseid. Selle mõiste alla ei käi küberruum, sest see ei ole füüsiline ruum. Üksnes asjaolu, et konkreetsele ruumile juurdepääsuks on kehtestatud teatavad tingimused, näiteks pileti olemasolu või vanusepiirang, ei tähenda, et see ruum ei ole avalikult juurdepääsetav käesoleva määruse tähenduses. Seega peetakse avalikult juurdepääsetavaks ruumiks lisaks avalikule ruumile, nagu tänavad, valitsushoonete asjakohased osad ja suurem osa transporditaristust, tavaliselt ka selliseid ruume nagu kinod, teatrid, poed ja kaubanduskeskused. See, kas

---

35 Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta määrus (EL) 2016/679 füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus) (ELT L 119, 4.5.2016, lk 1).

36 Euroopa Parlamendi ja nõukogu 23. oktoobri 2018. aasta määrus (EL) 2018/1725, mis käsitleb füüsiliste isikute kaitset isikuandmete töötlemisel liidu institutsioonides, organites ja asutustes ning isikuandmete vaba liikumist, ning millega tunnistatakse kehtetuks määrus (EÜ) nr 45/2001 ja otsus nr 1247/2002/EÜ (ELT L 295, 21.11.2018, lk 39).

37 Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta 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 andmete vaba liikumist ning millega tunnistatakse kehtetuks nõukogu raamotsus 2008/977/JSK (õiguskaitsedirektiiv) (ELT L 119, 4.5.2016, lk 89).

konkreetne ruum on avalikult juurdepääsetav, tuleks siiski otsustada igal üksikjuhul eraldi, võttes arvesse vaadeldava olukorra iseärasusi.

(10) Selleks et tagada võrdsed tingimused ning üksikisikute õiguste ja vabaduste tulemuslik kaitse kogu liidus, tuleks käesoleva määrusega kehtestatud õigusnorme kohaldada tehisintellektisüsteemide pakkujate suhtes, diskrimineerimata pakkujaid selle põhjal, kas nad tegutsevad liidus või mõnes kolmandas riigis, ja liidus tegutsevate tehisintellektisüsteemide kasutajate suhtes.

(11) Arvestades tehisintellektisüsteemide digitaalset olemust, peaksid teatavad tehisintellektisüsteemid kuuluma käesoleva määruse kohaldamisalasse isegi siis, kui neid ei ole liidus turule lastud ega kasutusele võetud ja kui neid liidus ei kasutata. See kehtib näiteks siis, kui tegemist on liidus tegutseva operaatoriga, kes sõlmib väljaspool liitu tegutseva operaatoriga lepingu teatavate teenuste kohta, mis on seotud sellise tehisintellektisüsteemi teostatava tegevusega, mis kvalifitseeruks suure riskiga tehisintellektisüsteemiks ja mis mõjutab liidus asuvaid füüsilisi isikuid. Sellisel juhul võib väljaspool liitu asuva operaatori kasutatav tehisintellektisüsteem töödelda andmeid, mis on seaduslikult liidus kogutud ja mida liidust edastatakse, ning anda liidus asuvale lepingu sõlminud operaatorile väljundi, mille see tehisintellektisüsteem kõnealuse töötlemise tulemusena genereeris, ilma et see tehisintellektisüsteem oleks liidus turule lastud, kasutusele võetud või kasutatav. Et hoida ära käesoleva määruse sätetest kõrvalehoidmist ja tagada liidus asuvate füüsiliste isikute tulemuslik kaitse, tuleks käesolevat määrust kohaldada ka tehisintellektisüsteemide kolmandas riigis tegutsevate pakkujate ja kasutajate suhtes niivõrd, kuivõrd nende süsteemide genereeritud väljundit kasutatakse liidus. Võtmaks siiski arvesse olemasolevaid kokkuleppeid ja erivajadusi, mis puudutavad koostööd välispartneritega, kellega vahetatakse teavet ja tõendeid, ei tuleks käesolevat määrust kohaldada kolmanda riigi ametiasutuste ja rahvusvaheliste organisatsioonide suhtes, kui tegutsetakse selliste rahvusvaheliste lepingute alusel, mis on riigi või Euroopa tasandil sõlmitud liidu või selle liikmesriikidega tehtava õiguskaitse- ja õigusalase koostöö kohta. Selliseid lepinguid on sõlmitud kahepoolselt liikmesriikide ja kolmandate riikide vahel, aga ka Euroopa Liidu, Europoli ja muude ELi asutuste ning kolmandate riikide ja rahvusvaheliste organisatsioonide vahel.

(12) Käesolevat määrust tuleks kohaldada ka liidu institutsioonide, organite ja asutuste suhtes, kui need tegutsevad tehisintellektisüsteemi pakkuja või kasutajana. Käesoleva määruse kohaldamisalast tuleks välja jätta tehisintellektisüsteemid, mis on välja töötatud või mida kasutatakse eranditult sõjalisel otstarbel, kui nende kasutamine kuulub Euroopa Liidu leping V jaotise alusel reguleeritava ühise välis- ja julgeolekupoliitika ainupädevusse. Käesolev määrus ei tohiks mõjutada Euroopa Parlamendi ja nõukogu direktiivi 2000/31/EÜ vahendajatest teenuseosutajate vastutust käsitlevate sätete [asendatakse digiteenuste õigusakti vastavate sätetega] kohaldamist.

(13) Selleks et tagada järjekindel ja kõrgetasemeline avalike huvide kaitse tervishoiu, ohutuse ja põhiõiguste vallas, tuleks kõigi suure riskiga tehisintellektisüsteemide jaoks kehtestada ühised normatiivsed standardid. Need standardid peaksid olema kooskõlas Euroopa Liidu põhiõiguste hartaga (edaspidi „põhiõiguste harta“) ning ühtlasi peaksid need olema mittediskrimineerivad ja kooskõlas liidu rahvusvaheliste kaubanduskohustustega.

(14) Selleks et kehtestada tehisintellektisüsteemide suhtes proportsionaalsed, mõjusad ja siduvad õigusnormid, tuleks järgida selgelt määratletud riskipõhist lähenemisviisi. Sellise lähenemisviisi kohaselt tuleks nende õigusnormide liiki ja sisu kujundada

vastavalt tehisintellektisüsteemide põhjustatavate riskide intensiivsusele ja ulatusele. Seepärast tuleb keelata teatavad tehisintellektisüsteemide kasutusviisid, näha ette suure riskiga tehisintellektisüsteemide suhtes kohaldatavad nõuded ja asjaomaste operaatorite kohustused ning kehtestada teatavate tehisintellektisüsteemide puhul läbipaistvuskohustused.

(15) Lisaks sellele, et tehisintellektil on mitmeid kasulikke rakendusvõimalusi, on seda tehnoloogiat võimalik ka kurjasti kasutada ning luua uudseid ja võimsaid manipuleerimise, ärakasutamise ja sotsiaalse kontrolli vahendeid. Sellised kasutusviisid on eriti kahjulikud ning tuleks ära keelata, sest need on vastuolus selliste liidu väärtustega nagu inimväärikuse austamine, vabadust, võrdsus, demokraatia ja õigusriik ning liidu põhiõigustega, kaasa arvatud õigusega mittediskrimineerimisele, andmekaitsele ja privaatsusele, aga ka lapse õigustega.

(16) Keelata tuleks selliste tehisintellektisüsteemide turule laskmine, kasutusele võtmine ja kasutamine, mille eesmärk on moonutada inimeste käitumist ja millega võib tõenäoliselt põhjustada füüsilist või psühholoogilist kahju. Sellistes tehisintellektisüsteemides kasutatakse alalävisele tajule suunatud elemente, mida inimesed ei suuda tajuda, või kasutatakse ära laste haavatavust ja inimeste vanusest või füüsilisest või vaimsest võimetusest tulenevaid nõrku kohti. Selle eesmärk on oluliselt moonutada inimese käitumist viisil, mis kahjustab või tõenäoliselt kahjustab seda või mõnd teist isikut. Sellist eesmärki ei saa eeldada, kui inimese käitumist moonutavad tehisintellektisüsteemivälised tegurid, mis ei ole pakkuja või kasutaja kontrolli all. Selline keeld ei tohiks takistada kõnealuseid tehisintellektisüsteeme käsitlevaid õiguspärastel eesmärkidel tehtavaid teadusuuringuid, kui selliste teadusuuringute puhul pole tegemist tehisintellektisüsteemi kasutamisega inimeste ja masinate vahelistes suhetes viisil, mis seab inimesed ohtu, ning kui selliseid teadusuuringuid tehakse kooskõlas teadusuuringute tunnustatud eetikanormidega.

(17) Tehisintellektisüsteemid, mida kasutatakse avalike võimude poolt või nende nimel füüsiliste isikute üldotstarbeliseks sotsiaalseks hindamiseks, võivad tuua kaasa diskrimineerimise ja teatavate rühmade kõrvalejätmise. Need süsteemid võivad rikkuda õigust väärikusele ja mittediskrimineerimisele ning olla vastuolus võrdsuse ja õigluse väärtustega. Sellised tehisintellektisüsteemid hindavad või liigitavad füüsiliste isikute usaldusväärsust, tuginedes nende sotsiaalsele käitumisele eri kontekstides või prognoositud isiku- või iseloomuomadustele. Selliste tehisintellektisüsteemide antud sotsiaalne hinne võib tuua kaasa füüsilisi isikuid või terveid inimrühmi kahjustavat või nende suhtes ebasoodsat kohtlemist sotsiaalses kontekstis, mis ei ole seotud kontekstiga, kus andmed algselt genereeriti või koguti, või kahjustavat kohtlemist, mis ei ole nende sotsiaalse käitumise problemaatilisusega võrreldes proportsionaalne või põhjendatud. Seepärast peaksid sellised tehisintellektisüsteemid olema keelatud.

(18) Tehisintellektisüsteemide kasutamist avalikult juurdepääsetavas ruumis õiguskaitse eesmärgil reaalajas toimuva füüsiliste isikute biomeetrilise kaugtuvastamise jaoks peetakse eriti tõsiseks sekkumiseks asjaomaste isikute õigustesse ja vabadustesse, sest see võib mõjutada suure osa elanikkonna eraelu, tekitada pideva jälgimise tunde ning kaudselt veenda loobuma kogunemisvabaduse ja muude põhiõiguste kasutamisest. Kuna selliste reaalajas 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.

(19) Seepärast peaks selliste süsteemide kasutamine õiguskaitse eesmärgil olema keelatud, välja arvatud kolmes ammendavalt loetletud ja kitsalt määratletud olukorras, kus nende süsteemide kasutamine on rangelt vajalik selleks, et saavutada olulise avaliku huvi eesmärk, mille tähtsus kaalub riskid üles. Selliste olukordade hulka kuuluvad võimalike kuriteoohvrite, kaasa arvatud kadunud laste otsimine, teatavad füüsiliste isikute elu või füüsilist turvalisust ähvardavad ohud või terrorirünnaku oht ning nõukogu raamotsuses 2002/584/JSK[38] osutatud kuritegude toimepanijate või sellistes kuritegudes kahtlustatavate avastamine, nende asukohta kindlaks tegemine, nende tuvastamine või neile süüdistuse esitamine, kui sellise kuriteo eest karistatakse asjaomases liikmesriigis vabadusekaotuse või vabadust piirava julgeolekumeetmega, mille maksimaalne pikkus on vähemalt kolm aastat, nagu selle liikmesriigi õigusaktides kindlaks määratud. Sellise ajalise piiri seadmine siseriikliku õiguse kohasele vabadusekaotusele või vabadust piiravale julgeolekumeetmele aitab tagada, et reaalajas toimuva biomeetrilise kaugtuvastamise süsteemide kasutamine oleks õigustatud vaid piisavalt tõsiste rikkumiste korral. Peale selle on nõukogu raamotsuses 2002/584/JSK loetletud 32 kuriteost mõned praktikas tõenäoliselt teistest asjakohasemad, sest reaalajas toimuva biomeetrilise kaugtuvastamise kasutamise eeldatav vajalikkus ja proportsionaalsus varieeruvad märkimisväärselt, kui tegemist on loetelus nimetatud kuriteo toimepanija või sellises kuriteos kahtlustatava reaalse avastamise, tema asukoha kindlaks tegemise, tema tuvastamise või talle süüdistuse esitamisega ja kui võetakse arvesse võimalike negatiivsete tagajärgede raskusastme, tõenäosuse ja ulatuse tõenäolisi erinevusi.

(20) Lisaks sellele on nende süsteemide vastutustundliku ja proportsionaalse kasutamise tagamiseks oluline panna paika, et igaühes neist kolmest ammendavalt loetletud ja kitsalt määratletud olukorrast tuleks arvesse võtta teatavaid elemente, eeskätt mis puudutab taotluse aluseks oleva olukorra olemust ja kasutamise tagajärgi seoses kõigi asjaomaste isikute õiguste ja vabadustega ning kasutamise korral ettenähtud kaitsemeetmeid ja tingimusi. Peale selle peaks reaalajas toimuva biomeetrilise kaugtuvastamise süsteemi kasutamine avalikult juurdepääsetavas ruumis õiguskaitse eesmärgil olema ajas ja ruumis asjakohaselt piiratud, võttes eelkõige arvesse tõendeid või viiteid ohu, ohvrite või toimepanija kohta. Isikute võrdlusandmebaas peaks olema iga eespool nimetatud kolme olukorra puhul iga kasutusmalli jaoks sobiv.

(21) Iga kord, kui reaalajas toimuva biomeetrilise kaugtuvastamise süsteemi kasutatakse avalikult juurdepääsetavas ruumis õiguskaitse eesmärgil, peaks selleks olema liikmesriigi õigusasutuse või sõltumatu haldusasutuse selge ja konkreetne luba. Põhimõtteliselt tuleks selline luba saada enne kasutamist, kui just pole tegemist nõuetekohaselt põhjendatud kiireloomulise juhtumiga, st olukorraga, kus vajadus kõnealuste süsteemide kasutamise järele on selline, et enne kasutamise algust ei ole reaalselt ega objektiivselt võimalik luba saada. Selliste kiireloomuliste juhtumite korral peaks kasutamine piirduma hädavajaliku miinimumiga ning selle suhtes peaksid kehtima asjakohased kaitsemeetmed ja tingimused, mis on kindlaks määratud siseriiklikus õiguses ja mida õiguskaitseasutus iga individuaalse kiireloomulise kasutusjuhtumi korral täpsustab. Lisaks sellele peaks õiguskaitseasutus sellistel juhtudel püüdma saada loa nii pea kui võimalik ja põhjendama, miks ta ei saanud luba varem taotleda.

---

[38] Nõukogu 13. juuni 2002. aasta raamotsus 2002/584/JSK Euroopa vahistamismääruse ja liikmesriikidevahelise üleandmiskorra kohta (EÜT L 190, 18.7.2002, lk 1).

(22) Ühtlasi on käesoleva määrusega kehtestatavas ammendavas raamistikus otstarbekas ette näha, et selline kasutamine liikmesriigi territooriumil kooskõlas käesoleva määrusega peaks olema võimalik üksnes siis ja niivõrd, kuivõrd kõnealune liikmesriik on otsustanud oma siseriikliku õiguse üksikasjalikes õigusnormides selgelt sätestada võimaluse sellist kasutamist lubada. Seega jääb liikmesriikidele käesoleva määruse alusel vabadus sellist võimalust üldse mitte ette näha või näha selline võimalus ette üksnes mõne eesmärgi jaoks, mille puhul on käesolevas määruses kirjeldatud lubatud kasutamine õigustatud.

(23) Tehisintellektisüsteemide kasutamine avalikult juurdepääsetavas ruumis õiguskaitse eesmärgil reaalajas toimuva füüsiliste isikute biomeetrilise kaugtuvastamise jaoks eeldab igal juhul biomeetriliste andmete töötlemist. Käesoleva määruse sätted, millega keelatakse selline kasutamine teatavate eranditega ja mis põhinevad ELi toimimise lepingu artiklil 16, tuleks direktiivi (EL) 2016/680 artiklis 10 sätestatud biomeetriliste andmete töötlemist käsitlevate õigusnormide suhtes, peaksid kehtima erinormina (*lex specialis*), nii et selline kasutamine ja sellega kaasnev biomeetriliste andmete töötlemine oleksid ammendavalt reguleeritud. Seega peaks selline kasutamine ja töötlemine olema võimalik üksnes siis, kui see on kooskõlas käesoleva määrusega kehtestatud raamistikuga, ning väljaspool seda raamistikku ei tohiks pädevatel asutustel olla võimalik õiguskaitse eesmärgil tegutsedes kasutada selliseid süsteeme ja töödelda sellega seoses selliseid andmeid direktiivi (EL) 2016/680 artiklis 10 loetletud põhjustel. Seoses sellega ei ole käesoleva määruse eesmärk anda õiguslikku alust isikuandmete töötlemiseks direktiivi 2016/680 artikli 8 alusel. Käesoleva määrusega loodud eriraamistik, mis käsitleb sellist kasutamist õiguskaitse eesmärgil, ei peaks siiski hõlmama reaalajas toimuva biomeetrilise kaugtuvastamise süsteemide kasutamist avalikult juurdepääsetavas ruumis muul otstarbel kui õiguskaitse eesmärgil, ka siis, kui seda teevad pädevad asutused. Seega ei peaks selliseks kasutamise suhtes muul otstarbel kui õiguskaitse eesmärgil kehtima käesoleva määruse kohase loa nõue ega selle jõustamiseks kohaldatavad üksikasjalikud siseriiklikud õigusnormid.

(24) Igasugune biomeetriliste ja muude isikuandmete töötlemine, mis on seotud tehisintellektisüsteemide kasutamisega biomeetrilise tuvastamise jaoks, v.a juhul, kui see toimub seoses käesoleva määrusega reguleeritud reaalajas toimuva biomeetrilise kaugtuvastamise süsteemide kasutamisega avalikult juurdepääsetavas ruumis õiguskaitse eesmärgil, kaasa arvatud juhul, kui pädevad asutused kasutavad neid süsteeme avalikult juurdepääsetavas ruumis muul otstarbel kui õiguskaitse eesmärgil, peaks ka edaspidi vastama kõigile määruse (EL) 2016/679, artikli 9 lõikest 1, määruse (EL) 2018/1725 artikli 10 lõikest 1 ja direktiivi (EL) 2016/680 artiklist 10 tulenevatele nõuetele, nagu on asjakohane.

(25) ELi lepingule ja ELi toimimise lepingule lisatud protokolli nr 21 (Ühendkuningriigi ja Iirimaa seisukoha kohta vabadusel, turvalisusel ja õigusel rajaneva ala suhtes) artikli 6a kohaselt ei ole ELi toimimise lepingu artikli 16 põhjal vastu võetud käesoleva määruse artikli 5 lõike 1 punktis d ning lõigetes 2 ja 3 normid füüsiliste isikute kaitse kohta isikuandmete töötlemisel liikmesriikide poolt ELi toimimise lepingu kolmanda osa V jaotise 4. ja 5. peatüki kohaldamisalasse kuuluva tegevuse puhul Iirimaa suhtes siduvad, kui Iirimaa suhtes ei ole siduvad normid, mis käsitlevad õigusalast koostööd kriminaalasjades või politseikoostööd, mille raames tuleb järgida ELi toimimise lepingu artikli 16 alusel kehtestatud sätteid.

(26) ELi lepingule ja ELi toimimise lepingule lisatud protokolli nr 22 (Taani seisukoha kohta) artiklite 2 ja 2a kohaselt ei ole ELi toimimise lepingu artikli 16 põhjal vastu võetud käesoleva määruse artikli 5 lõike 1 punktis d ning lõigetes 2 ja 3 sätestatud

normid füüsiliste isikute kaitse kohta isikuandmete töötlemisel liikmesriikide poolt ELi toimimise lepingu kolmanda osa V jaotise 4. ja 5. peatüki kohaldamisalasse kuuluva tegevuse puhul Taani suhtes siduvad ega kohaldatavad.

(27) Suure riskiga tehisintellektisüsteem tuleks liidus turule lasta või kasutusele võtta üksnes siis, kui see vastab teatavatele kohustuslikele nõuetele. Need nõuded peaksid tagama, et liidus kättesaadavad suure riskiga tehisintellektisüsteemid või tehisintellektisüsteemid, mille väljundit kasutatakse liidus muul viisil, ei kujuta endast vastuvõetamatut riski liidu õigusega tunnustatud ja kaitstud liidu oluliste avalike huvide suhtes. Suure riskiga tehisintellektisüsteemideks tuleks pidada üksnes selliseid tehisintellektisüsteeme, millel on liidus oluline kahjulik mõju inimeste tervisele, ohutusele ja põhiõigustele, ning selline piirang minimeerib kõik võimalikud rahvusvahelise kaubanduse piirangud, kui neid peaks olema.

(28) Tehisintellektisüsteemid võivad kahjustada inimeste tervist ja ohutust, eriti juhul, kui sellised süsteemid on toodete komponendid. Kooskõlas liidu ühtlustamisõigusaktide eesmärkidega hõlbustada toodete vaba liikumist siseturul ja tagada, et siseturule saabuvad ainult ohutud ja muul viisil nõuetele vastavad tooted, on oluline tõhusalt ära hoida ja leevendada riske, mille toode kui tervik võib põhjustada oma digitaalsete komponentide, sh tehisintellektisüsteemide tõttu. Näiteks üha autonoomsemad robotid peaksid suutma ohutult töötada ja täita oma ülesandeid keerukates keskkondades, seda nii tootmise kui ka isikliku abi ja hoolduse valdkonnas. Sama moodi peaksid usaldusväärsed ja täpsed olema tervishoiusektoris kasutatavad üha keerulisemad diagnostikasüsteemid ja inimeste otsuseid toetavad süsteemid, sest seal on tegemist elu ja tervise seisukohast eriti oluliste otsustega. Tehisintellektisüsteemi liigitamisel suure riskiga tehisintellektisüsteemiks on eriti oluline see, kui ulatuslik on tehisintellektisüsteemi kahjulik mõju põhiõiguste hartaga kaitstud põhiõigustele. Nende õiguste hulka kuuluvad õigus inimväärikusele, era- ja perekonnaelu austamine, isikuandmete kaitse, väljendus- ja teabevabadus, kogunemis- ja ühinemisvabadus, mittediskrimineerimine, tarbijakaitse, töötajate õigused, puuetega inimeste õigused, õigus tõhusale õiguskaitsevahendile ja õiglasele kohtulikule arutamisele, õigus kaitsele, süütuse presumptsioon ja õigus heale haldusele. Lisaks nimetatud õigustele on oluline rõhutada, et lastel on eraldi õigused, mis on sätestatud ELi 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. Hinnates, kui tõsist kahju võib tehisintellektisüsteem põhjustada, muu hulgas inimeste tervise ja ohutuse vallas, tuleks kaaluda ka põhiõiguste hartas sätestatud ja liidu põhimõtetega rakendatud põhiõigust kõrgetasemelisele keskkonnakaitsele.

(29) Mis puudutab suure riskiga tehisintellektisüsteeme, mis on toodete või süsteemide turvakomponendid või mis on ise tooted või süsteemid, mis kuuluvad Euroopa Parlamendi ja nõukogu määruse (EÜ) nr 300/2008[39], Euroopa Parlamendi ja nõukogu määruse (EL) nr 167/2013[40], Euroopa Parlamendi ja nõukogu määruse (EL) nr

[39] Euroopa Parlamendi ja nõukogu 11. märtsi 2008. aasta määrus (EÜ) nr 300/2008, mis käsitleb tsiviillennundusjulgestuse ühiseeskirju ja millega tunnistatakse kehtetuks määrus (EÜ) nr 2320/2002 (ELT L 97, 9.4.2008, lk 72).

[40] Euroopa Parlamendi ja nõukogu 5. veebruari 2013. aasta määrus (EL) nr 167/2013 põllu- ja metsamajanduses kasutatavate sõidukite kinnituse ja turujärelevalve kohta (ELT L 60, 2.3.2013, lk 1).

168/2013[41], Euroopa Parlamendi ja nõukogu direktiivi 2014/90/EL[42], Euroopa Parlamendi ja nõukogu direktiivi (EL) 2016/797[43], Euroopa Parlamendi ja nõukogu määruse (EL) 2018/858[44], Euroopa Parlamendi ja nõukogu määruse (EU) 2018/1139[45] ja Euroopa Parlamendi ja nõukogu määruse (EL) 2019/2144[46] kohaldamisalasse, siis on otstarbekas muuta kõnealuseid õigusakte tagamaks, et kui komisjon võtab nimetatud õigusaktide põhjal edaspidi vastu asjaomaseid delegeeritud või rakendusakte, võtab ta arvesse käesolevas määruses suure riskiga tehisintellektisüsteemide kohta sätestatud kohustuslikke nõudeid, tuginedes iga sektori tehnilistele ja regulatiivsetele iseärasustele ja ilma, et ta sekkuks nende õigusaktidega kehtestatud olemasolevatesse juhtimis-, vastavushindamis- ja jõustamismehhanismidesse või -asutustesse.

(30) Mis puudutab tehisintellektisüsteeme, mis on toodete turvakomponendid või mis on ise tooted, mis kuuluvad teatavate liidu ühtlustamisõigusaktide kohaldamisalasse, siis on otstarbekas liigitada need tehisintellektisüsteemid käesoleva määruse alusel suure riskiga tehisintellektisüsteemideks, kui nende asjaomaste liidu õigusaktide alusel teeb kõnealuse toote vastavushindamise kolmandast isikust vastavushindamisasutus. Sellised tooted on eeskätt masinad, mänguasjad, liftid, plahvatusohtlikus keskkonnas kasutatavad seadmed ja kaitsesüsteemid, raadioseadmed, surveseadmed, lõbusõidulaevade varustus, köisteed, küttegaasiseadmed, meditsiiniseadmed ja *in vitro* diagnostika meditsiiniseadmed.

(31) See, kui tehisintellektisüsteem liigitatakse käesoleva määruse alusel suure riskiga tehisintellektisüsteemiks, ei peaks ilmtingimata tähendama, et toodet, mille turvakomponent see tehisintellektisüsteem on, või tehisintellektisüsteemi ennast kui toodet peetakse suure riskiga tooteks vastavalt selle toote suhtes kohaldatavate asjaomaste liidu ühtlustamisõigusaktidega kehtestatud kriteeriumidele. Esmajoones

---

41 Euroopa Parlamendi ja nõukogu 15. jaanuari 2013. aasta määrus (EL) nr 168/2013 kahe-, kolme- ja neljarattaliste sõidukite kinnituse ja turujärelevalve kohta (ELT L 60, 2.3.2013, lk 52).

42 Euroopa Parlamendi ja nõukogu 23. juuli 2014. aasta direktiiv 2014/90/EL, milles käsitletakse laevavarustust ja millega tunnistatakse kehtetuks nõukogu direktiiv 96/98/EÜ (ELT L 257, 28.8.2014, lk 146);

43 Euroopa Parlamendi ja nõukogu 11. mai 2016. aasta direktiiv (EL) 2016/797 Euroopa Liidu raudteesüsteemi koostalitluse kohta (ELT L 138, 26.5.2016, lk 44).

44 Euroopa Parlamendi ja nõukogu 30. mai 2018. aasta määrus (EL) 2018/858 mootorsõidukite ja mootorsõidukite haagiste ning nende jaoks ette nähtud süsteemide, osade ja eraldi seadmestike tüübikinnituse ja turujärelevalve kohta, ning millega muudetakse määruseid (EÜ) nr 715/2007 ja (EÜ) nr 595/2009 ning tunnistatakse kehtetuks direktiiv 2007/46/EÜ (ELT L 151, 14.6.2018, lk 1).

45 Euroopa Parlamendi ja nõukogu 4. juuli 2018. aasta määrus (EL) 2018/1139, mis käsitleb tsiviillennunduse valdkonna ühisnorme ja millega luuakse Euroopa Liidu Lennundusohutusamet ning millega muudetakse Euroopa Parlamendi ja nõukogu määrusi (EÜ) nr 2111/2005, (EÜ) nr 1008/2008, (EL) nr 996/2010, (EL) nr 376/2014 ja Euroopa Parlamendi ja nõukogu direktiive 2014/30/EL ning 2014/53/EL ning tunnistatakse kehtetuks Euroopa Parlamendi ja nõukogu määrused (EÜ) nr 552/2004 ja (EÜ) nr 216/2008 ning nõukogu määrus (EMÜ) nr 3922/91 (ELT L 212, 22.8.2018, lk 1).

46 Euroopa Parlamendi ja nõukogu 27. novembri 2019. aasta määrus (EL) 2019/2144, mis käsitleb mootorsõidukite ja nende haagiste ning mootorsõidukite jaoks ette nähtud süsteemide, osade ja eraldi seadmestike tüübikinnituse nõudeid seoses nende üldise ohutuse ning sõitjate ja vähekaitstud liiklejate kaitsega ning millega muudetakse Euroopa Parlamendi ja nõukogu määrust (EL) 2018/858 ja tunnistatakse kehtetuks Euroopa Parlamendi ja nõukogu määrused (EÜ) nr 78/2009, (EÜ) nr 79/2009 ja (EÜ) nr 661/2009 ning komisjoni määrused (EÜ) nr 631/2009, (EL) nr 406/2010, (EL) nr 672/2010, (EL) nr 1003/2010, (EL) nr 1005/2010, (EL) nr 1008/2010, (EL) nr 1009/2010, (EL) nr 19/2011, (EL) nr 109/2011, (EL) nr 458/2011, (EL) nr 65/2012, (EL) nr 130/2012, (EL) nr 347/2012, (EL) nr 351/2012, (EL) nr 1230/2012 ja (EL) 2015/166 (ELT L 325, 16.12.2019, lk 1).

puudutab see Euroopa Parlamendi ja nõukogu määrust (EL) 2017/745[47] ja Euroopa Parlamendi ja nõukogu määrust (EL) 2017/746,[48] kui keskmise ja suure riskiga toodete puhul on ette nähtud kolmanda isiku tehtav vastavushindamine.

(32) Eraldiseisvad tehisintellektisüsteemid, st suure riskiga tehisintellektisüsteemid, mis ei ole toodete turvakomponendid või ise tooted, on otstarbekas liigitada suure riskiga tehisintellektisüsteemideks, kui need põhjustavad oma sihtotstarbe tõttu suure riski ja ähvardavad kahjustada inimeste tervist ja ohutust või põhiõigusi, võttes arvesse nii võimaliku kahju tõsidust kui ka selle tekkimise tõenäosust, ja kui neid kasutatakse määruses eelnevalt täpselt kindlaks määratud valdkondades. Nende süsteemide kindlakstegemine põhineb samadel meetoditel ja kriteeriumidel, mida kavatsetakse kasutada suure riskiga tehisintellektisüsteemide loetelu tulevaste võimalike muudatuste jaoks.

(33) Füüsiliste isikute biomeetrilise kaugtuvastamise jaoks mõeldud tehisintellektisüsteemide tehniline ebatäpsus võib kaasa tuua tulemuste kallutatuse ja põhjustada diskrimineerimist. Eriti oluline on see vanuse, etniline päritolu, soo või puuete puhul. Seepärast tuleks nii reaalajas kui ka tagantjärele toimuva biomeetrilise kaugtuvastamise süsteemid liigitada suure riskiga süsteemideks. Arvestades, milliseid riske need süsteemid põhjustavad, tuleks mõlemat liiki biomeetrilise kaugtuvastamise süsteemide suhtes kohaldada logimisvõimekuse ja inimjärelevalve erinõudeid.

(34) Elutähtsa taristu juhtimise ja käitamisega seoses on otstarbekas liigitada suure riskiga tehisintellektisüsteemiks need tehisintellektisüsteemid, mis on mõeldud kasutamiseks maanteeliikluse korraldamise ja käitamise või vee, gaasi, kütteenergia ja elektri tarnimise turvakomponentidena, sest nende tõrge või talitlushäire võib seada ohtu paljude inimeste elu ja tervise ning põhjustada märgatavaid häireid tavapärases sotsiaalses ja majandustegevuses.

(35) Tehisintellektisüsteeme, mida kasutatakse hariduses või kutseõppes esmajoones selleks, et määrata kindlaks juurdepääs haridus- ja kutseõppeasutustele või määrata isikud neisse või hinnata hariduse osana või selle eeltingimusena isikute teste, tuleks käsitada suure riskiga süsteemidena, sest need võivad ära määrata inimese haridusliku ja kutsealase käekäigu ning mõjutada seega nende toimetulekut. Kui sellised süsteemid ei ole korralikult projekteeritud või kui neid ei kasutata korralikult, võivad need rikkuda õigust haridusele ja koolitusele, aga ka õigust mitte olla diskrimineeritud, ning põlistada aegade jooksul välja kujunenud diskrimineerimismustreid.

(36) Suure riskiga tehisintellektisüsteemideks tuleks liigitada ka tehisintellektisüsteemid, mida kasutatakse tööhõive, töötajate juhtimise ja füüsilisest isikust ettevõtjana tegutsemise võimaluste valdkonnas, eeskätt inimeste töölevõtmiseks ja valikuks, edutamise ja töösuhte lõpetamise otsuste tegemiseks ning ülesannete jagamise, seire või inimeste hindamise jaoks tööga seotud lepingulistes suhete kontekstis, sest need süsteemid võivad märkimisväärselt mõjutada nende inimeste tulevasi karjääriväljavaateid ja toimetulekut. Asjaomased tööga seotud lepingulised suhted peaksid käima ka selliste töötajate ja isikute kohta, kes osutavad teenuseid platvormide

---

47 Euroopa Parlamendi ja nõukogu 5. aprilli 2017. aasta määrus (EL) 2017/745, milles käsitletakse meditsiiniseadmeid, millega muudetakse direktiivi 2001/83/EÜ, määrust (EÜ) nr 178/2002 ja määrust (EÜ) nr 1223/2009 ning millega tunnistatakse kehtetuks nõukogu direktiivid 90/385/EMÜ ja 93/42/EMÜ (ELT L 117, 5.5.2017, lk 1).

48 Euroopa Parlamendi ja nõukogu 5. aprilli 2017. aasta määrus (EL) 2017/746 *in vitro* diagnostikameditsiiniseadmete kohta ning millega tunnistatakse kehtetuks direktiiv 98/79/EÜ ja komisjoni otsus 2010/227/EL (ELT L 117, 5.5.2017, lk 176).

kaudu, nagu on nimetatud komisjoni 2021. aasta tööprogrammis. Põhimõtteliselt ei tuleks selliseid isikuid käsitada kasutajatena käesoleva määruse tähenduses. Värbamisprotsessi käigus ning isikute hindamisel, edutamisel ja ametisse jäämisel tööga seotud lepinguliste suhete kontekstis võivad sellised süsteemid põlistada aegade jooksul välja kujunenud diskrimineerimismustreid, mis on suunatud näiteks naiste, teatavate vanuserühmade, puuetega inimeste või teatava rassilise või etnilise päritolu või seksuaalse sättumusega isikute vastu. Tehisintellektisüsteemid, mida kasutatakse nende isikute töötulemuste ja käitumise seireks, võivad mõjutada ka nende õigust andmekaitsele ja privaatsusele.

(37) Veel üks valdkond, milles tuleks tehisintellektisüsteemide kasutamisele erilist tähelepanu pöörata, on teatavate selliste oluliste era- ja avalik-õiguslike teenuste ja hüvede juurdepääsetavus ja kasutamine, mida inimesed vajavad, et ühiskonnas täielikult osaleda või oma elatustaset parandada. Eeskätt tuleks suure riskiga tehisintellektisüsteemideks liigitada tehisintellektisüsteemid, mida kasutatakse füüsilistele isikutele krediidihinnangu andmiseks või nende krediidivõimelisuse hindamiseks, sest need panevad paika inimese juurdepääsu finantsvahenditele või olulistele teenustele, nagu kinnisvara, elekter ja telekommunikatsiooniteenused. Sel otstarbel kasutatavad tehisintellektisüsteemid võivad põhjustada inimeste või rühmade diskrimineerimist ja põlistada aegade jooksul välja kujunenud diskrimineerimismustreid, mille aluseks on näiteks rassiline või etniline päritolu, puuded, vanus, seksuaalne sättumus, või avaldada uut liiki diskrimineerivat mõju. Arvestades mõju väga piiratud ulatust ja turul kättesaadavaid alternatiive, on otstarbekas teha erand tehisintellektisüsteemidele, mille eesmärk on krediidivõimelisuse hindamine ja krediidihindamine, kui sellised süsteemid võtavad kasutusele väikepakkujad oma tarbeks. Füüsilised isikud, kes taotlevad või saavad avaliku sektori asutustelt sotsiaaltoetusi ja -teenuseid, sõltuvad tavaliselt nendest toetustest ja teenustest ning on vastutavate asutustega võrreldes haavatavas olukorras. Kui tehisintellektisüsteeme kasutatakse selleks, et teha kindlaks, kas ametiasutus peaks sellise toetuse või teenuse tagasi lükkama, seda vähendama, selle tühistama või tagasi nõudma, võib neil süsteemidel olla märkimisväärne mõju inimese toimetulekule ning need süsteemid võivad rikkuda inimeste põhiõigusi, näiteks õigust sotsiaalkaitsele, mittediskrimineerimisele, inimväärikusele või tõhusale õiguskaitsevahendile. Seepärast tuleks need süsteemid liigitada suure riskiga tehisintellektisüsteemideks. Samas ei tohiks käesolev määrus takistada uuenduslike lähenemisviiside väljatöötamist ja kasutamist avalikus halduses, kus oleks nõuetekohaste ja ohutute tehisintellektisüsteemide laialdasemast kasutamisest rohkelt kasu tingimusel, et need süsteemid ei põhjusta juriidilistele ja füüsilistele isikutele suuri riske. Lisaks eelnimetatule tuleks suure riskiga tehisintellektisüsteemideks liigitada ka tehisintellektisüsteemid, mida kasutatakse kiirabi ja päästeteenistuse väljasaatmiseks ja väljakutsete prioriseerimiseks, sest need teevad otsuseid olukordades, mis on inimeste elu, tervise ja vara seisukohast väga kriitilised.

(38) Õiguskaitseasutuste toiminguid, millega kaasneb tehisintellektisüsteemide teatav kasutamine, iseloomustab võimu väga ebavõrdne jaotumine ja nende tulemuseks võib olla jälgimine, arreteerimine või füüsilise isiku vabaduse võtmine, aga ka muu kahjulik mõju põhiõiguste hartaga tagatud põhiõigustele. Tehisintellektisüsteem võib olla inimeste valikul diskrimineeriv või muul moel ebatäpne või ebaõiglane, eriti juhul, kui selle treenimiseks ei ole kasutatud kvaliteetseid andmeid, kui süsteemi täpsus või stabiilsus ei ole piisavad või kui seda ei ole enne turule laskmist või muul moel kasutusele võtmist korralikult projekteeritud ja testitud. Kahjustatud võib saada ka võimalus kasutada selliseid olulisi menetluslikke põhiõigusi, nagu õigus tõhusale

õiguskaitsevahendile ja õiglasele kohtulikule arutamisele, õigus kaitsele ja süütuse presumptsioon, seda eriti juhul, kui sellised tehisintellektisüsteemid ei ole piisavalt läbipaistvad, selgitatavad ja dokumenteeritud. Seepärast on asjakohane liigitada suure riskiga tehisintellektisüsteemiks hulk tehisintellektisüsteeme, mis on mõeldud kasutamiseks õiguskaitses, kus täpsus, usaldusväärsus ja läbipaistvus on eriti olulised, et hoida ära kahjulikku mõju, säilitada üldsuse usaldus ning tagada aruandekohustus ja tõhus õiguskaitse. Arvestades kõnealuste toimingute olemust ja nendega seotud riske, peaksid selliste suure riskiga tehisintellektisüsteemide hulka kuuluma eeskätt need tehisintellektisüsteemid, mis on mõeldud õiguskaitseasutustele kasutamiseks individuaalsete riskihindamiste, valedetektorite ja samalaadsete vahendite jaoks või füüsilise isiku emotsionaalse seisundi tuvastamiseks, süvavõltsingute avastamiseks, tõendite usaldusväärsuse hindamiseks kriminaalmenetluses, tegeliku või potentsiaalse kuriteo esinemise või kordumise prognoosimiseks füüsiliste isikute profiilianalüüsi põhjal või füüsiliste isikute või rühmade isikuomaduste, erijoonte või varasema kuritegeliku käitumise hindamiseks, kuritegude avastamise, uurimise või nende eest vastutusele võtmise käigus tehtavaks profiilianalüüsiks, aga ka füüsilisi isikuid puudutavaks kuritegude analüüsiks. Tehisintellektisüsteeme, mis on mõeldud spetsiaalselt maksu- ja tolliasutustele haldusmenetlustes kasutamiseks, ei tuleks käsitada suure riskiga tehisintellektisüsteemidena, mida õiguskaitseasutused kasutavad süütegude tõkestamise, avastamise, uurimise ja nende eest vastutusele võtmise eesmärgil.

(39) Rände-, varjupaiga- ja piirkontrollihalduses kasutatavad tehisintellektisüsteemid mõjutavad inimesi, kes on tihtipeale eriti haavatavas olukorras ja sõltuvad pädevate asutuste tegevuse tulemustest. Seepärast on sellises kontekstis kasutatavate tehisintellektisüsteemide täpsus, mittediskrimineeriv olemus ja läbipaistvus eriti oluline, et tagada mõjutatud isikute põhiõiguste austamine, eeskätt nende õigus vabale liikumisele, mittediskrimineerimisele, eraelu ja isikuandmete kaitsele, rahvusvahelisele kaitsele ja heale haldusele. Seepärast on otstarbekas liigitada suure riskiga tehisintellektisüsteemiks sellised tehisintellektisüsteemid, mis on mõeldud rände-, varjupaiga- ja piirikontrollihaldusega tegelevatele pädevatele asutustele kasutamiseks valedetektorite ja samalaadsete vahenditena või füüsilise isiku emotsionaalse seisundi tuvastamiseks; teatavate liikmesriigi territooriumile siseneva või viisat või varjupaika taotleva füüsilise isiku põhjustatavate riskide hindamiseks; füüsiliste isikute asjaomaste dokumentide ehtsuse kontrollimiseks; pädevate asutuste abistamiseks varjupaiga-, viisa- ja elamisloataotluste ja nendega seotud kaebuste läbivaatamisel, et teha kindlaks sellist staatust taotlevate füüsiliste isikute vastavus tingimustele. Rände-, varjupaiga- ja piirikontrollihalduse valdkonna tehisintellektisüsteemid, mis kuuluvad käesoleva määruse kohaldamisalasse, peaksid vastama Euroopa Parlamendi ja nõukogu direktiivis 2013/32/EL,[49] Euroopa Parlamendi ja nõukogu määruses (EÜ) nr 810/2009[50] ja muudes asjaomastes õigusaktides sätestatud asjaomastele menetlusnõuetele.

(40) Teatavad õigusemõistmise ja demokraatlike protsesside jaoks mõeldud tehisintellektisüsteemid tuleks liigitada suure riskiga tehisintellektisüsteemideks, arvestades nende võimalikku märkimisväärset mõju demokraatiale, õigusriigile,

[49] Euroopa Parlamendi ja nõukogu 26. juuni 2013. aasta direktiiv 2013/32/EL rahvusvahelise kaitse seisundi andmise ja äravõtmise menetluse ühiste nõuete kohta (ELT L 180, 29.6.2013, lk 60).

[50] Euroopa Parlamendi ja nõukogu 13. juuli 2009. aasta määrus (EÜ) nr 810/2009, millega kehtestatakse ühenduse viisaeeskiri (viisaeeskiri) (ELT L 243, 15.9.2009, lk 1).

üksikisiku vabadustele ning õigusele tõhusale õiguskaitsevahendile ja õiglasele kohtulikule arutamisele. Eeskätt võimalikust kallutatusest, vigadest ja läbipaistmatusest tulenevate riskidega toimetulemiseks on otstarbekas liigitada suure riskiga tehisintellektisüsteemideks need tehisintellektisüsteemid, mis on mõeldud abistama õigusasutusi faktide ja seadustega tutvumisel ja nende tõlgendamisel ning õiguse rakendamisel konkreetse faktide kogumi suhtes. Samas ei tohiks selline liigitamine siiski laieneda tehisintellektisüsteemidele, mis on mõeldud puhtalt halduslikeks abitegevusteks, mis ei mõjuta tegelikku õigusemõistmist konkreetsetel juhtudel, nagu kohtuotsuste, dokumentide või andmete anonüümimine või pseudonüümimine, töötajatevaheline suhtlus, haldusülesanded või ressursside jaotamine.

(41) Kui tehisintellektisüsteem on käesoleva määruse alusel liigitatud suure riskiga tehisintellektisüsteemiks, ei tuleks seda tõlgendada nii, et süsteemi kasutamine on ilmtingimata seaduslik muude liidu õigusaktide või liidu õigusega kooskõlas olevate siseriiklike õigusaktide alusel, mis käsitlevad näiteks isikuandmete kaitset, valedetektorite või samalaadsete toodete kasutamist või muude süsteemide kasutamist füüsiliste isikute emotsionaalse seisundi tuvastamiseks. Edaspidi peaks igasugune selline kasutamine toimuma üksnes kooskõlas kohaldatavate nõuetega, mis tulenevad põhiõiguste hartast ja kohaldatavatest liidu teisese õiguse aktidest ja siseriiklikust õigusest. Käesolevat määrust ei tohiks käsitada isikuandmete, sealhulgas asjakohasel juhul isikuandmete eriliikide töötlemise õigusliku alusena.

(42) Et leevendada riske, mida liidus turule lastud või muul moel kasutusele võetud tehisintellektisüsteemid põhjustavad kasutajatele ja mõjutatud isikutele, tuleks kohaldada teatavaid kohustuslikke nõudeid, võttes arvesse süsteemi kasutamise sihtotstarvet ja toimides pakkuja kehtestatud riskijuhtimissüsteemi kohaselt.

(43) Suure riskiga tehisintellektisüsteemide suhtes tuleks kohaldada nõudeid seoses kasutatavate andmestike kvaliteedi, tehnilise dokumentatsiooni ja andmete säilitamise, läbipaistvuse ja kasutajate teavitamise, inimjärelevalve, stabiilsuse, täpsuse ja küberturvalisusega. Sellised nõuded on vajalikud, et tulemuslikult leevendada riske tervisele, ohutusele ja põhiõigustele, nagu on asjakohane süsteemi sihtotstarvet arvestades ning kuna muud kaubandust vähem piiravad meetmed ei ole mõistlikult kättesaadavad, et seega vältida põhjendamatuid kaubanduspiiranguid.

(44) Kvaliteetsed andmed on paljude tehisintellektisüsteemide toimimiseks hädavajalikud, eriti kui kasutatakse mudelite treenimise meetodeid, et tagada suure riskiga tehisintellektisüsteemide sihipärane ja ohutu töö ja see, et neist ei saa liidu õigusega keelatud diskrimineerimise allikas. Kvaliteetsete treenimis-, valideerimis- ja testimisandmestike olemasolu eeldab asjakohaste andmehalduse ja juhtimistavade rakendamist.. Treenimis-, valideerimis- ja testimisandmestikud peaksid olema süsteemi sihtotstarvet arvestades piisavalt asjakohased, representatiivsed, vigadeta ja täielikud. Neid peaksid iseloomustama asjakohased statistilised omadused, sealhulgas mis puudutab selliseid isikuid või isikute rühmi, kelle peal kavatsetakse suure riskiga tehisintellektisüsteemi kasutada. Eeskätt tuleb treenimis-, valideerimis- ja testimisandmestikes võtta sihtotstarbe jaoks vajalikus ulatuses arvesse funktsioone, omadusi või elemente, mis iseloomustavad konkreetset geograafilist, käitumuslikku või funktsionaalset olukorda või konteksti, kus kavatsetakse suure riskiga tehisintellektisüsteemi kasutada. Et kaitsta teiste õigust tehisintellektisüsteemide kallutatusest tuleneda võiva diskrimineerimise eest, peaksid pakkujad saama töödelda isikuandmete eriliike olulise avaliku huvi nimel, et tagada suure riskiga tehisintellektisüsteemide puhul kallutatuse seire, avastamine ja korrigeerimine.

(45) Suure riskiga tehisintellektisüsteemide arendamiseks peaks teatavatel asjaosalistel, näiteks pakkujatel, teavitatud asutustel ja muudel asjaomastel üksustel, näiteks digitaalse innovatsiooni keskustel, testimis- ja eksperimenteerimisrajatistel ja teadlastel, olema oma käesoleva määrusega seotud tegevusvaldkondades juurdepääs kvaliteetsetele andmestikele ja nad peaksid saama neid kasutada. Komisjoni loodud Euroopa ühised andmeruumid ning avaliku huvi nimel hõlpsam andmete jagamine ettevõtete vahel ja valitsustega on äärmiselt tähtis, et pakkuda tehisintellektisüsteemide treenimiseks, valideerimiseks ja testimiseks usaldusväärset, vastutustundlikku ja mittediskrimineerivat juurdepääsu kvaliteetsetele andmetele. Näiteks tervishoiu valdkonnas hõlbustab tervishoiu Euroopa andmeruum mittediskrimineerivat juurdepääsu terviseandmetele ja tehisintellekti algoritmide treenimist selliste andmestikega privaatsust tagaval, turvalisel, õigeaegsel, läbipaistval ja usaldusväärsel viisil ning asjakohase institutsioonilise juhtimise tingimustes. Asjaomased pädevad asutused, sealhulgas valdkondlikud asutused, kes pakuvad või toetavad juurdepääsu andmetele, võivad toetada ka kvaliteetsete andmete pakkumist tehisintellektisüsteemide treenimiseks, valideerimiseks ja testimiseks.

(46) Selleks, et kontrollida vastavust käesoleva määruse kohastele nõuetele, on äärmiselt oluline omada teavet selle kohta, kuidas on suure riskiga tehisintellektisüsteemid välja töötatud ja kuidas need oma elutsükli jooksul töötavad. Selleks on vaja säilitada andmeid ja tagada sellise tehnilise dokumentatsiooni kättesaadavus, mis sisaldab tehisintellektisüsteemi asjakohastele nõuetele vastavuse hindamiseks vajalikku teavet. Sellise teabe hulka peaksid kuuluma süsteemi üldised omadused, võimekused ja piirid, algoritmid, andmed, kasutatud treenimis-, testimis- ja valideerimisprotsessid ning dokumentatsioon asjaomase riskijuhtimissüsteemi kohta. Tehniline dokumentatsioon peaks olema ajakohane.

(47) Seoses läbipaistmatusega, mis võib muuta teatavad tehisintellektisüsteemid füüsiliste isikute jaoks arusaamatuks või liiga keeruliseks, tuleks suure riskiga tehisintellektisüsteemide puhul nõuda teatavat läbipaistvust. Kasutajad peaksid suutma süsteemi väljundit tõlgendada ja asjakohaselt kasutada. Seepärast peaks suure riskiga tehisintellektisüsteemidega olema kaasas asjaomane dokumentatsioon ja kasutusjuhendid, mis peaksid sisaldama täpset ja selget teavet muu hulgas võimalike riskide kohta, mis võivad esineda seoses põhiõiguste ja diskrimineerimisega, kui see on asjakohane.

(48) Suure riskiga tehisintellektisüsteeme tuleks projekteerida ja arendada selliselt, et füüsilised isikud saavad teha järelevalvet nende toimimise üle. Selleks peaks süsteemi pakkuja tegema enne süsteemi turule laskmist või kasutusele võtmist kindlaks asjakohased inimjärelevalve meetmed. Kui see on asjakohane, tuleks selliste meetmetega eeskätt tagada, et süsteemi on sisse ehitatud käitamisega seotud piirangud, mida süsteem ise ei saa tühistada, et süsteem reageerib inimoperaatori käskudele ning et järelevalvega tegelema määratud füüsilised isikud on selle ülesande täitmiseks piisavalt pädevad ning neil on vajalik koolitus ja õigused.

(49) Suure riskiga tehisintellektisüsteemid peaksid toimima kogu oma elutsükli jooksul järjepidevalt ning nende täpsus, stabiilsus ja küberturvalisus peaks olema asjakohasel tasemel vastavalt tehnika üldtunnustatud tasemele. Täpsusaste ja täpsuse parameetrid tuleks kasutajatele teatavaks teha.

(50) Suure riskiga tehisintellektisüsteemide üks peamisi nõudeid on tehniline stabiilsus. Need süsteemid peaksid olema vastupidavad nii süsteemi piirangutega seotud riskide (st vead, rikked, ebakõlad, ootamatud olukorrad) kui ka pahatahtliku tegevuse suhtes,

mis võib kahjustada tehisintellektisüsteemi turvalisust ja põhjustada kahjulikku või muul viisil soovimatut käitumist. Suutmatus kaitsta nende riskide eest võib mõjutada ohutust või kahjustada põhiõigusi näiteks ekslike otsuste või tehisintellektisüsteemi genereeritud ekslike või kallutatud väljundite tõttu.

(51) Küberturvalisusel on oluline roll, et tagada tehisintellektisüsteemide vastupidavus pahatahtlike kolmandate isikute katsetele muuta süsteemi nõrku kohti ära kasudes süsteemi kasutust, käitumist või toimimist või kahjustada selle turvaomadusi. Tehisintellektisüsteemide vastu suunatud küberrünnetes võidakse ära kasutada tehisintellektispetsiifilisi ressursse, näiteks treeningandmestikke (nt andmemürgitus, i.k. *data poisoning*) või treenitud mudeleid (nt vastandründed, i.k. *adversarial attacks*), või tehisintellektisüsteemi digivarade või IKT alustaristu nõrkusi. Seega peaksid suure riskiga tehisintellektisüsteemide pakkujad võtma riskidele vastava küberturvalisuse taseme tagamiseks sobivaid meetmeid, arvestades sealjuures vastavalt vajadusele ka IKT alustaristuga.

(52) Suure riskiga tehisintellektisüsteemide turule laskmise, kasutusele võtmise ja kasutamise suhtes kohaldatavad õigusnormid kui liidu ühtlustamisõigusaktide osa tuleks kehtestada kooskõlas Euroopa Parlamendi ja nõukogu määrusega (EÜ) nr 765/2008,[51] millega sätestatakse akrediteerimise ja turujärelevalve nõuded, Euroopa Parlamendi ja nõukogu otsusega nr 768/2008/EÜ[52] toodete turustamise ühise raamistiku kohta ja Euroopa Parlamendi ja nõukogu määrusega (EL) 2019/1020[53] turujärelevalve ja toodete vastavuse kohta (edaspidi „uus toodete turustamise õigusraamistik“).

(53) On otstarbekas, et suure riskiga tehisintellektisüsteemi turule laskmise või kasutusele võtmise eest võtab vastutuse konkreetne füüsiline või juriidiline isik, kes on määratletud kui pakkuja, olenemata sellest, kas see füüsiline või juriidiline isik on süsteemi projekteerija või arendaja.

(54) Pakkuja peaks kehtestama usaldusväärse kvaliteedijuhtimissüsteemi, tagama nõutava vastavushindamismenetluse teostamise, koostama asjakohase dokumentatsiooni ja kehtestama stabiilse turustamisjärgse seire süsteemi. Avaliku sektori asutused, kes võtavad suure riskiga tehisintellektisüsteemi kasutusele oma tarbeks, võivad võtta vastu kvaliteedijuhtimissüsteemi reeglid ja neid rakendada olenevalt asjaoludest riigi või piirkonna tasemel vastuvõetud kvaliteedijuhtimissüsteemi osana, võttes arvesse sektori iseärasusi ning asjaomase avaliku sektori asutuse pädevust ja töökorraldust.

(55) Kui uue õigusraamistiku asjaomase valdkondliku õigusakti kohaldamisalasse kuuluva toote turvakomponendiks olevat suure riskiga tehisintellektisüsteemi ei lasta turule ega võeta kasutusele tootest sõltumatult, peaks uue õigusraamistiku asjakohases õigusaktis määratletud lõpptoote tootja täitma käesolevas määruses pakkujale kehtestatud kohustusi ja eeskätt tagama selle, et lõpptootesse integreeritud tehisintellektisüsteem vastab käesoleva määruse nõuetele.

---

51 Euroopa Parlamendi ja nõukogu 9. juuli 2008. aasta määrus (EÜ) nr 765/2008, millega sätestatakse akrediteerimise ja turujärelevalve nõuded seoses toodete turustamisega ja tunnistatakse kehtetuks määrus (EMÜ) nr 339/93 (ELT L 218, 13.8.2008, lk 30).

52 Euroopa Parlamendi ja nõukogu 9. juuli 2008. aasta otsus nr 768/2008/EÜ toodete turustamise ühise raamistiku kohta ja millega tunnistatakse kehtetuks nõukogu otsus 93/465/EMÜ (ELT L 218, 13.8.2008, lk 82).

53 Euroopa Parlamendi ja nõukogu 20. juuni 2019. aasta määrus (EL) 2019/1020 turujärelevalve ja toodete vastavuse kohta ning millega muudetakse direktiivi 2004/42/EÜ ja määruseid (EÜ) nr 765/2008 ja (EL) nr 305/2011 (ELT L 169, 25.6.2019, lk 1–44).

(56) Et võimaldada käesoleva määruse täitmine ja luua operaatoritele võrdsed tingimused, võttes sealjuures arvesse digitoodete kättesaadavaks tegemise eri vorme, on oluline tagada, et mõni liidus tegutsev isik saab igas olukorras esitada ametiasutustele kogu vajaliku teabe tehisintellektisüsteemi nõuetele vastavuse kohta. Seepärast peab väljaspool liitu asuv pakkuja juhul, kui importijat ei ole võimalik kindlaks teha, enne oma süsteemi liidu turul kättesaadavaks tegemist määrama kirjaliku volitusega liidus asuva volitatud esindaja.

(57) Kooskõlas uue õigusraamistiku põhimõtetega tuleks asjaomaste ettevõtjate, nt importijate ja turustajate jaoks kehtestada spetsiifilised kohustused, et tagada õiguskindlus ja muuta õigusnormide täitmine neile asjaomastele ettevõtjatele hõlpsamaks.

(58) Arvestades tehisintellektisüsteemide olemust ning nende kasutamisega potentsiaalselt seotud riske ohutusele ja põhiõigustele, muu hulgas seoses vajadusega tagada reaalsetes oludes tehisintellektisüsteemi toimimise nõuetekohane seire, on otstarbekas näha kasutajatele ette konkreetsed kohustused. Esmajoones peaksid kasutajad kasutama suure riskiga tehisintellektisüsteeme kasutusjuhendi kohaselt ning vastavalt vajadusele tuleks kehtestada teatavad muud kohustused seoses tehisintellektisüsteemide töö seire ja andmete säilitamisega.

(59) Oleks mõistlik eeldada, et tehisintellektisüsteemi kasutaja on füüsiline või juriidiline isik, ametiasutus, ametkond või muud organ, kelle volituste alusel tehisintellektisüsteemi käitatakse, välja arvatud juhul, kui tehisintellektisüsteemi kasutatakse isikliku, mitte kutselise tegevuse jaoks.

(60) Arvestades tehisintellekti väärtusahela keerukust, peaksid asjaomased kolmandad isikud, eriti need, kes tegelevad tarkvara, tarkvaratööriistade ja -komponentide, eeltreenitud mudelite ja andmete müügi ja tarnimisega, või võrguteenuste osutajad tegema vastavalt vajadusele koostööd pakkujate ja kasutajatega, et võimaldada neil täita käesolevast määrusest tulenevaid kohustusi, ja käesoleva määruse alusel loodud pädevate asutustega.

(61) Olulisel kohal on siinjuures standardimine, mis peaks andma pakkujatele tehnilised lahendused käesoleva määruse nõuete täitmiseks. Euroopa Parlamendi ja nõukogu määruses (EL) nr 1025/2012[54] määratletud harmoneeritud standardite järgimine peaks olema pakkujate jaoks vahend, millega tõendada käesoleva määruse nõuete täitmist. Valdkondades, kus harmoneeritud standardid puuduvad või on ebapiisavad, võiks komisjon siiski vastu võtta ühiseid tehnilisi kirjeldusi.

(62) Selleks et tagada suure riskiga tehisintellektisüsteemide usaldusväärsuse kõrge tase, peaksid need süsteemid enne turule laskmist või kasutuselevõtmist läbima vastavushindamise.

(63) Operaatorite koormuse vähendamiseks ja võimaliku dubleerimise vältimiseks on otstarbekas hinnata uue õigusraamistiku lähenemisviisi järgi olemasolevate liidu ühtlustamisõigusaktide kohaldamisalasse kuuluvate suure riskiga

[54] Euroopa Parlamendi ja nõukogu 25. oktoobri 2012. aasta määrus (EL) nr 1025/2012, mis käsitleb Euroopa standardimist ning millega muudetakse nõukogu direktiive 89/686/EMÜ ja 93/15/EMÜ ning Euroopa Parlamendi ja nõukogu direktiive 94/9/EÜ, 94/25/EÜ, 95/16/EÜ, 97/23/EÜ, 98/34/EÜ, 2004/22/EÜ, 2007/23/EÜ, 2009/23/EÜ ja 2009/105/EÜ ning millega tunnistatakse kehtetuks nõukogu otsus 87/95/EMÜ ning Euroopa Parlamendi ja nõukogu otsus nr 1673/2006/EÜ (ELT L 316, 14.11.2012, lk 12).

tehisintellektisüsteemide vastavust käesoleva määruse nõuetele osana kõnealuste õigusaktidega juba ette nähtud vastavushindamisest. Seega ei tohiks käesoleva määruse nõuete kohaldatavus mõjutada uue õigusraamistiku konkreetsete asjaomaste õigusaktide kohaselt tehtava vastavushindamise eriomast loogikat, metoodikat või üldist ülesehitust. Käesoleva määruse ja [masinamääruse] vastastikune mõju kajastab täielikult sellist lähenemisviisi. Masinates turvafunktsioone täitvate tehisintellektisüsteemide riske käsitletakse käesoleva määruse nõuetes, kuid tehisintellektisüsteemi ohutu integreerimine üldisse masinavärki tagatakse [masinamääruse] teatavate konkreetsete nõuetega, et mitte seada ohtu masina kui terviku ohutust. [Masinamääruses] on kasutatud sama tehisintellektisüsteemi määratlust kui käesolevas määruses.

(64) Kuna kutselistel turustamiseelsetel sertifitseerijatel on tooteohutuse valdkonnas laialdasemad kogemused ja kaasnevad riskid on oma olemuselt erinevad, on otstarbekas vähemalt käesoleva määruse kohaldamise algjärgus piirata kolmanda isiku tehtava vastavushindamise kohaldamise ulatust muude kui toodetega seotud suure riskiga tehisintellektisüsteemide puhul. Seepärast peaks selliste süsteemide vastavushindamise üldjuhul tegema pakkuja omal vastutusel; ainsaks erandiks on tehisintellektisüsteemid, mis on mõeldud kasutamiseks isikute biomeetrilise kaugtuvastamise jaoks ja mille puhul tuleks ette näha teavitatud asutuse osalemine vastavushindamises, eeldusel, et sellised süsteemid ei ole keelatud.

(65) Selleks, et isikute biomeetrilises kaugtuvastamises kasutamiseks mõeldud tehisintellektisüsteem saaks läbida kolmanda isiku tehtava vastavushindamise, peaksid riikide pädevad asutused käesoleva määruse alusel määrama teavitatud asutused, tingimusel et need vastavad teatavatele nõuetele eeskätt sõltumatuse, pädevuse ja huvide konflikti puudumise vallas.

(66) Liidu ühtlustamisõigusaktidega reguleeritud toodete olulise muutmise laialdaselt juurdunud mõistega kooskõlas on otstarbekas, et tehisintellektisüsteem läbib uue vastavushindamise iga kord, kui aset leiab muutus, mis võib mõjutada süsteemi vastavust käeoleva määruse nõuetele, või kui muutub süsteemi sihtotstarve. Lisaks sellele tuleb tehisintellektisüsteemidele, mis n-ö õpivad edasi ka pärast turule laskmist või kasutusele võtmist (st nad kohandavad funktsioonide täitmist automaatselt), näha ette õigusnormid, mille kohaselt ei tohiks olla tegemist olulise muutusega, kui pakkuja on algoritmi ja selle töö muutumise eelnevalt kindlaks määranud ja kui seda on vastavushindamise ajal hinnatud.

(67) Suure riskiga tehisintellektisüsteemidel peaks olema CE-märgis, mis näitab nende vastavust käesolevale määrusele, et nad saaksid siseturul vabalt liikuda. Liikmesriigid ei tohiks luua põhjendamatuid tõkkeid käesolevas määruses sätestatud nõuetele vastavate ja CE-märgisega suure riskiga tehisintellektisüsteemide turule laskmisele või kasutusele võtmisele.

(68) Teatavatel tingimustel võib uuenduslike tehnoloogiate kiire kättesaadavus olla inimeste tervise ja ohutuse ning ühiskonna kui terviku jaoks olla äärmiselt tähtis. Seepärast on otstarbekas, et teatavatel erandlikel põhjustel, mis on seotud avaliku julgeoleku või füüsiliste isikute elu ja tervise kaitse ning tööstus- ja kaubandusomandi kaitsega, võiksid liikmesriigid lubada selliste tehisintellektisüsteemide turule laskmist või kasutusele võtmist, mis ei ole vastavushindamist läbinud.

(69) Et hõlbustada tööd, mida komisjon ja liikmesriigid tehisintellekti vallas teevad, ja suurendada avalikkuse jaoks läbipaistvust, peaksid muude kui asjaomaste olemasolevate liidu ühtlustamisõigusaktide kohaldamisalasse kuuluvate toodetega

seotud suure riskiga tehisintellektisüsteemide pakkujad olema kohustatud registreerima oma suure riskiga tehisintellektisüsteemi ELi andmebaasis, mille loob ja mida haldab komisjon. Selle andmebaasi vastutav töötleja peaks olema komisjon vastavalt Euroopa Parlamendi ja nõukogu määrusele (EL) 2018/1725[55]. Et andmebaas oleks kasutuselevõtmisel täielikult toimiv, peaks andmebaasi loomise protseduur hõlmama funktsionaalsete kirjelduste väljatöötamist komisjoni poolt ja sõltumatut auditiaruannet.

(70) Teatavate tehisintellektisüsteemide puhul, mis on mõeldud suhtlema füüsiliste isikutega või sisu looma, võib esineda kellenagi esinemise või pettuse spetsiifilisi riske olenemata sellest, kas süsteemid on liigitatud suure riskiga süsteemideks või mitte. Seepärast peaks nende süsteemide kasutamise suhtes teatavates olukordades kehtima spetsiifilised läbipaistvuskohustused, ilma et see piiraks suure riskiga tehisintellektisüsteemide suhtes kehtivate nõuete ja kohustuste kohaldamist. Esmajoones tuleks füüsilistele isikutele teada anda, et nad suhtlevad tehisintellektisüsteemiga, kui see just ei ole asjaoludest ja kasutamise kontekstist tulenevalt ilmselge. Peale selle tuleks füüsilisi isikuid teavitada, kui nad puutuvad kokku emotsioonide tuvastamise süsteemi või biomeetrilise liigitamise süsteemiga. Selline teave tuleks edastada vormingus, mis on puuetega inimestele juurdepääsetaval kujul. Kui kasutaja kasutab tehisintellektisüsteemi, et luua või manipuleerida kujutisi või audio- või videosisu, mis sarnaneb märgatavalt olemasolevate isikute, kohtade või sündmustega ja võib inimesele ekslikult ehtne näida, peaks kõnealune kasutaja avalikustama, et see sisu on kunstlikult loodud või seda on manipuleeritud, tähistades tehisintellekti väljundi vastavalt ja avalikustades selle tehisliku päritolu.

(71) Tehisintellekt on kiirelt arenev tehnoloogiaharu, mis eeldab uudset regulatiivset järelevalvet ja turvalist katsetamisruumi, aga ka seda, et tagatud oleks vastutustundlik innovatsioon ning asjakohaste kaitsemeetmete ja riskileevendusmeetmete integreerimine. Innovatsioonisõbraliku, tulevikukindla ja häirete suhtes vastupanuvõimelise õigusraamistiku tagamiseks tuleks ühe või mitme liikmesriigi pädevaid asutusi julgustada looma tehisintellekti regulatsiooni testkeskkondi, mis hõlbustaksid innovatiivsete tehisintellektisüsteemide arendamist ja testimist range regulatiivse järelevalve all, enne kui need süsteemid turule lastakse või muul moel kasutusele võetakse.

(72) Regulatsiooni testkeskkondade eesmärk peaks olema edendada tehisintellekti alast innovatsiooni kontrollitud eksperimenteerimis- ja katsekeskkonna loomisega arendus- ja turustamiseelses etapis, et tagada innovatiivsete tehisintellektisüsteemide vastavus käesolevale määrusele ning muudele asjakohastele liidu ja liikmesriikide õigusaktidele; parandada novaatorite õiguskindlust ja pädevate asutuste järelevalvet ning arusaamist tehisintellekti kasutamise võimalustest, tekkivatest riskidest ja mõjudest ning kiirendada turulepääsu muu hulgas sellega, et kaotatakse väikeseid ja keskmise suurusega ettevõtjaid ja idufirmasid piiravad tõkked. Selleks, et tagada ühetaoline rakendamine kogu liidus ja mastaabisääst, on otstarbekas kehtestada regulatsiooni katsetuskeskkondade rakendamise ühised eeskirjad ja katsetuskeskkondade järelevalvega tegelevate asjaomaste ametiasutusete vahelise koostöö raamistik. Käesoleva määrusega tuleks ette näha õiguslik alus muul otstarbel kogutud isikuandmete kasutamiseks, et arendada tehisintellekti regulatsiooni

[55] Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta määrus (EL) 2016/679 füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus) (ELT L 119, 4.5.2016, lk 1).

testkeskkonnas avalikes huvides teatavaid tehisintellektisüsteeme kooskõlas määruse (EL) 2016/679 artikli 6 lõikega 4 ja määruse (EL) 2018/1725 artikliga 6 ning ilma, et see piiraks direktiivi (EL) 2016/680 artikli 4 lõike 2 kohaldamist. Testkeskkonnas osalejad peaksid tagama asjakohased kaitsemeetmed ja tegema koostööd pädevate asutustega, järgides muu hulgas nende juhendeid ning tegutsedes viivitusteta ja heas usus, et leevendada ohutust ja põhiõigusi ähvardavaid suuri riske, mis võivad testimiskeskkonnas arendustegevuse ja eksperimenteerimise käigus tekkida. Kui pädevad asutused otsustavad, kas määrata haldustrahv määruse 2016/679 artikli 83 lõike 2 ja direktiivi 2016/680 artikli 57 alusel, tuleks osalejate käitumist testkeskkonnas arvesse võtta.

(73) Innovatsiooni edendamiseks ja kaitsmiseks on oluline pöörata erilist tähelepanu väikepakkujate ja tehisintellektisüsteemide kasutajate huvidele. Liikmesriigid peaksid selle eesmärgi nimel välja töötama nimetatud operaatoritele suunatud algatusi, muu hulgas teadlikkuse suurendamise ja teabe edastamise teemal. Ühtlasi tuleb väikepakkujate konkreetsete huvide ja vajadustega arvestada, kui teavitatud asutused panevad paika vastavushindamise tasud. Kohustusliku dokumentatsiooni ja ametiasutustega suhtlemisega seotud tõlkekulud võivad osutuda pakkujate ja muude operaatorite jaoks märkimisväärseks, eriti juhul, kui tegemist on väiksemate ettevõtjatega. Liikmesriigid peaksid võimaluse korral tagama, et üks nende poolt asjaomaste pakkujate dokumentatsiooni ja operaatoritega suhtlemise jaoks kindlaks määratud ja neile vastuvõetavatest keeltest on keel, mis on üldjoontes arusaadav võimalikult suurele arvule piiriülestele kasutajatele.

(74) Selleks, et minimeerida rakendamisega seotud riske, mis tulenevad teadmiste ja oskusteabe puudumisest turul, ja muuta käesolevast määrusest tulenevate kohustuste täitmine pakkujate ja teavitatud asutuste jaoks hõlpsamaks, peaksid tehisintellekti nõudeplatvorm, Euroopa digitaalse innovatsiooni keskused ning komisjoni ja liikmesriikide poolt riigi või ELi tasandil loodud testimis- ja eksperimenteerimisrajatised võimaluse korral aitama kaasa käesoleva määruse rakendamisele. Need asutused võivad pakkuda teavitatud asutustele ja pakkujatele oma vastavate ülesannete ja pädevusvaldkondade piires eeskätt tehnilist ja teaduslikku tuge.

(75) On otstarbekas, et komisjon hõlbustab võimaluste piires asjaomaste liidu ühtlustamisõigusaktide kohaselt loodud või akrediteeritud ning nende liidu ühtlustamisõigusaktide kohaldamisalasse kuuluvate toodete või seadmete vastavushindamise raames ülesandeid täitvate organite, rühmade või laborite juurdepääsu testimis- ja eksperimenteerimisrajatistele. Eeskätt kehtib see meditsiiniseadmete valdkonna eksperdirühmade, eksperdilaborite ja referentlaborite kohta vastavalt määrusele (EL) 2017/745 ja määrusele (EL) 2017/746.

(76) Et hõlbustada käesoleva määruse sujuvat, tulemuslikku ja ühtset rakendamist, tuleks luua Euroopa tehisintellekti nõukoda. Nõukoda peaks vastutama mitmesuguste nõustamisalaste ülesannete eest, sh arvamuste, soovituste, nõuannete või juhendite väljaandmine käesoleva määruse rakendamisega seotud küsimustes, muu hulgas tehniliste kirjelduste või olemasolevate standardite kohta, mis puudutavad käesoleva määrusega kehtestatud nõudeid, ning komisjonile nõu ja abi andmine konkreetsetes tehisintellektiga seotud küsimustes.

(77) Liikmesriikidel on käesoleva määruse kohaldamisel ja täitmise tagamisel tähtis roll. Seoses sellega peaks iga liikmesriik määrama ühe või mitu riigi pädevat asutust tegelema käesoleva määruse kohaldamise ja rakendamise järelevalvega. Selleks, et

suurendada liikmesriikide töökorralduse tõhusust ja luua ametlik kontaktpunkt suhtlemiseks üldsuse ja muude vastaspooltega liikmesriigi ja liidu tasandil, tuleks igas liikmesriigis määrata üks riigi ametiasutus riigi järelevalveasutuseks.

(78) Tagamaks, et suure riskiga tehisintellektisüsteemide pakkujad saavad võtta oma süsteemide ja projekteerimis- ja arendusprotsessi parandamiseks arvesse suure riskiga tehisintellektisüsteemide kasutamise käigus saadud kogemusi või võtta õigeaegselt võimalikke parandusmeetmeid, peaks kõigil pakkujatel olema sisse seatud turustamisjärgse seire süsteem. Selline süsteem on oluline ka selleks, et tõhusamalt ja õigeaegsemalt saaks tegeleda riskidega, mis tulenevad suure riskiga tehisintellektisüsteemidest, mis n-ö õpivad edasi ka pärast turule laskmist või kasutusele võtmist. Seoses sellega tuleks pakkujatelt nõuda ka seda, et neil oleks olemas süsteem, et teatada asjaomastele asutustele mis tahes tõsistest intsidentidest või sellest, kui tehisintellektisüsteemi kasutamise tõttu on rikutud põhiõigusi kaitsvat siseriiklikku või liidu õigust.

(79) Selleks et kindlustada liidu ühtlustamisõigusaktide hulka kuuluvas käesolevas määruses sätestatud nõuete ja kohustuste täitmise asjakohane ja tulemuslik tagamine, tuleks määrusega (EL) 2019/1020 kehtestatud toodete turujärelevalve ja nõuetele vastavuse süsteemi kohaldada täies ulatuses. Põhiõiguste kaitset käsitleva liidu õiguse järelevalvega tegelevatel riigi ametiasutustel või organitel, sh võrdõiguslikkust edendavatel asutustel peaks olema juurdepääs käesoleva määruse kohaselt loodud dokumentatsioonile, kui see on vajalik nende ülesannete täitmiseks.

(80) Finantsteenuseid käsitlevad liidu õigusaktid sisaldavad sisemise juhtimissüsteemi ja riskihalduse kohta käivaid õigusnorme ja nõudeid, mida kohaldatakse reguleeritud finantsasutuste suhtes nende teenuste pakkumise käigus, kaasa arvatud siis, kui nad kasutavad tehisintellektisüsteeme. Käesolevast määrusest tulenevate kohustuste ja finantsteenuseid käsitlevate liidu õigusaktide asjaomaste õigusnormide ja nõuete sidusa kohaldamise ja täitmise tagamiseks tuleks finantsteenuseid käsitlevate õigusaktide järelevalve ja täitmise tagamise eest vastutavad ametiasutused, sh vajaduse korral Euroopa Keskpank, määrata pädevateks asutusteks, kes tegelevad käesoleva määruse rakendamise järelevalvega, sealhulgas turujärelevalvega, seoses reguleeritud ja järelevalve all olevate finantsasutuste pakutavate või kasutatavate tehisintellektisüsteemidega. Et veelgi suurendada käesoleva määruse ja Euroopa Parlamendi ja nõukogu direktiivi 2013/36/EL[56] alusel reguleeritud krediidiasutuste suhtes kohaldatavate õigusnormide sidusust, on ühtlasi otstarbekas integreerida vastavushindamismenetlus ja pakkujate mõned riskijuhtimise, turustamisjärgse seire ja dokumentatsiooniga seotud menetluslikud kohustused direktiivi 2013/36/EL kohaste olemasolevate kohustuste ja menetlustega. Kattuvuse vältimiseks tuleks ette näha ka piiratud erandid seoses pakkujate kvaliteedijuhtimissüsteemidega ja seirekohustusega, mis on pandud suure riskiga tehisintellektisüsteemide kasutajatele, niivõrd kuivõrd neid kohaldatakse direktiiviga 2013/36/EL reguleeritud krediidiasutuste suhtes.

(81) Muude tehisintellektisüsteemide kui suure riskiga tehisintellektisüsteemide arendamine kooskõlas käesoleva määruse nõuetega võib tuua kaasa usaldusväärse tehisintellekti laialdasema kasutamise liidus. Muude kui suure riskiga

[56] Euroopa Parlamendi ja nõukogu 26. juuni 2013. aasta direktiiv 2013/36/EL, mis käsitleb krediidiasutuste tegevuse alustamise tingimusi ning krediidiasutuste ja investeerimisühingute usaldatavusnõuete täitmise järelevalvet, millega muudetakse direktiivi 2002/87/EÜ ning millega tunnistatakse kehtetuks direktiivid 2006/48/EÜ ja 2006/49/EÜ (ELT L 176, 27.6.2013, lk 338).

tehisintellektisüsteemide pakkujaid tuleks julgustada koostama käitumisjuhendeid, mille eesmärk on soodustada suure riskiga tehisintellektisüsteemide suhtes kohaldatavate kohustuslike nõuete vabatahtlikku kohaldamist. Samuti tuleks pakkujaid julgustada kohaldama vabatahtlikult täiendavaid nõudeid, mis on seotud näiteks keskkonnasäästlikkusega, juurdepääsetavusega puuetega inimeste jaoks, sidusrühmade osalemisega tehisintellektisüsteemide projekteerimises ja arendamises ning arendusmeeskondade mitmekesisusega. Komisjon võib töötada välja algatusi, sh valdkondlikke algatusi, et aidata vähendada tehnilisi tõkkeid, mis takistavad tehisintellekti arendamise jaoks toimuvat piiriülest andmevahetust, keskendudes muu hulgas andmetele juurdepääsu taristule ning eri andmeliikide semantilisele ja tehnilisele koostalitlusvõimele.

(82) On oluline, et tehisintellektisüsteemid, mis on seotud toodetega, mis ei ole käesoleva määruse alusel suure riskiga ja mis seega ei pea vastama käesolevaga sätestatud nõuetele, oleksid siiski ohutud, kui need turule lastakse või kasutusele võetakse. Selle eesmärgi saavutamiseks kohaldatakse turvaabinõuna Euroopa Parlamendi ja nõukogu direktiivi 2001/95/EÜ[57].

(83) Pädevate asutuste usaldusliku ja konstruktiivse koostöö tagamiseks liidu ja riikide tasandil peaksid kõik käeoleva määruse kohaldamises osalejad austama oma ülesannete täitmise käigus saadud teabe ja andmete konfidentsiaalsust.

(84) Liikmesriigid peaksid võtma kõik vajalikud meetmed, et tagada käesoleva määruse sätete rakendamine, sealhulgas kehtestades tõhusad, proportsionaalsed ja hoiatavad karistused nende rikkumise eest. Teatavate konkreetsete rikkumiste puhul peaksid liikmesriigid võtma arvesse käesolevas määruses sätestatud piire ja kriteeriume. Euroopa Andmekaitseinspektoril peaks olema õigus määrata trahve käesoleva määruse kohaldamisalasse kuuluvatele liidu institutsioonidele, asutustele ja organitele.

(85) Tagamaks, et õigusraamistikku saab vajaduse korral kohandada, tuleks komisjonile delegeerida õigus võtta vastu õigusakte kooskõlas ELi toimimise lepingu artikliga 290, et muuta I lisas osutatud meetodeid ja lähenemisviise tehisintellektisüsteemide defineerimiseks, II lisas loetletud liidu ühtlustamisõigusakte, III lisas loetletud suure riskiga tehisintellektisüsteeme, IV lisas loetletud tehnilist dokumentatsiooni käsitlevaid sätteid, V lisas esitatud ELi vastavusdeklaratsiooni sisu, VI ja VII lisas esitatud vastavushindamismenetlusi käsitlevaid sätteid ja sätteid, millega pannakse paika need suure riskiga tehisintellektisüsteemid, mille suhtes tuleks kohaldada kvaliteedijuhtimissüsteemi ja tehnilise dokumentatsiooni hindamisel põhinevat vastavushindamist. On eriti oluline, et komisjon korraldaks ettevalmistava töö käigus läbi asjakohaseid konsultatsioone, sealhulgas ekspertide tasandil, ja et kõnealused konsultatsioonid toimuksid kooskõlas 13. aprilli 2016. aasta institutsioonidevahelises parema õigusloome kokkuleppes[58] sätestatud põhimõtetega. Eelkõige selleks, et tagada delegeeritud õigusaktide ettevalmistamises võrdne osalemine, saavad Euroopa Parlament ja nõukogu kõik dokumendid liikmesriikide ekspertidega samal ajal ning nende ekspertidel on pidev juurdepääs komisjoni eksperdirühmade koosolekutele, millel arutatakse delegeeritud õigusaktide ettevalmistamist.

---

57 Euroopa Parlamendi ja nõukogu 3. detsembri 2001. aasta direktiiv 2001/95/EÜ üldise tooteohutuse kohta (EÜT L 11, 15.1.2002, lk 4).

58 ELT L 123, 12.5.2016, lk 1.

(86) Selleks et tagada käesoleva määruse ühetaolised rakendamistingimused, tuleks komisjonile anda rakendamisvolitused. Neid volitusi tuleks teostada kooskõlas Euroopa Parlamendi ja nõukogu määrusega (EL) nr 182/2011[59].

(87) Liikmesriigid ei suuda käesoleva määruse eesmärki piisalt saavutada, küll aga saab neid meetmete ulatuse ja toime tõttu paremini saavutada liidu tasandil, ning seega võib liit võtta meetmeid kooskõlas ELi lepingu artiklis 5 sätestatud subsidiaarsuse põhimõttega. Kõnealuses artiklis sätestatud proportsionaalsuse põhimõtte kohaselt ei lähe käesolev määrus nimetatud eesmärgi saavutamiseks vajalikust kaugemale.

(88) Käesolevat määrust tuleks kohaldada alates ... [*väljaannete talitus – palun sisestada artiklis 85 sätestatud kuupäev*]. Juhtimise ja vastavushindamissüsteemiga seotud taristu peaks hakkama toimima siiski juba enne nimetatud kuupäeva ning seepärast tuleks teavitatud asutusi ja juhtimisstruktuuri käsitlevaid sätteid kohaldada alates ... [*väljaannete talitus – palun sisestada kuupäev: kolm kuud pärast käesoleva määruse jõustumist*]. Lisaks peaksid liikmesriigid nägema ette õigusnormid karistuste, kaasa arvatud haldustrahvide kohta, teatama neist komisjonile ning tagama, et need õigusnormid on käesoleva määruse kohaldamise kuupäevaks nõuetekohaselt ja tulemuslikult rakendatud. Seepärast tuleks karistusi käsitlevaid sätteid hakata kohaldama alates [*väljaannete talitus, palun sisestage kuupäev: kaksteist kuud pärast käesoleva määruse jõustumist*]

(89) Vastavalt määruse (EL) nr 2018/1725 artikli 42 lõikele 2 on konsulteeritud Euroopa Andmekaitseinspektori ja Euroopa Andmekaitsenõukoguga, kes esitasid oma arvamuse [...],

ON VASTU VÕTNUD KÄESOLEVA MÄÄRUSE:

I JAOTIS

ÜLDSÄTTED

Artikkel 1
Reguleerimisese

Käesoleva määrusega nähakse ette:

(a) ühtlustatud õigusnormid, mis reguleerivad tehisintellektisüsteemide turule laskmist, kasutusele võtmist ja kasutamist liidus;

(b) teatavate tehisintellekti kasutusviiside keelustamine;

(c) erinõuded suure riskiga tehisintellektisüsteemidele ja selliste süsteemide operaatorite kohustused;

(d) ühtlustatud läbipaistvusnormid füüsiliste isikutega suhtlemiseks mõeldud tehisintellektisüsteemide, emotsioonide tuvastamise süsteemide ja biomeetrilise kategooriatesse jaotamise süsteemide ning pildi-, audio- või videosisu loomiseks või töötlemiseks kasutatavate tehisintellektisüsteemide jaoks;

[59] Euroopa Parlamendi ja nõukogu 16. veebruari 2011. aasta määrus (EL) nr 182/2011, millega kehtestatakse eeskirjad ja üldpõhimõtted, mis käsitlevad liikmesriikide läbiviidava kontrolli mehhanisme, mida kohaldatakse komisjoni rakendamisvolituste teostamise suhtes (ELT L 55, 28.2.2011, lk 13).

(e) turuseire ja -järelevalve normid.

Artikkel 2
Kohaldamisala

1. Käesolevat määrust kohaldatakse järgmise suhtes:

   (a) pakkujad, kes tegelevad liidus tehisintellektisüsteemide liidus turule laskmise või kasutusele võtmisega olenemata sellest, kas pakkuja tegevuskoht on liidus või kolmandas riigis;

   (b) liidus asuvad tehisintellektisüsteemide kasutajad;

   (c) kolmandates riikides asuvad tehisintellektisüsteemide pakkujad ja kasutajad, kui süsteemi väljundit kasutatakse liidus.

2. Suure riskiga tehisintellektisüsteemide suhtes, mis on toodete või süsteemide turvakomponendid või mis on ise tooted või süsteemid, mis kuuluvad järgmiste õigusaktide kohaldamisalasse, kohaldatakse üksnes käesoleva määruse artiklit 84:

   (a) määrus (EÜ) nr 300/2008;

   (b) määrus (EL) nr 167/2013;

   (c) määrus (EL) nr 168/2013;

   (d) direktiiv 2014/90/EL;

   (e) direktiiv (EL) 2016/797;

   (f) määrus (EL) 2018/858;

   (g) määrus (EL) 2018/1139;

   (h) määrus (EL) 2019/2144.

3. Käesolevat määrust ei kohaldata tehisintellektisüsteemide suhtes, mis on välja töötatud või mida kasutatakse üksnes sõjalisel otstarbel.

4. Käesolevat määrust ei kohaldata kolmanda riigi ametiasutuste ega vastavalt lõikele 1 käesoleva määruse kohaldamisalasse kuuluvate rahvusvaheliste organisatsioonide suhtes, kui need asutused või organisatsioonid kasutavad tehisintellektisüsteeme liidu või ühe või mitme liikmesriigiga õiguskaitse ja õigusalase koostöö jaoks sõlmitud rahvusvaheliste lepingute raames.

5. Käesolev määrus ei mõjuta Euroopa Parlamendi ja nõukogu direktiivi 2000/31/EÜ[60] II peatüki 4. jao vahendajatest teenuseosutajate vastutust käsitlevate sätete [*asendatakse digiteenuste õigusakti vastavate sätetega*] kohaldamist.

Artikkel 3
Mõisted

Käesolevas määruses kasutatakse järgmisi mõisteid:

(1) „tehisintellektisüsteem“ – tarkvara, mille arendamiseks on kasutatud üht või mitut I lisas loetletud tehnoloogiat või lähenemisviisi ja mis võib teatavate inimese kindlaks

[60] Euroopa Parlamendi ja nõukogu 8. juuni 2000. aasta direktiiv 2000/31/EÜ infoühiskonna teenuste teatavate õiguslike aspektide, eriti elektroonilise kaubanduse kohta siseturul (direktiiv elektroonilise kaubanduse kohta) (EÜT L 178, 17.7.2000, lk 1).

määratud eesmärkide jaoks luua väljundeid, näiteks sisu, prognoose, soovitusi või otsuseid, mis mõjutavad keskkondi, millega nad suhtlevad;

(2) „pakkuja“ – füüsiline või juriidiline isik, ametiasutus, ametkond või muu organ, kes töötab välja tehisintellektisüsteemi või laseb tehisintellektisüsteemi välja töötada, et see turule lasta või kasutusele võtta oma nime või kaubamärgi all kas tasu eest või tasuta;

(3) „väikepakkuja“ – pakkuja, kes on mikro- või väikeettevõtja komisjoni soovituse 2003/361/EÜ tähenduses[61];

(4) „kasutaja“ – füüsiline või juriidiline isik, ametiasutus, ametkond või muu organ, kes kasutab tehisintellektisüsteemi oma volituste alusel, välja arvatud juhul, kui tehisintellektisüsteemi kasutatakse isikliku, mitte kutselise tegevuse jaoks;

(5) „volitatud esindaja“ – liidus asuv füüsiline või juriidiline isik, kes on saanud tehisintellektisüsteemi pakkujalt kirjaliku volituse täita käesoleva määrusega kehtestatud kohustusi ja sooritada menetlusi tema nimel;

(6) „importija“ – liidus asuv füüsiline või juriidiline isik, kes laseb turule või võtab kasutusele väljaspool liitu asuva füüsilise või juriidilise isiku nime või kaubamärki kandva tehisintellektisüsteemi;

(7) „turustaja“ – füüsiline või juriidiline isik tarneahelas, välja arvatud pakkuja või importija, kes teeb tehisintellektisüsteemi liidu turul kättesaadavaks ilma selle omadusi mõjutamata;

(8) „operaator“ – pakkuja, kasutaja, volitatud esindaja, importija ja turustaja;

(9) „turule laskmine“ – tehisintellektisüsteemi liidu turul esmakordselt kättesaadavaks tegemine;

(10) „turul kättesaadavaks tegemine“ – tehisintellektisüsteemi tasu eest või tasuta tarnimine liidu turule kaubandustegevuse käigus kas turustamiseks või kasutamiseks;

(11) „kasutusele võtmine“ – tehisintellektisüsteemi tarnimine esmakordseks kasutamiseks otse kasutajale või oma tarbeks, et kasutada seda sihtotstarbeliselt liidu turul;

(12) „sihtotstarve“ – 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;

(13) „mõistlikult prognoositav väärkasutamine“ – tehisintellektisüsteemi kasutamine viisil, mis ei ole kooskõlas selle sihtotstarbega, kuid mis võib tuleneda põhjendatult prognoositavast inimkäitumisest või interaktsioonist muude süsteemidega;

(14) „toote või süsteemi turvakomponent“ – toote või süsteemi komponent, mis täidab selle toote või süsteemi ohutusfunktsiooni või mille tõrge või talitlushäire ohustab inimeste tervist ja ohutust või vara;

(15) „kasutusjuhend“ – teave, mille pakkuja esitab, et teavitada kasutajat eeskätt tehisintellektisüsteemi kasutusotstarbest ja nõuetekohasest kasutamisest, kaasa arvatud konkreetsest geograafilisest, käitumuslikust ja funktsionaalsest raamistikust, milles kasutamiseks suure riskiga tehisintellektisüsteem on ette nähtud;

---

[61] Komisjoni 6. mai 2003. aasta soovitus mikroettevõtjate ning väikeste ja keskmise suurusega ettevõtjate määratlemise kohta (ELT L 124, 20.5.2003, lk 36).

(16) „tehisintellektisüsteemi tagasikutsumine“ – mistahes meede, mille eesmärk on saavutada kasutajatele kättesaadavaks tehtud tehisintellektisüsteemi tagastamine pakkujale;

(17) „tehisintellektisüsteemi turult kõrvaldamine“ – mistahes meede, mille eesmärk on hoida ära tehisintellektisüsteemi turustamist, esitlemist ja pakkumist;

(18) „tehisintellektisüsteemi toimimine“ – tehisintellektisüsteemi suutlikkus täita talle seatud sihtotstarvet;

(19) „teavitav asutus“ – riigi ametiasutus, kes vastutab vastavushindamisasutuste hindamise, määramise ja neist teavitamise ning nende seire jaoks vajalike menetluste väljatöötamise ja läbiviimise eest;

(20) „vastavushindamine“ protsess, mille käigus kontrollitakse, kas tehisintellektisüsteemi kohta käesoleva määruse III jaotise 2. peatükis sätestatud nõuded on täidetud;

(21) „vastavushindamisasutus“ – asutus, kes teeb kolmanda isikuna vastavushindamise toiminguid, sealhulgas testimist, sertifitseerimist ja kontrollimist;

(22) „teavitatud asutus“ käesoleva määruse ja liidu muude asjaomaste ühtlustamisalaste õigusaktide kohaselt määratud vastavushindamisasutus;

(23) „oluline muudatus“ – tehisintellektisüsteemis pärast selle turule laskmist või kasutusele võtmist tehtud muudatus, mis mõjutab tehisintellektisüsteemi vastavust käesoleva määruse III jaotise 2. peatükis sätestatud nõuetele või mille tulemusena muutub kasutusotstarve, mida silmas pidades on tehisintellektisüsteemi hinnatud;

(24) „CE-vastavusmärgis“ või „CE-märgis“ – märgis, millega pakkuja annab teada, et tehisintellektisüsteem vastab käesoleva määruse III jaotise 2. peatükis ja muudes kohaldatavates toodete turustamise tingimusi ühtlustavates liidu õigusaktides (edaspidi „liidu ühtlustamisõigusaktid“) sätestatud märgise paigaldamist käsitlevatele nõuetele;

(25) „turustamisjärgne seire“ – igasugune tehisintellektisüsteemi pakkuja tegevus, et proaktiivselt koguda ja läbi vaadata tema poolt turule lastud või kasutusele võetud tehisintellektisüsteemide kasutamise käigus saadud kogemusi, eesmärgiga teha kindlaks juhud, kui tuleb viivitamata võtta vajalikke parandus- või ennetusmeetmeid;

(26) „turujärelevalveasutus“ – riigi ametiasutus, kes teeb toiminguid ja võtab meetmeid vastavalt määrusele (EL) 2019/1020;

(27) „harmoneeritud standard“ – määruse (EL) nr 1025/2012 artikli 2 lõike 1 punktis c määratletud Euroopa standard;

(28) „ühtne kirjeldus“ – dokument, v.a standard, mis sisaldab tehnilisi lahendusi, mille abil täita teatavaid käesoleva määrusega kehtestatud nõudeid ja kohustusi;

(29) „treeningandmed“ – andmed, mida kasutatakse tehisintellektisüsteemi treenimiseks läbi õpiparameetrite sobituse, mh närvivõrgu kaaludega;

(30) „valideerimisandmed“ – andmed, mida kasutatakse treenitud tehisintellektisüsteemi hindamiseks ning selle mitteõpitavate parameetrite ja õppimisprotsessi reguleerimiseks, muu hulgas selleks, et hoiduda ülesobitamisest; sealjuures võib valideerimisandmestik olla kas eraldi andmestik või treeningandmestiku osa kindlaksmääratud või muutuva jaotuse alusel;

(31) „testandmed“ – andmed, mida kasutatakse sõltumatu hinnangu andmiseks treenitud ja valideeritud tehisintellektisüsteemile, et kinnitada selle süsteemi toimimise eeldustekohasust, enne kui süsteem lastakse turule või võetakse kasutusele;

(32) „sisendandmed“ – andmed, mis esitatakse tehisintellektisüsteemile või mille tehisintellektisüsteem vahetult saab ning mille põhjal süsteem genereerib väljundi;

(33) „biomeetrilised andmed“ – konkreetse tehnilise töötlemise abil saadavad isikuandmed füüsilise isiku füüsiliste, füsioloogiliste ja käitumuslike omaduste kohta, mis võimaldavad kõnealust füüsilist isikut kordumatult tuvastada või kinnitavad selle füüsilise isiku tuvastamist, näiteks näokujutis ja sõrmejälgede andmed;

(34) „emotsioonituvastussüsteem“ – tehisintellektisüsteem, mille eesmärk on tuvastada või tuletada füüsiliste isikute emotsioone või kavatsusi nende biomeetriliste andmete põhjal;

(35) „biomeetrilise liigitamise süsteem“ – tehisintellektisüsteem, mille eesmärk on jagada füüsilisi isikuid nende biomeetriliste andmete, näiteks soo, vanuse, juuksevärvi, silmade värvi, tätoveeringute, etnilise päritolu või seksuaalse või poliitilise sättumuse põhjal teatavatesse kategooriatesse;

(36) „biomeetrilise kaugtuvastamise süsteem“ – tehisintellektisüsteem, mille eesmärk on tuvastada füüsilisi isikuid eemalt, võrreldes isiku biomeetrilisi andmeid võrdlusbaasis sisalduvate biomeetriliste andmetega, ilma et tehisintellektisüsteemi kasutaja teaks ette, kas see isik on ise kohal ja kas teda on võimalik tuvastada;

(37) „reaalajas toimuva biomeetrilise kaugtuvastamise süsteem“ – biomeetrilise kaugtuvastamise süsteem, milles biomeetriliste andmete hõive, võrdlemine ja tuvastamine toimub ilma märkimisväärse viivituseta. Lisaks viivitamatule tuvastamisele hõlmab see ka piiratud lühikesi viivitusi, et vältida kõrvalehoidmist;

(38) „tagantjärele toimuva biomeetrilise kaugtuvastamise süsteem“ – biomeetrilise kaugtuvastamise süsteem, mis ei ole reaalajas toimuva biomeetrilise kaugtuvastamise süsteem;

(39) „avalikult juurdepääsetav ruum“ – füüsiline koht, millele üldsusel on juurdepääs, olenemata sellest, kas kehtivad teatavad juurdepääsutingimused;

(40) „õiguskaitseasutus“ –

(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

(b) muu asutus või üksus, kes teostab liikmesriigi õiguse kohaselt 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;

(41) „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 ennetamiseks;

(42) „riiklik järelevalveasutus“ – ametiasutus, kellele liikmesriik paneb vastutuse käesoleva määruse rakendamise ja kohaldamise eest, liikmesriigile usaldatud

toimingute koordineerimise eest, komisjoniga suhtluses ühtse kontaktpunktina tegutsemise eest ja liikmesriigi esindamise eest Euroopa tehisintellekti nõukojas;

(43) „riigi pädev asutus“ – riiklik järelevalveasutus, teavitav asutus ja turujärelevalveasutus;

(44) „tõsine intsident“ – juhtum, mis otseselt või kaudselt põhjustab, võis põhjustada või võib põhjustada ühe järgmistest tagajärgedest:

(a) inimese surm või tõsine kahju inimese tervisele, varale või keskkonnale;

(b) elutähtsa taristu juhtimise ja käitamise tõsine ja pöördumatu katkemine.

Artikkel 4
I lisa muutmine

Komisjonil on õigus võtta kooskõlas artikliga 73 vastu delegeeritud õigusakte, et muuta I lisas esitatud meetodite ja lähenemisviiside loetelu ajakohastamaks seda vastavalt turu ja tehnika arengule, lähtudes omadustest, mis sarnanevad seal loetletud tehnoloogiate ja lähenemisviisidega.

II JAOTIS

TEHISINTELLEKTI KEELATUD KASUTUSVIISID

Artikkel 5

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, et oluliselt moonutada isiku käitumist viisil, mis põhjustab või tõenäoliselt põhjustab sellele või mõnele teisele isikule füüsilist või psühholoogilist kahju;

(b) selliste tehisintellektisüsteemide turule laskmine, kasutusele võtmine või kasutamine, mis kasutavad ära konkreetse isikute rühma mis tahes haavatavusi, mis tulenevad nende vanusest või füüsilise või vaimse tervise häirest, et oluliselt moonutada sellesse rühma kuuluva isiku käitumist viisil, mis põhjustab või tõenäoliselt põhjustab sellele või mõnele teisele isikule füüsilist või psühholoogilist kahju;

(c) selliste tehisintellektisüsteemide turule laskmine, kasutusele võtmine või kasutamine ametiasutuste poolt või nende nimel, et hinnata või liigitada füüsiliste isikute usaldusväärsust teatava aja jooksul, lähtudes nende sotsiaalsest käitumisest või teadaolevatest või prognoositud iseloomulikest või isikuomadustest, kusjuures ühiskondliku reitingu tulemuseks on üks või mõlemad järgmisest:

i) teatavaid füüsilisi isikuid või füüsiliste 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 füüsiliste isikute rühmi kahjustav või nende suhtes ebasoodne kohtlemine, mis ei ole põhjendatud või on

ebaproportsionaalne võrreldes nende sotsiaalse käitumise või selle kaalukusega;

(d) avalikult juurdepääsetavas ruumis reaalajas 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 võimalike kuriteoohvrite, kaasa arvatud kadunud laste, sihipärane otsimine;

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

iii) nõukogu raamotsuse 2002/584/JSK[62] artikli 2 lõikes 2 osutatud kuriteo toimepanija või sellises kuriteos kahtlustatava avastamine, tema asukohta kindlaks tegemine, tema tuvastamine või vastutusele võtmine, kui tegemist on kuriteoga, mille eest karistatakse asjaomases liikmesriigis vabadusekaotuse või vabadust piirava julgeolekumeetmega, mille maksimaalne pikkus on vähemalt kolm aastat, nagu selle liikmesriigi õigusaktides kindlaks määratud.

2. Kui reaalajas toimuva biomeetrilise kaugtuvastamise süsteemi kasutatakse avalikult juurdepääsetavas ruumis õiguskaitse jaoks ükskõik millisel lõike 1 punktis d osutatud eesmärgil, 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 kasutata;

(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 lõike 1 punktis d osutatud eesmärgil olema vastavuses kasutamise suhtes kehtivate vajalike ja proportsionaalsete kaitsemeetmete ja tingimustega ning seda eeskätt ajaliste, geograafiliste ja isikutega seotud piirangute osas.

3. Lõike 1 punkti d ja lõike 2 puhul on reaalajas toimuva biomeetrilise kaugtuvastamise süsteemi igaks kasutamiseks avalikult juurdepääsetavas ruumis vaja eelnevat luba, mille annab selle liikmesriigi õigusasutus või sõltumatu haldusasutus, kus kasutamine hakkab toimuma, ja mis antakse põhjendatud taotluse põhjal kooskõlas lõikes 4 osutatud üksikasjalike siseriiklike õigusnormidega. Nõuetekohaselt põhjendatud kiireloomulistel juhtudel võib siiski hakata süsteemi kasutama ilma loata ja loa võib taotleda alles kasutamise ajal või pärast seda.

Pädev õigus- või haldusasutus annab loa üksnes juhul, kui on talle esitatud objektiivsete tõendite või selgete asjaolude valguses veendunud, et kõnealuse reaalajas toimuva biomeetrilise kaugtuvastamise süsteemi kasutamine on vajalik ja proportsionaalne mõne lõike 1 punktis d täpsustatud ja taotluses nimetatud eesmärgi

[62] Nõukogu 13. juuni 2002. aasta raamotsus 2002/584/JSK Euroopa vahistamismääruse ja liikmesriikidevahelise üleandmiskorra kohta (EÜT L 190, 18.7.2002, lk 1).

saavutamiseks. Pädev õigus- või haldusasutus teeb taotluse kohta otsuse, võttes arvesse lõikes 2 osutatud elemente.

4. Liikmesriik võib otsustada näha ette võimaluse osaliselt või täielikult lubada reaalajas toimuva biomeetrilise kaugtuvastamise süsteemi kasutamist avalikult juurdepääsetavas ruumis õiguskaitse jaoks lõike 1 punktis d ning lõigetes 2 ja 3 loetletud piirides ja tingimustel. Selline liikmesriik kehtestab oma siseriiklikus õiguses lõikes 3 osutatud lubade taotlemise, andmise ja kasutamise ning nende lubadega seotud järelevalve jaoks vajalikud üksikasjalikud õigusnormid. Kõnealustes õigusnormides tuleb täpsustada, milliste lõike 1 punktis d loetletud eesmärkide, sealhulgas milliste selle punkti alapunktis iii osutatud kuritegude puhul võib anda pädevatele asutustele loa kasutada neid süsteeme õiguskaitse jaoks.

III JAOTIS

SUURE RISKIGA TEHISINTELLEKTISÜSTEEMID

1. PEATÜKK

TEHISINTELLEKTISÜSTEEMI LIIGITAMINE SUURE RISKIGA TEHISINTELLEKTISÜSTEEMIKS

Artikkel 6
Suure riskiga tehisintellektisüsteemide liigitamise reeglid

1. Olenemata sellest, kas tehisintellektisüsteem lastakse turule või võetakse kasutusse punktides a ja b osutatud toodetest sõltumatult, peetakse seda tehisintellektisüsteemi suure riskiga süsteemiks, kui täidetud on mõlemad järgmised tingimused:

   (a) tehisintellektisüsteem on mõeldud kasutamiseks toote turvakomponendina või on ise toode, milles suhtes kehtivad II lisas loetletud liidu ühtlustamisõigusaktid;

   (b) toode, mille turvakomponent tehisintellektisüsteem on, või tehisintellektisüsteem ise kui toode peab läbima kolmanda isiku tehtava vastavushindamise, et selle saaks turule lasta või kasutusele võtta vastavalt II lisas loetletud liidu ühtlustamisõigusaktidele.

2. Lisaks lõikes 1 osutatud suure riskiga tehisintellektisüsteemidele peetakse suure riskiga süsteemideks ka III lisas osutatud tehisintellektisüsteeme.

Artikkel 7
III lisa muutmine

1. Komisjonil on õigus võtta kooskõlas artikliga 73 vastu delegeeritud õigusakte, et ajakohastada III lisas esitatud loetelu ja lisada sellesse suure riskiga tehisintellektisüsteeme, kui täidetud on mõlemad järgmised tingimused:

   (a) tehisintellektisüsteemid on mõeldud kasutamiseks mõnes III lisa punktides 1–8 loetletud valdkonnas;

   (b) tehisintellektisüsteemid võivad kahjustada tervist ja ohutust või avaldada negatiivset mõju põhiõigustele ning sellise riski raskusaste ja esinemise

tõenäosus on samaväärne või suurem kui III lisas juba osutatud suure riskiga tehisintellektisüsteemide põhjustatud kahju või negatiivse mõju riski puhul.

2. Kui lõike 1 kohaldamisel hinnatakse, kas tehisintellektisüsteem võib kahjustada tervist ja ohutust või avaldada negatiivset mõju põhiõigustele ning sellise riski raskusaste ja esinemise tõenäosus on samaväärne või suurem kui III lisas juba osutatud suure riskiga tehisintellektisüsteemide põhjustatud kahju riski puhul, võtab komisjon arvesse järgmisi kriteeriume:

(a) mis on tehisintellektisüsteemi sihtotstarve;

(b) millises ulatuses on tehisintellektisüsteemi kasutatud või tõenäoliselt kasutatakse;

(c) millises ulatuses on tehisintellektisüsteemi kasutamine juba teinud kahju tervisele ja ohutusele või avaldanud negatiivset mõju põhiõigustele või tekitanud tõsist muret, et selline kahju või negatiivne mõju võib tekkida, nagu on näidanud riikide pädevatele asutustele esitatud aruanded või dokumenteeritud väited;

(d) milline oleks sellise kahju või negatiivse mõju võimalik ulatus, eeskätt intensiivsus ja võime mõjutada paljusid isikuid;

(e) millises ulatuses sõltuvad potentsiaalselt kahjustatud või negatiivselt mõjutatud isikud tulemusest, milleni on jõutud tehisintellektisüsteemi abil, eeskätt seetõttu, et praktilistel või õiguslikel põhjustel ei ole mõistlikult võimalik loobuda selle tulemuse rakendamisest;

(f) millises ulatuses on potentsiaalselt kahjustatud või negatiivselt mõjutatud isikud haavatavas olukorras võrreldes tehisintellektisüsteemi kasutajaga, eeskätt võimu, teadmiste, majanduslike või sotsiaalsete olude või vanusega seotud ebavõrdsuse tõttu;

(g) millises ulatuses on tehisintellektisüsteemi abil saavutatud tulemus kergesti tagasipööratav, kusjuures tulemust, millel on mõju inimeste tervisele või ohutusele, ei peeta kergesti tagasipööratavaks;

(h) millises ulatuses on kehtivate liidu õigusaktidega ette nähtud:

i) mõjusad õiguskaitsevahendid seoses tehisintellektisüsteemist tulenevate riskidega, välja arvatud kahjunõuded;

ii) mõjusad meetmed, et neid riske ära hoida või neid oluliselt vähendada.

2. PEATÜKK

SUURE RISKIGA TEHISINTELLEKTISÜSTEEMIDELE ESITATAVAD NÕUDED

Artikkel 8
Nõuetelevastavus

1. Suure riskiga tehisintellektisüsteemid peavad vastama käesolevas peatükis kehtestatud nõuetele.

2. Neile nõuetele vastavuse tagamisel võetakse arvesse suure riskiga tehisintellektisüsteemi sihtotstarvet ja artiklis 9 osutatud riskijuhtimissüsteemi.

Artikkel 9
Riskijuhtimissüsteem

1. Suure riskiga tehisintellektisüsteemide jaoks luuakse riskijuhtimissüsteem, seda rakendatakse ja see dokumenteeritakse ning seda hooldatakse.

2. Riskijuhtimissüsteem seisneb suure riskiga tehisintellektisüsteemi kogu olelusringi jooksul pidevalt korduvas protsessis, mida tuleb korrapäraselt ja süstemaatiliselt ajakohastada. See peab sisaldama järgmisi etappe:

   (a) iga suure riskiga tehisintellektisüsteemiga seotud teadaolevate ja prognoositavate riskide kindlakstegemine ja analüüsimine;

   (b) selliste riskide prognoosimine ja hindamine, mis võivad tekkida, kui suure riskiga tehisintellektisüsteemi kasutatakse vastavalt selle sihtotstarbele, aga ka mõistlikult prognoositava väärkasutamise tingimustes;

   (c) muude tekkida võivate riskide hindamine artiklis 61 osutatud turustamisjärgse seire süsteemist saadud andmete analüüsi põhjal;

   (d) sobivate riskijuhtimismeetmete vastuvõtmine kooskõlas järgmiste lõigete sätetega.

3. Lõike 2 punktis d osutatud riskijuhtimismeetmetes võetakse nõuetekohaselt arvesse käesolevas 2. peatükis sätestatud nõuete kombineeritud kohaldamisest tulenevat mõju ja võimalikku koostoimet. Samuti võetakse neis arvesse tehnika üldtunnustatud taset, muu hulgas selliselt, nagu seda on kajastatud asjaomastes harmoneeritud standardites või ühtsetes kirjeldustes.

4. Lõike 2 punktis d osutatud riskijuhtimismeetmed on sellised, et iga ohuga seotud mistahes jääkriski ja suure riskiga tehisintellektisüsteemide üldist jääkriski peetakse vastuvõetavaks, tingimusel et suure riskiga tehisintellektisüsteemi kasutatakse vastavalt selle sihtotstarbele või mõistlikult prognoositava väärkasutamise tingimustes. Neist jääkriskidest antakse kasutajale teada.

   Kõige otstarbekamate riskijuhtimismeetmete kindlaksmääramisel tuleb tagada järgmine:

   (a) riskide kõrvaldamine või vähendamine nii palju kui võimalik sobiva projekteerimise ja arendamise kaudu;

   (b) asjakohasel juhul sobivate riskimaandamis- ja kontrollimeetmete rakendamine selliste riskide puhul, mida ei saa kõrvaldada;

   (c) piisava teabe andmine vastavalt artiklile 13, eeskätt seoses käesoleva artikli lõike 2 punktis b osutatud riskidega, ning asjakohasel juhul kasutajate koolitamine.

   Suure riskiga tehisintellektisüsteemi kasutamisega seotud riskide kõrvaldamisel või vähendamisel võetakse nõuetekohaselt arvesse kasutajalt eeldatavaid tehnilisi teadmisi, kogemusi, haridust ja koolitust, ning keskkonda, milles kasutamiseks on süsteem mõeldud.

5. Suure riskiga tehisintellektisüsteeme testitakse, et teha kindlaks kõige otstarbekamad riskijuhtimismeetmed. Testimisega tagatakse, et suure riskiga tehisintellektisüsteemid töötavad sihtotstarbe seisukohast järjepidevalt ning vastavad käesolevas peatükis sätestatud nõuetele.

6. Testimisprotseduurid peavad olema tehisintellektisüsteemi sihtotstarbe saavutamiseks sobivad ega tohi minna kaugemale kui selle eesmärgi saavutamiseks vajalik.

7. Suur riskiga tehisintellektisüsteemide testimine toimub vastavalt vajadusele mistahes ajal kogu arendusprotsessi jooksul ja igal juhul enne selle turule laskmist või kasutusele võtmist. Testimiseks kasutatakse eelnevalt kindlaks määratud parameetreid ja tõenäosuskünniseid, mis on suure riskiga tehisintellektisüsteemi sihtotstarbe seisukohast sobivad.

8. Lõigetes 1–7 kirjeldatud riskijuhtimissüsteemi rakendamisel pööratakse erilist tähelepanu sellele, kas on tõenäoline, et suure riskiga tehisintellektisüsteemile pääsevad juurde lapsed või et see mõjutab lapsi.

9. Direktiivi 2013/36/EL kohaldamisalasse kuuluvate krediidiasutuste puhul peavad lõigetes 1–8 kirjeldatud aspektid olema nende asutuste poolt selle direktiivi artikli 74 kohaselt kehtestatud riskijuhtimisprotseduuride osa.

Artikkel 10
Andmed ja andmehaldus

1. Kui tegemist on suure riskiga tehisintellektisüsteemidega, milles kasutatavad meetodid hõlmavad mudelite treenimist andmetega, tuleb nende süsteemide arendamiseks kasutada treenimis-, valideerimis- ja testimisandmestikke, mis vastavad lõigetes 2–5 osutatud kvaliteedikriteeriumidele.

2. Treenimis-, valideerimis- ja testimisandmestike suhtes kohaldatakse asjakohaseid andmehaldus- ja juhtimistavasid. Need tavad puudutavad eeskätt järgmist:

   (a) asjakohased projekteerimise käigus tehtavad valikud;

   (b) andmete kogumine;

   (c) andmete ettevalmistamiseks tehtavad asjakohased töötlemistoimingud, näiteks kommenteerimine, märgendamine, puhastamine, rikastamine ja koondamine;

   (d) asjakohaste eelduste sõnastamine, eeskätt seoses teabega, mida andmed peaksid mõõtma ja kajastama;

   (e) vajalike andmestike kättesaadavuse, koguste ja sobivuse eelhindamine;

   (f) läbi vaatamine võimaliku kallutatuse seisukohast;

   (g) võimalike andmelünkade või puuduste kindlakstegemine ja võimalused nende lünkade ja puuduste kõrvaldamiseks.

3. Treenimis-, valideerimis- ja testimisandmestikud peavad olema asjakohased, representatiivsed, vigadeta ja täielikud. Neid peavad iseloomustama asjakohased statistilised omadused, sealhulgas vajaduse korral seoses isikute või isikute rühmadega, kelle peal kavatsetakse suure riskiga tehisintellektisüsteemi kasutada. Need andmestiku omadused võivad olla täidetud üksikute andmestike või nende kombinatsiooni tasandil.

4. Treenimis-, valideerimis- ja testimisandmestikes tuleb sihtotstarbe jaoks vajalikus ulatuses võtta arvesse omadusi või elemente, mis iseloomustavad konkreetset geograafilist, käitumuslikku või funktsionaalset olukorda, kus kavatsetakse suure riskiga tehisintellektisüsteemi kasutada.

5. Niivõrd, kuivõrd see on rangelt vajalik kallutatuse seire, avastamise ja parandamise jaoks suure riskiga tehisintellektisüsteemide puhul, võivad selliste süsteemide pakkujad töödelda määruse (EL) 2016/679 artikli 9 lõikes 1, direktiivi (EL) 2016/680 artiklis 10 ja määruse (EL) 2018/1725 artikli 10 lõikes 1 osutatud isikuandmete eriliike, tingimusel et füüsiliste isikute põhiõiguste ja vabaduste kaitseks kohaldatakse asjakohaseid kaitsemeetmeid, sh tehnilisi piiranguid, mis puudutavad tipptasemel turvalisuse tagamise ja privaatsuse säilitamise meetmete, näiteks pseudonüümimise taaskasutamist ja kasutamist või krüpteerimist, kui anonüümimine võib avaldada olulist mõju taotletavale eesmärgile.

6. Suure riskiga tehisintellektisüsteemide arendamisel kohaldatakse asjakohaseid andmehaldus- ja juhtimistavasid, välja arvatud juhul, kui tegemist on selliste tehisintellektisüsteemidega, milles kasutatavad meetodid hõlmavad mudelite treenimist, et tagada selliste suure riskiga tehisintellektisüsteemide vastavus lõikele 2.

Artikkel 11
Tehniline dokumentatsioon

1. Suure riskiga tehisintellektisüsteemi tehniline dokumentatsioon koostatakse enne süsteemi turule laskmist või kasutusele võtmis ning see hoitakse ajakohasena.

   Tehniline dokumentatsioon koostatakse selliselt, et see tõendaks suure riskiga tehisintellektisüsteemi vastavust käesolevas peatükis sätestatud nõuetele ja annaks riikide pädevatele asutustele ja teavitatud asutustele kogu teabe, mis on vajalik, et hinnata tehisintellektisüsteemi vastavust neile nõuetele. Dokumentatsioon peab sisaldama vähemalt IV lisas loetletud elemente.

2. Kui turule lastakse või kasutusse võetakse suure riskiga tehisintellektisüsteem, mis on seotud tootega, mille suhtes kohaldatakse II lisa A jaos loetletud õigusakte, koostatakse üks ühtne tehniline dokumentatsioon, mis sisaldab nii kogu IV lisas kirjeldatud teavet kui ka nimetatud õigusaktide kohaselt nõutavat teavet.

3. Komisjonil on õigus võtta kooskõlas artikliga 73 vastu delegeeritud õigusakte, et muuta IV lisa, kui see on vajalik, et tagada, et tehniline dokumentatsioon sisaldab tehnika arengut arvestades kogu vajalikku teavet, et hinnata süsteemi vastavust käesolevas peatükis sätestatud nõuetele.

Artikkel 12
Andmete säilitamine

1. Suure riskiga tehisintellektisüsteeme tuleb nii projekteerida ja arendada, et nende süsteemide töötamise ajal oleks võimalik sündmusi automaatselt registreerida („logid“). Selline logimisvõime peab vastama tunnustatud standarditele või ühtsetele kirjeldustele.

2. Logimisfunktsioonid peavad tagama kogu tehisintellektisüsteemi elutsükli jooksul selle süsteemi toimimise jälgitavuse süsteemi sihtotstarbe seisukohast otstarbekal tasemel.

3. Eeskätt peavad logimisfunktsioonid võimaldama suure riskiga tehisintellektisüsteemi töö seiret seoses selliste olukordade esinemisega, mille tulemusena võib tehisintellektisüsteem tekitada riski artikli 65 lõike 1 tähenduses või põhjustada olulise muudatuse, ning hõlbustama artiklis 61 osutatud turustamisjärgset seiret.

4. III lisa punkti 1 alapunktis a osutatud suure riskiga tehisintellektisüsteemide logimisfunktsioonid peavad pakkuma vähemalt järgmist:

(a) süsteemi iga kasutuskorra ajavahemiku registreerimine (iga kasutuskorra alguse ja lõpu kuupäev ja kellaaeg);

(b) võrdlusandmebaas, millega süsteem sisendandmeid võrdleb;

(c) sisendandmed, mille otsimine on andnud vastuseks tulemuse;

(d) tulemuste kontrollimises osalenud füüsiliste isikute isikusamasuse kontroll, nagu on viidatud artikli 14 lõikes 5.

Artikkel 13
Läbipaistvus ja kasutajate teavitamine

1. Suure riskiga tehisintellektisüsteeme tuleb projekteerida ja arendada selliselt, et oleks tagatud nende töö piisav läbipaistvus selleks, et kasutajad saaksid tõlgendada süsteemi väljundit ja seda asjakohaselt kasutada. Tagada tuleb käesoleva jaotise 3. peatükis sätestatud kasutaja ja pakkuja asjaomaste kohustuste täitmiseks asjakohast liiki ja asjakohasel tasemel läbipaistvus.

2. Suure riskiga tehisintellektisüsteemiga peab kaasas olema sobivas digivormingus või muus vormis kasutusjuhend, mis sisaldab kokkuvõtlikku, täielikku, täpset ja selget teavet, mis on kasutajatele oluline, juurdepääsetav ja mõistetav.

3. Lõikes 2 osutatud teabest peavad selguma järgmised asjaolud:

(a) pakkuja ning asjakohasel juhul tema volitatud esindaja nimi ja kontaktandmed;

(b) suure riskiga tehisintellektisüsteemi omadused, funktsioonid ja toimimispiirangud, muu hulgas:

i) süsteemi sihtotstarve;

ii) artiklis 15 osutatud täpsuse, stabiilsuse ja küberturvalisuse tase, mille põhjal on suure riskiga tehisintellektisüsteem testitud ja valideeritud ja mida võib eeldada, ning kõik teadaolevad ja prognoositavad asjaolud, mis võivad seda täpsuse, stabiilsuse ja küberturvalisuse taset mõjutada;

iii) kõik teadaolevad või prognoositavad asjaolud, mis on seotud suure riskiga tehisintellektisüsteemi kasutamisega vastavalt selle sihtotstarbele või mõistlikult prognoositava väärkasutamise tingimustes, mis võib seada ohtu tervise ja ohutuse või põhiõigused;

iv) süsteemi toimimine, mis puudutab isikuid või isikute rühmi, kelle peal kavatsetakse suure riskiga tehisintellektisüsteemi kasutada.

v) kui see on asjakohane, siis sisendandmete spetsifikatsioonid või muu asjakohane teave kasutatud treenimis-, valideerimis- ja testimisandmestike kohta, võttes arvesse tehisintellektisüsteemi sihtotstarvet;

(c) suure riskiga tehisintellektisüsteemi ja selle toimimise muudatused, mille pakkuja on esialgse vastavushindamise ajal ette kindlaks määranud, kui neid on;

(d) artiklis 14 osutatud inimjärelevalve meetmed, kaasa arvatud tehnilised meetmed, mis on kehtestatud selleks, et kasutajatel oleks lihtsam tehisintellektisüsteemide väljundit tõlgendada;

(e) suure riskitasemega tehisintellektisüsteemi eeldatav eluiga ning mistahes hooldus- ja hoolikusmeetmed, mis on vajalikud, et tagada tehisintellektisüsteemi nõuetekohane toimimine, muu hulgas tarkvarauuenduste vallas.

Artikkel 14
Inimjärelevalve

1. Suure riskiga tehisintellektisüsteeme tuleb projekteerida ja arendada selliselt, kasutades muu hulgas asjakohaseid inimene-masin kasutajaliideseid, et füüsilised isikud saaksid teha tehisintellektisüsteemi kasutamise ajal selle üle reaalset järelevalvet.

2. Inimjärelevalve eesmärk on hoida ära või minimeerida tervist, ohutust või põhiõigusi ähvardavaid riske, mis võivad tekkida, kui suure riskiga tehisintellektisüsteemi kasutatakse vastavalt selle sihtotstarbele või mõistlikult prognoositava väärkasutamise tingimustes, eeskätt juhul, kui sellised riskid jäävad alles ka siis, kui kohaldatakse muid käesolevas peatükis sätestatud nõudeid.

3. Inimjärelevalve tagatakse kas ühe või kõigi järgmiste meetmetega:

(a) meetmed, mille pakkuja on enne suure riskiga tehisintellektisüsteemi turule laskmist või kasutusele võtmist kindlaks teinud ja, kui see on tehniliselt teostatav, sellisesse süsteemi sisse ehitanud;

(b) meetmed, mille pakkuja on enne suure riskiga tehisintellektisüsteemi turule laskmist või kasutusele võtmist kindlaks teinud ja mis sobivad selleks, et kasutaja saaks neid rakendada.

4. Lõikes 3 osutatud meetmed võimaldavad isikutel, kellele on antud ülesanne tegeleda inimjärelevalvega, teha olenevalt asjaoludest järgmist:

(a) mõista täielikult suure riskiga tehisintellektisüsteemi võimekusi ja piiranguid ning suuta tegeleda sellise süsteemi nõuetekohase seirega, et võimalikult kiiresti avastada märke kõrvalekalletest, väärtalitlusest ja ootamatust toimimisest ning need kõrvaldada;

(b) olla pidevalt teadlik võimalusest, et tekib kalduvus hakata automaatselt tuginema või liigselt tuginema suure riskiga tehisintellektisüsteemi toodetud väljundile (nn kalduvus eelistada automatiseerimist), seda eriti siis, kui tegemist on suure riskiga tehisintellektisüsteemidega, mida kasutatakse, et saada teavet või soovitusi füüsiliste isikute tehtavate otsuste jaoks;

(c) suuta korrektselt tõlgendada suure riskiga tehisintellektisüsteemi väljundit, võttes arvesse eeskätt süsteemi omadusi ning kättesaadavaid tõlgendamisvahendeid ja -meetodeid;

(d) suuta igas konkreetses olukorras otsustada, et suure riskiga tehisintellektisüsteemi ei kasutata, või jätta suure riskiga tehisintellektisüsteemi väljund muul moel kõrvale, sürjutada või tagasi võtta;

(e) suuta sekkuda suure riskiga tehisintellektisüsteemi töösse või katkestada süsteemi töö stopp-nupu või muu sarnase protseduuriga.

5. III lisa punkti 1 alapunktis a osutatud suure riskiga tehisintellektisüsteemide puhul tuleb lõikes 3 osutatud meetmetega tagada, et lisaks sellele ei tee ega otsusta kasutaja süsteemist saadud tuvastamise põhjal midagi, kui seda ei ole kontrollinud ja kinnitanud vähemalt kaks füüsilist isikut.

Artikkel 15
Täpsus, stabiilsus ja küberturvalisus

1. Suure riskiga tehisintellektisüsteeme tuleb projekteerida ja arendada selliselt, et nad saavutaksid oma sihtotstarbe seisukohast asjakohase täpsuse, stabiilsuse ja küberturvalisuse taseme ning et nende sooritus oleks kolmes nimetatud aspektis kogu elutsükli jooksul järjekindel.

2. Suure riskiga tehisintellektisüsteemide täpsuse tasemed ja asjakohased täpsuse parameetrid tuleb deklareerida süsteemiga kaasas olevas kasutusjuhendis.

3. Suure riskiga tehisintellektisüsteemid peavad olema süsteemis või süsteemi töökeskkonnas tekkida võivate vigade, rikete või ebakõlade suhtes vastupidavad, eriti juhul, kui põhjuseks on süsteemi interaktsioon füüsiliste isikute või muude süsteemidega.

   Suure riskiga tehisintellektisüsteemide stabiilsuse võib saavutada tehnilise liiasuse lahendustega, mis võivad hõlmata varuplaane või tõrkekindluse plaane.

   Suure riskiga tehisintellektisüsteeme, mis õpivad edasi ka pärast turule laskmist või kasutusele võtmist, tuleb projekteerida ja arendada selliselt, et tagatud oleks asjakohaste leevendusmeetmete kasutamine, et hoida ära kallutatud väljundi tekkimise võimalus, mille põhjustab väljundi kasutamine edasiste toimingute sisendina („tagasisideahelad“).

4. Suure riskiga tehisintellektisüsteemid peavad pidama vastu volitamata kolmandate isikute katsetele muuta süsteemi kasutamist või toimimist, kasutades ära süsteemi nõrkusi.

   Suure riskiga tehisintellektisüsteemide küberturvalisuse tagamiseks kasutatavad tehnilised lahendused peavad vastama asjaomastele asjaoludele ja riskidele.

   Tehisintellektile iseloomulike nõrkustega toimetulemiseks kasutatavad tehnilised lahendused hõlmavad olenevalt asjaoludest meetmeid, millega hoida ära ja kontrollida ründeid, millega püütakse manipuleerida treenimisandmestikku („andmemürgitus“), sisendeid, mille eesmärk on panna mudel viga tegema („vastandnäited“), või mudelivigu.

3. PEATÜKK

SUURE RISKIGA TEHISINTELLEKTISÜSTEEMIDE PAKKUJATE JA KASUTAJATE NING MUUDE OSALISTE KOHUSTUSED

Artikkel 16
Suure riskiga tehisintellektisüsteemide pakkujate kohustused

Suure riskiga tehisintellektisüsteemide pakkujad peavad:

(a) tagama, et nende suure riskiga tehisintellektisüsteemid vastavad käesoleva jaotise 2. peatükis sätestatud nõuetele;

(b) võtma kasutusele kvaliteedijuhtimissüsteemi, mis vastab artikli 17 nõuetele;

(c) koostama suure riskiga tehisintellektisüsteemi tehnilise dokumentatsiooni;

(d) säilitama oma suure riskiga tehisintellektisüsteemide automaatselt loodud logisid, kui need on nende kontrolli all;

(e) tagama, et suure riskiga tehisintellektisüsteem läbib enne turule laskmist või kasutusele võtmist asjakohase vastavushindamise;

(f) täitma artiklis 51 osutatud registreerimiskohustusi;

(g) võtma vajalikud parandusmeetmed, kui suure riskiga tehisintellektisüsteem ei ole vastavuses käesoleva jaotise 2. peatükis sätestatud nõuetega;

(h) teatama mittevastavusest ja võetud parandusmeetmetest nende liikmesriikide pädevatele asutustele, kus nad on tehisintellektisüsteemi kättesaadavaks teinud või kasutusele võtnud, ja vajaduse korral teavitatud asutusele;

(i) kinnitama kooskõlas artikliga 49 oma suure riskiga tehisintellektisüsteemile CE-märgise, et näidata vastavust käesolevale määrusele;

(j) tõendama riigi pädeva asutuse taotlusel suure riskiga tehisintellektisüsteemi vastavust käesoleva jaotise 2. peatükis sätestatud nõuetele.

Artikkel 17
Kvaliteedijuhtimissüsteem

1. Suure riskiga tehisintellektisüsteemide pakkujad võtavad kasutusele kvaliteedijuhtimissüsteemi, mis tagab käesoleva määruse järgimise. Kvaliteedijuhtimissüsteem peab olema kirjalike põhimõtete, menetluste ja juhendite kujul süsteemselt ja nõuetekohaselt dokumenteeritud ning sisaldama vähemalt järgmisi aspekte:

   (a) strateegia õigusnormidele vastavuse tagamiseks, sealhulgas vastavushindamise ja suure riskiga tehisintellektisüsteemis tehtavate muudatuste haldamismenetluste järgimiseks;

   (b) meetodid, protseduurid ja süstemaatilised meetmed, mida kasutatakse suure riskiga tehisintellektisüsteemi projekteerimiseks, projekteerimise järelevalveks ja projektide kontrollimiseks;

   (c) meetodid, protseduurid ja süstemaatilised meetmed, mida kasutatakse suure riskiga tehisintellektisüsteemi arendamiseks, kvaliteedi kontrollimiseks ja kvaliteedi tagamiseks;

   (d) enne suure riskiga tehisintellektisüsteemi arendamist, selle ajal ja pärast seda teostatavad läbivaatamis-, testimis- ja valideerimisprotseduurid ning nende teostamise sagedus;

   (e) kohaldatavad tehnilised kirjeldused, sh standardid, ja juhul, kui asjaomaseid harmoneeritud standardeid ei kohaldata täies mahus, siis ka vahendid, mida kasutatakse, et tagada suure riskiga tehisintellektisüsteemi vastavus käesoleva jaotise 2. peatükis sätestatud nõuetele;

   (f) andmehalduse süsteemid ja protseduurid, sh andmete kogumine, andmeanalüüs, andmete märgendamine, andmete talletamine, andmete filtreerimine, andmekaeve, andmete agregeerimine, andmesäilitus ja mis tahes muud andmetega seotud toimingud, mida teostatakse suure riskiga

tehisintellektisüsteemide turule laskmise või kasutusele võtmise eel ja eesmärgil;

(g) artiklis 9 osutatud riskijuhtimissüsteem;

(h) turustamisjärgse seire süsteemi loomine, rakendamine ja toimivana hoidmine vastavalt artiklile 61;

(i) protseduurid, mis on seotud tõsistest intsidentidest ja tõrgetest teatamisega vastavalt artiklile 62;

(j) suhtlemine riikide pädevate asutustega, pädevate asutustega, sh valdkondlike pädevate asutustega, kes pakuvad või toetavad juurdepääsu andmetele, teavitatud asutustega, teiste operaatoritega, klientidega või muude huvitatud isikutega;

(k) kõigi vajalike dokumentide ja teabega seotud andmete säilitamise süsteemid ja protseduurid;

(l) ressursside haldamine, sh varustuskindlusega seotud meetmed;

(m) aruandekohustuse raamistik, millega nähakse ette juhtkonna ja muude töötajate vastutus seoses kõigi käesolevas lõikes loetletud aspektidega.

2. Lõikes 1 osutatud aspektide rakendamine peab olema proportsionaalne pakkuja organisatsiooni suurusega.

3. Kui pakkuja on direktiivi 2013/36/EL kohaldamisalasse kuuluv krediidiasutus, loetakse kvaliteedijuhtimissüsteemi kasutusele võtmise kohustus täidetuks, kui vastavalt nimetatud direktiivi artiklile 74 on täidetud sisejuhtimise korralduse, protseduuride ja korra alased nõuded. Seoses sellega võetakse arvesse käesoleva määruse artiklis 40 osutatud harmoneeritud standardeid.

Artikkel 18
Tehnilise dokumentatsiooni koostamise kohustus

1. Suure riskiga tehisintellektisüsteemide pakkujad koostavad artiklis 11 osutatud tehnilise dokumentatsiooni kooskõlas IV lisaga.

2. Pakkujad, kes on direktiivi 2013/36/EL kohaldamisalasse kuuluvad krediidiasutused, haldavad tehnilist dokumentatsiooni nimetatud direktiivi artikli 74 kohase sisejuhtimist, korraldust, protseduure ja korda käsitleva dokumentatsiooni osana.

Artikkel 19
Vastavushindamine

1. Suure riskiga tehisintellektisüsteemide pakkujad peavad tagama, et nende süsteemid läbivad enne turule laskmist või kasutusele võtmist asjakohase vastavushindamise vastavalt artiklile 43. Kui sellise vastavushindamise kohaselt tõendatakse, et tehisintellektisüsteemid vastavad käesoleva jaotise 2. peatüki nõuetele, koostavad pakkujad ELi vastavusdeklaratsiooni vastavalt artiklile 48 ja kinnitavad tootele CE-vastavusmärgise vastavalt artiklile 49.

2. III lisa punkti 5 alapunktis b osutatud suure riskiga tehisintellektisüsteemide puhul, mille lasevad turule või võtavad kasutusele pakkujad, kes on direktiivi 2013/36/EL kohaldamisalasse kuuluvad krediidiasutused, toimub vastavushindamine osana nimetatud direktiivi artiklites 97–101 osutatud protseduuridest.

Artikkel 20
Automaatselt genereeritud logid

1. Suure riskiga tehisintellektisüsteemide pakkujad säilitavad oma suure riskiga tehisintellektisüsteemide automaatselt genereeritud logisid niivõrd, kuivõrd sellised logid on nende kontrolli all tulenevalt lepingupõhisest kokkuleppest kasutajaga või muul õiguslikul alusel. Logisid peetakse sellise aja jooksul, mis on suure riskiga tehisintellektisüsteemi sihtotstarbe ja liidu või liikmesriigi õiguse alusel kohaldatavate juriidiliste kohustuste seisukohast asjakohane.

2. Pakkujad, kes on direktiivi 2013/36/EL kohaldamisalasse kuuluvad krediidiasutused, haldavad oma suure riskiga tehisintellektisüsteemide automaatselt genereeritud logisid nimetatud direktiivi artikli 74 kohase dokumentatsiooni osana.

Artikkel 21
Parandusmeetmed

Suure riskiga tehisintellektisüsteemide pakkujad, kes arvavad või kellel on põhjust arvata, et suure riskiga tehisintellektisüsteem, mille nad on turule lasknud või kasutusele võtnud, ei vasta käesolevale määrusele, võtavad viivitamatult vajalikud parandusmeetmed, et viia süsteem vastavusse, võtta see turult tagasi või kutsuda tagasi, nagu on asjakohane. Nad teavitavad sellest asjaomase suure riskiga tehisintellektisüsteemi levitajaid ning vajaduse korral volitatud esindajat ja importijaid.

Artikkel 22
Teavitamiskohustus

Kui suure riskiga tehisintellektisüsteem kujutab endast riski artikli 65 lõike 1 tähenduses ja see risk on süsteemi pakkujale teada, peab see pakkuja viivitamata teavitama nende liikmesriikide pädevaid asutusi, kus ta on süsteemi kättesaadavaks teinud, ja vajaduse korral teavitatud asutust, kes andis selle suure riskiga tehisintellektisüsteemi jaoks välja sertifikaadi, eeskätt tuleb teave esitada mittevastavuse ja võetud parandusmeetmete kohta.

Artikkel 23
Koostöö pädevate asutustega

Suure riskiga tehisintellektisüsteemide pakkujad peavad riigi pädeva asutuse taotluse peale esitama sellele asutusele kogu teabe ja dokumentatsiooni, mis on vajalik, et tõendada suure riskiga tehisintellektisüsteemi vastavust käesoleva jaotise 2. peatükis sätestatud nõuetele, asjaomase liikmesriigi poolt kindlaks määratud liidu ametlikus keeles. Riigi pädeva asutuse põhjendatud taotluse peale annavad pakkujad sellele asutusele juurdepääsu suure riskiga tehisintellektisüsteemi automaatselt genereeritud logidele niivõrd, kuivõrd sellised logid on nende kontrolli all tulenevalt lepingupõhisest kokkuleppest kasutajaga või muul õiguslikul alusel.

Artikkel 24
Toote valmistajate kohustused

Kui II lisa A jaos loetletud õigusaktidega reguleeritud tootega seotud suure riskiga tehisintellektisüsteem lastakse turule või võetakse kasutusele koos kõnealuste õigusaktide kohaselt valmistatud tootega ja toote valmistaja nime all, võtab toote valmistaja vastutuse selle eest, et tehisintellektisüsteem vastab käesolevale määrusele, ning tal on seoses

tehisintellektisüsteemiga samad kohustused, mis on käesoleva määrusega kehtestatud pakkuja suhtes.

Artikkel 25
Volitatud esindajad

1. Kui importijat ei ole võimalik kindlaks teha, peab väljaspool liitu asuv pakkuja enne oma süsteemi liidu turul kättesaadavaks tegemist määrama kirjaliku volitusega liidus asuva volitatud esindaja.

2. Volitatud esindaja täidab pakkujalt saadud volituses kindlaksmääratud ülesandeid. Volitus annab volitatud esindajale õiguse täita järgmisi ülesandeid:

   (a) säilitada riigi pädevate asutuste ja artikli 63 lõikes 7 osutatud riiklike asutuste jaoks kättesaadavana ELi vastavusdeklaratsiooni ja tehnilise dokumentatsiooni koopiat;

   (b) esitada riigi pädevale asutusele põhjendatud taotluse peale kogu teave ja dokumentatsioon, mis on vajalik, et tõendada suure riskiga tehisintellektisüsteemi vastavust käesoleva jaotise 2. peatükis sätestatud nõuetele, sealhulgas pakkuda juurdepääsu suure riskiga tehisintellektisüsteemi automaatselt genereeritud logidele niivõrd, kuivõrd sellised logid on pakkuja kontrolli all tulenevalt lepingupõhisest kokkuleppest kasutajaga või muul õiguslikul alusel;

   (c) teha riikide pädevate asutustega põhjendatud taotluse peale koostööd kõigis toimingutes, mida riigi pädev asutus seoses suure riskiga tehisintellektisüsteemiga ette võtab.

Artikkel 26
Importijate kohustused

1. Enne suure riskiga tehisintellektisüsteemi turule laskmist peavad sellise süsteemi importijad tagama, et:

   (a) selle tehisintellektisüsteemi pakkuja on teostanud asjakohase vastavushindamise;

   (b) pakkuja on koostanud tehnilise dokumentatsiooni kooskõlas IV lisaga;

   (c) süsteemil on nõutav vastavusmärgis ning sellega on kaasas nõutavad dokumendid ja kasutusjuhendid.

2. Kui importija arvab või tal on põhjust arvata, et suure riskiga tehisintellektisüsteem ei ole käesoleva määrusega vastavuses, ei vii ta seda süsteemi turule enne, kui see tehisintellektisüsteem on viidud määrusega vastavusse. Kui suure riskiga tehisintellektisüsteem kujutab endast riski artikli 65 lõike 1 tähenduses, teavitab importija sellest tehisintellektisüsteemi pakkujat ja turujärelevalveasutusi.

3. Importijad märgivad oma nime, registreeritud kaubanime või registreeritud kaubamärgi ja kontaktaadressi kas suure riskiga tehisintellektisüsteemile või, kui see ei ole võimalik, selle pakendile või kaasasolevatesse dokumentidesse, nagu on asjakohane.

4. Importija tagab vastavalt asjaoludele, et sel ajal, kui suure riskiga tehisintellektisüsteem on tema vastutuse all, ei ohusta ladustamise ega transpordi tingimused selle vastavust käesoleva jaotise 2. peatükis sätestatud nõuetele.

5. Importijad esitavad riigi pädevale asutusele põhjendatud taotluse peale kogu teabe ja dokumentatsiooni, mis on vajalik, et tõendada suure riskiga tehisintellektisüsteemi vastavust käesoleva jaotise 2. peatükis sätestatud nõuetele, selle riigi pädeva asutuse jaoks lihtsalt arusaadavas keeles, sealhulgas pakuvad nad juurdepääsu suure riskiga tehisintellektisüsteemi automaatselt genereeritud logidele niivõrd, kuivõrd sellised logid on pakkuja kontrolli all tulenevalt lepingupõhisest kokkuleppest kasutajaga või muul õiguslikul alusel. Samuti teevad nad nende asutustega koostööd kõigis toimingutes, mida riigi pädev asutus seoses selle süsteemiga ette võtab.

Artikkel 27
Turustajate kohustused

1. Enne suure riskiga tehisintellektisüsteemi turul kättesaadavaks tegemist kontrollivad turustajad, et suure riskiga tehisintellektisüsteem kannab nõutavat CE-vastavusmärgist, et sellega on kaasas nõutav dokumentatsioon ja kasutusjuhend ning et olenevalt asjaoludest on kas süsteemi pakkuja või importija täitnud käesolevas määruses sätestatud kohustused.

2. Kui turustaja arvab või tal on põhjust arvata, et suure riskiga tehisintellektisüsteem ei ole vastavuses käesoleva jaotise 2. peatükis sätestatud nõuetega, ei tee ta seda suure riskiga tehisintellektisüsteemi turul kättesaadavaks enne, kui see süsteem on viidud nende nõuetega vastavusse. Peale selle, kui suure riskiga tehisintellektisüsteem kujutab endast riski artikli 65 lõike 1 tähenduses, teavitab turustaja sellest süsteemi pakkujat või importijat, nagu on asjakohane.

3. Turustaja tagab vastavalt asjaoludele, et sel ajal, kui suure riskiga tehisintellektisüsteem on tema vastutuse all, ei ohusta ladustamise ega transpordi tingimused süsteemi vastavust käesoleva jaotise 2. peatükis sätestatud nõuetele.

4. Turustaja, kes arvab või kellel on põhjust arvata, et suure riskiga tehisintellektisüsteem, mille ta on turul kättesaadavaks teinud, ei vasta käesoleva jaotise 2. peatüki nõuetele, võtab parandusmeetmeid, mis on vajalikud, et viia süsteem nende nõuetega vastavusse, võtta see turult tagasi või kutsuda tagasi, või tagab, et olenevalt asjaoludest, kas pakkuja, importija või mõni asjaomane operaator võtab sellised parandusmeetmed. Kui suure riskiga tehisintellektisüsteem kujutab endast riski artikli 65 lõike 1 tähenduses, teavitab turustaja sellest viivitamata riigi pädevaid asutusi nendes liikmesriikides, kus ta on toote kättesaadavaks teinud, esitades eelkõige üksikasjad mittevastavuse ja võimalike võetud parandusmeetmete kohta.

5. Riigi pädeva asutuse põhjendatud taotluse peale esitab suure riskiga tehisintellektisüsteemi turustaja sellele asutusele kogu teabe ja dokumentatsiooni, mis on vajalik, et tõendada suure riskiga süsteemi vastavust käesoleva jaotise 2. peatükis sätestatud nõuetele. Ühtlasi teevad turustajad selle riigi pädeva asutusega koostööd kõigis toimingutes, mida see asutus ette võtab.

Artikkel 28
Turustajate, importijate, kasutajate ja muude kolmandate isikute kohustused

1. Turustajat, importijat, kasutajat või muud kolmandat isikut käsitatakse käesoleva määruse kohaldamisel pakkujana ning tema suhtes kohaldatakse artiklist 16 tulenevaid pakkuja kohustusi millisel tahes järgmisel juhul:

(a) nad lasevad suure riskiga tehisintellektisüsteemi turule või võtavad selle kasutusele oma nime või kaubamärgi all;

(b) nad muudavad juba turule lastud või kasutusele võetud suure riskiga tehisintellektisüsteemi sihtotstarvet;

(c) nad teevad suure riskiga tehisintellektisüsteemis olulise muudatuse.

2. Lõike 1 punktis b või c osutatud asjaolude ilmnemise korral ei käsitata suure riskiga tehisintellektisüsteemi algselt turule lasknud või kasutusele võtnud pakkujat enam käesoleva määruse kohaldamisel pakkujana.

Artikkel 29
Suure riskiga tehisintellektisüsteemide kasutajate kohustused

1. Suure riskiga tehisintellektisüsteemide kasutajad kasutavad selliseid süsteeme vastavalt süsteemiga kaasas olevale kasutusjuhendile kooskõlas lõigetega 2 ja 5.

2. Lõikes 1 sätestatud kohustused ei piira muid liidu või liikmesriigi õigusest tulenevaid kasutaja kohustusi ega kasutaja kaalutlusõigust oma vahendite ja tegevuse korraldamisel, et rakendada pakkuja märgitud inimjärelevalve meetmeid.

3. Niivõrd, kuivõrd kasutajal on kontroll sisendandmete üle, tagab see kasutaja, et sisendandmed on suure riskiga tehisintellektisüsteemi sihtotstarbe seisukohast asjakohased, ilma et see piiraks lõike 1 kohaldamist.

4. Kasutajad peavad tegelema suure riskiga tehisintellektisüsteemi töö seirega kasutusjuhendi alusel. Kui neil on põhjust arvata, et kasutusjuhendi kohase kasutamise tulemusena võib tehisintellektisüsteem tekitada riski artikli 65 lõike 1 tähenduses, teatab ta sellest pakkujale või turustajale ja peatab süsteemi kasutamise. Pakkujat või turustajat teavitavad nad ka siis, kui on kindlaks teinud tõsise intsidendi või talitlushäire artikli 62 tähenduses, ning ühtlasi katkestavad nad sellisel juhul tehisintellektisüsteemi kasutamise. Kui kasutaja ei saa pakkujaga ühendust, kohaldatakse artikli 62 *mutatis mutandis*.

Kui kasutaja on direktiivi 2013/36/EL kohaldamisalasse kuuluv krediidiasutus, loetakse esimeses lõigus sätestatud seirekohustus täidetuks, kui vastavalt nimetatud direktiivi artiklile 74 on täidetud sisejuhtimise korralduse, protseduuride ja korra alased nõuded.

5. Suure riskiga tehisintellektisüsteemide kasutajad säilitavad selle suure riskiga tehisintellektisüsteemi automaatselt genereeritud logisid niivõrd, kuivõrd sellised logid on nende kontrolli all. Logisid peetakse sellise aja jooksul, mis on suure riskiga tehisintellektisüsteemi sihtotstarbe ja liidu või liikmesriigi õiguse alusel kohaldatavate juriidiliste kohustuste seisukohast asjakohane.

Kasutajad, kes on direktiivi 2013/36/EL kohaldamisalasse kuuluvad krediidiasutused, haldavad logisid nimetatud direktiivi artikli 74 kohase sisejuhtimise korraldust, protseduure ja korda käsitleva dokumentatsiooni osana.

6. Suure riskiga tehisintellektisüsteemide kasutajad kasutavad artikli 13 alusel esitatavat teavet, et täita oma kohustust koostada vajaduse korral andmekaitsealane mõjuhinnang vastavalt määruse (EL) 2016/679 artiklile 35 või direktiivi (EL) 2016/680 artiklile 27.

4. PEATÜKK

TEAVITAVAD ASUTUSED JA TEAVITATUD ASUTUSED

Artikkel 30
Teavitavad asutused

1. Iga liikmesriik määrab või loob teavitava asutuse, kes vastutab vastavushindamisasutuste hindamise, määramise ja neist teavitamise ning nende seire jaoks vajalike menetluste väljatöötamise ja läbiviimise eest.

2. Liikmesriik võib teavitavaks asutuseks määrata määruses (EÜ) nr 765/2008 osutatud riikliku akrediteerimisasutuse.

3. Teavitavad asutused tuleb luua, nende töö korraldada ja neid juhtida nii, et ei tekiks huvide konflikti vastavushindamisasutustega ning et oleks kindlustatud nende tegevuse objektiivsus ja erapooletus.

4. Teavitavate asutuste töö korraldatakse nii, et kõik vastavushindamisasutusest teavitamisega seotud otsused teevad pädevad isikud, kes ei ole nende asutuste hindamist läbi viinud isikud.

5. Teavitavad asutused ei tohi pakkuda ega osutada teenuseid, mida osutavad vastavushindamisasutused, ega nõustamisteenuseid ärilisel või konkureerival alusel.

6. Teavitavad asutused tagavad saadud teabe konfidentsiaalsuse.

7. Teavitavatel asutustel on oma ülesannete nõuetekohaseks täitmiseks piisavalt pädevaid töötajaid.

8. Teavitavad asutused tagavad, et vastavushindamine toimub proportsionaalsel viisil, vältides pakkujate liigset koormamist, ning et teavitatud asutused täidavad oma ülesandeid, võttes nõuetekohaselt arvesse ettevõtja suurust, tegutsemisvaldkonda ja struktuuri ning asjaomase tehisintellektisüsteemi keerukuse astet.

Artikkel 31
Vastavushindamisasutuse teavitamistaotlus

1. Vastavushindamisasutus esitab teavitamistaotluse selle liikmesriigi teavitavale asutusele, mille territooriumil ta asub.

2. Teavitamistaotlusega koos esitatakse dokument, kus kirjeldatakse vastavushindamistoiminguid, vastavushindamismoodulit või -mooduleid ja tehisintellektitehnoloogiaid, millega tegelemiseks väidab see vastavushindamisasutus end pädev olevat, ning riikliku akrediteerimisasutuse väljastatud akrediteerimistunnistus (kui see on olemas), mis tõendab, et vastavushindamisasutus vastab artiklis 33 sätestatud nõuetele. Lisatakse mis tahes kehtivad dokumendid, mis on seotud taotlust esitava teavitatud asutuse olemasolevate määramistega mõne muu liidu ühtlustamisõigusakti alusel.

3. Kui vastavushindamisasutus ei saa akrediteerimistunnistust esitada, siis esitab ta teavitavale asutusele kogu dokumentaalse tõestuse, mis on vajalik, et kontrollida, tunnistada ja korrapäraselt jälgida tema vastavust artiklis 33 sätestatud nõuetele. Kui tegemist on teavitatud asutusega, mis on määratud mõne muu liidu ühtlustamisõigusakti alusel, võib vastavalt vajadusele kasutada kõiki kõnealuste

määramistega seotud dokumente ja tõendeid nende määramise toetuseks käesoleva määruse alusel.

Artikkel 32
Teavitamiskord

1. Teavitavad asutused võivad teavitada ainult neist vastavushindamisasutustest, mis vastavad artiklis 33 sätestatud nõuetele.
2. Teavitavad asutused kasutavad komisjoni ja teiste liikmesriikide teavitamiseks komisjoni välja töötatud ja hallatavat elektroonilist teavitamisvahendit.
3. Teavituses esitatakse täielik ülevaade vastavushindamistoimingutest, vastavushindamismoodulist või -moodulitest ja asjaomastest tehisintellektitehnoloogiatest.
4. Asjaomane vastavushindamisasutus võib teavitatud asutuse toiminguid teha ainult juhul, kui komisjon või teised liikmesriigid ei esita vastuväiteid ühe kuu jooksul pärast teavitamist.
5. Teavitav asutus teavitab komisjoni ja teisi liikmesriike kõigist edaspidistest teavitusega seotud olulistest muudatustest.

Artikkel 33
Teavitatud asutused

1. Teavitatud asutused kontrollivad suure riskiga tehisintellektisüsteemi vastavust artiklis 43 osutatud vastavushindamismenetluse kohaselt.
2. Teavitatud asutused täidavad organisatsioonilisi, kvaliteedijuhtimise, ressursside ja protsessidega seotud nõudeid, mis on vajalikud nende ülesannete täitmiseks.
3. Teavitatud asutuste organisatsiooniline struktuur, vastutusalade jaotus, aruandlusahelad ja tegevus peavad olema sellised, et oleks võimalik tagada usaldus teavitatud asutuste tegevuse ja nende teostatud vastavushindamistoimingute tulemuste suhtes.
4. Teavitatud asutused peavad olema sõltumatud suure riskiga tehisintellektisüsteemi pakkujast, mille vastavushindamisega nad tegelevad. Samuti peavad teavitatud asutused olema sõltumatud mis tahes muust operaatorist, kellel on majanduslik huvi hinnatava suure riskiga tehisintellektisüsteemi vastu, ja kõigist pakkuja konkurentidest.
5. Teavitatud asutused korraldatakse ja neid juhitakse nii, et kindlustada nende tegevuse sõltumatus, objektiivsus ja erapooletus. Teavitatud asutused dokumenteerivad ja rakendavad struktuuri ja menetlused, millega kindlustada erapooletus ning mille abil edendada ja kohaldada erapooletuse põhimõtteid, mis hõlmavad kogu organisatsiooni, personali ja hindamistoiminguid.
6. Teavitatud asutustel peavad olema dokumenteeritud menetlused, millega tagatakse, et nende töötajad, komiteed, tütarettevõtjad, alltöövõtjad ja kõik nendega seotud asutused või väliste asutuste töötajad austavad vastavushindamistoimingute teostamise käigus saadud teabe konfidentsiaalsust, välja arvatud juhul, kui avalikustamine on seadusega nõutud. Teavitatud asutuste töötajad on kohustatud kaitsma ametisaladusena teavet, mille nad on saanud käesoleva määruse alusel oma

ülesandeid täites, välja arvatud suhetes selle liikmesriigi teavitavate asutustega, kus teavitatud asutus tegutseb.

7. Teavitatud asutustel peavad olema menetlused toimingute teostamiseks, mis võtavad asjakohaselt arvesse ettevõtja suurust, tegutsemisvaldkonda, tema struktuuri ning kõnealuse tehisintellektisüsteemi keerukuse astet.

8. Teavitatud asutused peavad võtma endale asjakohase vastutuskindlustuse seoses oma vastavushindamistoimingutega, välja arvatud juhul, kui vastutust kannab asjaomane liikmesriik vastavalt siseriiklikele õigusaktidele või kui see liikmesriik vastutab otseselt vastavushindamise eest.

9. Teavitatud asutused peavad olema võimelised täitma kõiki oma käesoleva määruse kohaseid ülesandeid suurima erialase usaldusväärsuse ja nõutava erialase pädevusega nii siis, kui neid ülesandeid täidavad teavitatud asutused ise, kui ka siis, kui seda tehakse nende nimel ja nende vastutusel.

10. Teavitatud asutustel peab olema piisav sisepädevus, et tulemuslikult hinnata väliste isikute poolt nende nimel täidetud ülesandeid. Selleks peab teavitatud asutusele olema igal ajal ja iga vastavushindamise ning igat liiki suure riskiga tehisintellektisüsteemi puhul, mille jaoks nad on määratud, alaliselt kättesaadav piisavalt haldus-, tehnilisi ja teadustöötajaid, kellel on kogemused ja teadmised asjaomaste tehisintellektitehnoloogiate, andmete ja andmetöötluse ja käesoleva jaotise 2. peatükis sätestatud nõuete alal.

11. Teavitatud asutused osalevad artiklis 38 osutatud koordineerimistegevuses. Samuti osalevad nad otseselt või esindajate kaudu Euroopa standardiorganisatsioonides või tagavad, et nad on asjakohastest standarditest teadlikud ja värskeima arenguga kursis.

12. Teavitatud asutused teevad kättesaadavaks ja esitavad taotluse korral kogu asjakohase dokumentatsiooni, sealhulgas pakkuja dokumentatsiooni, artiklis 30 osutatud teavitavale asutusele, et sel oleks võimalik teostada hindamis-, määramis-, teavitamis- ning seire- ja järelevalvetoiminguid ning hõlbustada käesolevas peatükis kirjeldatud hindamist.

Artikkel 34
Teavitatud asutuste tütarettevõtjad ja alltöövõtjad

1. Kui teavitatud asutus kasutab vastavushindamisega seotud ülesannete täitmiseks alltöövõtjat või tütarettevõtjat, tagab ta, et alltöövõtja või tütarettevõtja vastab artiklis 33 sätestatud nõuetele, ning teatab sellest teavitavale asutusele.

2. Teavitatud asutused vastutavad täielikult oma alltöövõtjate ja tütarettevõtjate täidetud ülesannete eest, olenemata sellest, kus need asuvad.

3. Alltöövõtjat või tütarettevõtjat võib kasutada ainult pakkuja nõusolekul.

4. Teavitatud asutused hoiavad teavitavale asutusele kättesaadavana dokumente, mis puudutavad alltöövõtja või tütarettevõtja kvalifikatsiooni hindamist ja nende poolt käesoleva määruse alusel tehtud tööd.

Artikkel 35

Käesoleva määruse alusel määratud teavitatud asutuste identifitseerimisnumbrid ja loetelud

1. Komisjon määrab teavitatud asutustele identifitseerimisnumbrid. Komisjon määrab üheainsa identifitseerimisnumbri, isegi kui asutusest teavitatakse mitme erineva liidu õigusakti alusel.

2. Komisjon teeb üldsusele kättesaadavaks käesoleva määruse alusel teavitatud asutuste loetelu, mis sisaldab ka asutustele määratud identifitseerimisnumbreid ja toiminguid, mille teostamiseks neist on teavitatud. Komisjon tagab, et seda loetelu ajakohastatakse.

Artikkel 36

Muudatused teavitustes

1. Kui teavitaval asutusel on kahtlusi või talle on teada antud, et teavitatud asutus ei vasta enam artiklis 33 sätestatud nõuetele või et ta ei täida oma kohustusi, siis uurib kõnealune teavitav asutus seda küsimust viivitamata ja äärmiselt hoolikalt. Seoses sellega teatab ta asjaomasele teavitatud asutusele tekkinud vastuväidetest ja annab talle võimaluse esitada oma seisukohad. Kui teavitav asutus on jõudnud järeldusele, et uurimisalune teatatud asutus ei vasta enam artiklis 33 sätestatud nõuetele või et ta ei täida oma kohustusi, siis vastavalt vajadusele seab teavitav asutus teavitusele piirangud või peatab või tühistab selle sõltuvalt nõuetele mittevastavuse raskusastmest. Lisaks teatab ta sellest viivitamata komisjonile ja teistele liikmesriikidele.

2. Kui teavitust piiratakse või kui see peatatakse või tühistatakse või kui teavitatud asutus on lõpetanud oma tegevuse, astub teavitav asutus vajalikud sammud selle tagamiseks, et kõnealuse teavitatud asutuse dokumendid võtaks üle mõni teine teavitatud asutus või et need oleksid vastutavatele teavitavatele asutustele nende taotluse peale kättesaadavad.

Artikkel 37

Teavitatud asutuste pädevuse vaidlustamine

1. Komisjon uurib vajaduse korral kõiki juhtumeid, mille puhul on põhjust kahelda, kas teavitatud asutus vastab artiklis 33 sätestatud nõuetele.

2. Teavitav asutus annab komisjonile taotluse alusel kogu teabe asjaomase teavitatud asutuse teavitamise kohta.

3. Komisjon tagab, et käesoleva artikli kohase uurimise käigus omandatud konfidentsiaalset teavet käsitatakse konfidentsiaalsena.

4. Kui komisjon on veendunud, et teavitatud asutus ei täida või on lakanud täitmast artiklis 33 sätestatud nõudeid, võtab ta vastu põhjendatud otsuse, milles nõutakse, et teavitav liikmesriik võtaks vajalikud parandusmeetmed, sealhulgas vajaduse korral tühistaks teavituse. Kõnealune rakendusakt võetakse vastu artikli 74 lõikes 2 osutatud kontrollimenetluse kohaselt.

Artikkel 38

Teavitatud asutuste koordineerimine

1. Komisjon tagab, et käesoleva määrusega hõlmatud valdkondades kehtestatakse asjakohane koordineerimine ja koostöö teavitatud asutuste vahel, kes tegelevad

tehisintellektisüsteemide vastavushindamisega vastavalt käesolevale määrusele, ning et see toimub nõuetekohaselt teavitatud asutuste valdkondliku rühma vormis.

2. Liikmesriigid tagavad oma teavitatud asutuste osalemise nimetatud rühma töös otseselt või määratud esindajate vahendusel.

Artikkel 39
Kolmandate riikide vastavushindamisasutused

Sellise kolmanda riigi õiguse alusel asutatud vastavushindamisasutusel, kellega liit on sõlminud lepingu, võidakse lubada tegutseda teavitatud asutusena käesoleva määruse alusel.

5. PEATÜKK

STANDARDID, VASTAVUSHINDAMINE, SERTIFIKAADID, REGISTREERIMINE

Artikkel 40
Harmoneeritud standardid

Eeldatakse, et suure riskiga tehisintellektisüsteemid, mis vastavad harmoneeritud standarditele või nende osadele, mille viited on avaldatud *Euroopa Liidu Teatajas*, on vastavuses käesoleva jaotise 2. peatükis sätestatud nõuetega niivõrd, kuivõrd nimetatud standardid hõlmavad neid nõudeid.

Artikkel 41
Ühtsed kirjeldused

1. Kui artiklis 40 osutatud harmoneeritud standardeid ei ole olemas või kui komisjon leiab, et asjaomased harmoneeritud standardid ei ole piisavad või et lahendada on vaja spetsiifilised ohutuse või põhiõigustega seotud probleemid, võib komisjon võtta rakendusaktidega vastu ühtsed kirjeldused käesoleva jaotise 2. peatükis sätestatud nõuete kohta. Need rakendusaktid võetakse vastu kooskõlas artikli 74 lõikes 2 osutatud kontrollimenetlusega.

2. Lõikes 1 osutatud ühtsete kirjelduste ettevalmistamise käigus kogub komisjon kokku asjaomaste asutuste või asjaomaste valdkondlike liidu õigusaktide alusel loodud eksperdirühmade arvamused.

3. Eeldatakse, et suure riskiga tehisintellektisüsteemid, mis vastavad lõikes 1 osutatud ühtsetele kirjeldustele, on vastavuses käesoleva jaotise 2. peatükis sätestatud nõuetega niivõrd, kuivõrd nimetatud ühtsed kirjeldused hõlmavad neid nõudeid.

4. Kui pakkujad ei täida lõikes 1 osutatud ühtseid kirjeldusi, peavad nad nõuetekohaselt põhjendama, et nad on võtnud kasutusele vähemalt nende kirjeldustega samaväärsed tehnilised lahendused.

Artikkel 42
Eeldatav vastavus teatavatele nõetele

1. Võttes arvesse suure riskiga tehisintellektisüsteemi sihtotstarvet, eeldatakse, et kui suure riskiga tehisintellektisüsteeme on treenitud ja testitud andmetega, mis puudutavad konkreetset geograafilist, käitumuslikku ja funktsionaalset olustikku, milles kasutamiseks on need süsteemid mõeldud, siis vastavad need süsteemid artikli 10 lõike 4 nõuetele.

2. Eeldatakse, et suure riskiga tehisintellektisüsteemid, mis on sertifitseeritud või mille kohta on välja antud vastavusdeklaratsioon Euroopa Parlamendi ja nõukogu määruse (EL) 2019/881[63] kohase küberturvalisuse sertifitseerimise kava alusel ning mille viited on avaldatud *Euroopa Liidu Teatajas*, vastavad käesoleva määruse artiklis 15 sätestatud küberturvalisuse nõuetele niivõrd, kuivõrd küberturvalisuse sertifikaat või vastavusdeklaratsioon või nende osad hõlmavad neid nõudeid.

Artikkel 43
Vastavushindamine

1. Kui pakkuja on rakendanud artiklis 40 osutatud harmoneeritud standardeid või, kui see on asjakohane, artiklis 41 osutatud ühtset kirjeldust, et tõendada III lisa punktis 1 loetletud suure riskiga tehisintellektisüsteemide vastavust käesoleva jaotise 2. peatükis sätestatud nõuetele, järgib pakkuja üht järgmistest menetlustest:

   (a) VI lisas osutatud sisekontrollil põhinev vastavushindamine;

   (b) VII lisas osutatud vastavushindamine, mis põhineb kvaliteedijuhtimissüsteemi ja tehnilise dokumentatsiooni hindamisel ning milles osaleb teavitatud asutus.

   Kui selle tõendamiseks, et suure riskiga tehisintellektisüsteem vastab käesoleva jaotise 2. peatükis sätestatud nõuetele, ei ole pakkuja rakendanud artiklis 40 osutatud harmoneeritud standardeid või on neid rakendanud vaid osaliselt või kui selliseid harmoneeritud standardeid ei ole olemas ja artiklis 41 osutatud ühtsed kirjeldused ei ole kättesaadavad, järgib pakkuja VII lisas sätestatud vastavushindamist.

   VII lisas osutatud vastavushindamise jaoks võib pakkuja valida mistahes teavitatud asutuse. Kui aga süsteemi kavatsevad kasutusele võtta õiguskaitse-, rände- või varjupaigaasutused või ELi institutsioonid, organid või asutused, tegutseb teavitatud asutusena olenevalt asjaoludest artikli 63 lõikes 5 või lõikes 6 osutatud turujärelevalveasutus.

2. III lisa punktides 2–8 osutatud suure riskiga tehisintellektisüsteemide puhul järgivad pakkujad VI lisas osutatud sisekontrollil põhinevat vastavushindamist, mille korral ei ole teavitatud asutuse osalemist ette nähtud. III lisa punkti 5 alapunktis b osutatud suure riskiga tehisintellektisüsteemide puhul, mille lasevad turule või võtavad kasutusele direktiivi 2013/36/EL kohaldamisalasse kuuluvad krediidiasutused, toimub vastavushindamine nimetatud direktiivi artiklites 97–101 osutatud protseduuri käigus.

3. Suure riskiga tehisintellektisüsteemide puhul, mille suhtes kohaldatakse II lisa A jaotises loetletud õigusakte, järgib pakkuja nende õigusaktide kohaselt nõutavat asjaomast vastavushindamist. Selliste suure riskiga tehisintellektisüsteemide suhtes kohaldatakse käesoleva jaotise 2. peatükis sätestatud nõudeid ning need nõuded on vastavushindamise osa. Kohaldatakse ka VII lisa punkte 4.3, 4.4, 4.5 ja punkti 4.6 viiendat lõiku.

   Teavitatud asutustel, kellest on teavitatud nende õigusaktide alusel, on selliseks hindamiseks õigus kontrollida, kas suure riskiga tehisintellektisüsteemid vastavad

[63] Euroopa Parlamendi ja nõukogu 17. aprilli 2019. aasta määrus (EL) 2019/881, mis käsitleb ENISAt (Euroopa Liidu Küberturvalisuse Amet) ning info- ja kommunikatsioonitehnoloogia küberturvalisuse sertifitseerimist ja millega tunnistatakse kehtetuks määrus (EL) nr 526/2013 (küberturvalisuse määrus) (ELT L 151, 7.6.2019, lk 1).

käesoleva jaotise 2. peatükis sätestatud nõuetele, tingimusel et nende teavitatud asutuste vastavust artikli 33 lõigetes 4, 9 ja 10 sätestatud nõuetele on hinnatud nende õigusaktide kohase teavitamismenetluse raames.

Kui II lisa A jaos loetletud õigusaktid võimaldavad toote valmistajal loobuda kolmanda isiku tehtavast vastavushindamisest, tingimusel et see valmistaja on rakendanud kõiki harmoneeritud standardeid, mis hõlmavad kõiki olulisi nõudeid, võib see valmistaja nimetatud võimalust kasutada ainult siis, kui ta rakendab ka harmoneeritud standardeid või, kui see on asjakohane, artiklis 41 osutatud ühtseid kirjeldusi, mis hõlmavad käesoleva jaotise 2. peatükis sätestatud nõudeid.

4. Suure riskiga tehisintellektisüsteemidele tuleb teha uus vastavushindamine alati, kui neid oluliselt muudetakse olenemata sellest, kas muudetud süsteemi kavatsetakse edasi turustada või jätkab selle kasutamist praegune kasutaja.

Kui tegemist on suure riskiga tehisintellektisüsteemiga, mis õpib edasi ka pärast turule laskmist või kasutusele võtmist, ei käsitata oluliste muudatustena tehisintellektisüsteemi ja selle toimimise muudatusi, mis on pakkuja poolt esialgse vastavushindamise ajal paika pandud ja mis sisalduvad IV lisa punkti 2 alapunktis f osutatud tehnilises dokumentatsioonis.

5. Komisjonil on õigus võtta kooskõlas artikliga 73 vastu delegeeritud õigusakte, et ajakohastada VI ja VII lisa eesmärgiga võtta kasutusele vastavushindamise elemente, mis muutuvad vajalikuks tehnika arengu tõttu.

6. Komisjonil on õigus võtta vastu delegeeritud õigusakte, et muuta lõikeid 1 ja 2, et kohaldada III lisa punktides 2–8 osutatud suure riskiga tehisintellektisüsteemide suhtes VII lisas osutatud vastavushindamist või selle osi. Komisjon arvestab sellised delegeeritud õigusakte vastu võttes seda, kui mõjus on VI lisas osutatud sisekontrollil põhinev vastavushindamine, et hoida ära või minimeerida tervist, ohutust ja põhiõiguste kaitset ähvardavaid riske, mida sellised süsteemid põhjustavad, ning piisava suutlikkuse ja ressursside kättesaadavust teavitatud asutustes.

Artikkel 44
Sertifikaadid

1. Teavitatud asutuste poolt VII lisa kohaselt välja antavad sertifikaadid koostatakse teavitatud asutuse asukoha liikmesriigi poolt kindlaks määratud liidu ametlikus keeles või mõnes muus teavitatud asutusele vastuvõetavas liidu ametlikus keeles.

2. Sertifikaat kehtib selles märgitud ajavahemiku jooksul, mis ei ületa viit aastat. Pakkuja taotlusel võib sertifikaadi kehtivust pikendada korraga mitte rohkem kui viie aasta kaupa, võttes aluseks kohaldatavate vastavushindamismenetluste kohaselt tehtava uue hindamise.

3. Kui teavitatud asutus leiab, et tehisintellektisüsteem ei vasta enam käesoleva jaotise 2. peatükis sätestatud nõuetele, peatab ta väljastatud sertifikaadi, tunnistab selle kehtetuks või kehtestab selle suhtes piirangud, võttes seejuures arvesse proportsionaalsuse põhimõtet, kui süsteemi pakkuja ei taga nimetatud nõuete täitmist asjakohaste parandusmeetmete võtmisega teavitatud asutuse poolt kindlaks määratud tähtajaks. Teavitatud asutus põhjendab oma otsust.

Artikkel 45
Teavitatud asutuste otsuste vaidlustamine

Liikmesriigid tagavad, et isikud, kellel on teavitatud asutuse otsuse vastu õigustatud huvi, saavad kasutada menetlust teavitatud asutuste otsuste vaidlustamiseks.

Artikkel 46
Teavitatud asutuste teavitamiskohustused

1. Teavitatud asutused informeerivad teavitavat asutust järgmisest:

   (a) kõik VII lisa nõuete kohaselt välja antud liidu tehnilise dokumentatsiooni hindamise sertifikaadid, nende sertifikaatide lisad, kvaliteedijuhtimissüsteemi kinnitused;

   (b) kõik VII lisa nõuete kohaselt välja antud liidu tehnilise dokumentatsiooni hindamise sertifikaadi või kvaliteedijuhtimissüsteemi kinnituse tagasilükkamise, piiramise, peatamise või kehtetuks tunnistamise juhtumid;

   (c) teavitamise ulatust või tingimusi mõjutavad asjaolud;

   (d) turujärelevalveasutustelt saadud teabenõuded vastavushindamistoimingute kohta;

   (e) taotluse korral vastavushindamistoimingud, mida nad teavituse sihtvaldkonnas on teinud, ja muu tegevus, sealhulgas piiriülesed toimingud ja alltöövõtt.

2. Iga teavitatud asutus informeerib teisi teavitatud asutusi järgmisest:

   (a) kvaliteedijuhtimissüsteemi kinnitamised, mille andmisest ta keeldus, mille ta peatas või tunnistas kehtetuks, ja taotluse korral ka välja antud kvaliteedisüsteemide kinnitamised;

   (b) ELi tehnilise dokumentatsiooni hindamise sertifikaadid või nende lisad, mille andmisest ta keeldus, mille ta tunnistas kehtetuks, peatas või mida ta muul moel piiras, ning taotluse korral sertifikaadid ja/või nende lisad, mis ta on välja andnud.

3. Iga teavitatud asutus esitab teistele samu tehisintellektitehnoloogiaid puudutavate samalaadsete vastavushindamistoimingutega tegelevatele teavitatud asutustele asjakohase teabe negatiivsete ja taotluse korral ka positiivsete vastavushindamistulemuste kohta.

Artikkel 47
Erand vastavushindamisest

1. Erandina artiklist 43 võib mis tahes turujärelevalveasutus anda loa lasta asjaomase liikmesriigi territooriumil turule või võtta kasutusele konkreetne suure riskiga tehisintellektisüsteem, kui selleks on erandkorras põhjust avaliku julgeoleku või inimeste elu ja tervise kaitse, keskkonnakaitse või oluliste tööstus- ja taristuvarade kaitse tõttu. Selline luba antakse piiratud ajaks, kuni toimuvad vajalikud vastavushindamismenetlused, ning see lõpeb, kui need menetlused läbi saavad. Need menetlused võetakse ette viivitamata.

2. Lõikes 1 osutatud luba antakse üksnes juhul, kui turujärelevalveasutus järeldab, et suure riskiga tehisintellektisüsteem vastab käesoleva jaotise 2. peatüki nõuetele.

Turujärelevalveasutus teavitab komisjoni ja teisi liikmesriike kõigist lõike 1 kohaselt antud lubadest.

3. Kui ükski liikmesriik ega komisjon ei ole esitanud vastuväiteid liikmesriigi turujärelevalveasutuse lõike 1 kohaselt välja antud loa kohta 15 kalendripäeva jooksul alates lõikes 2 osutatud teabe kättesaamisest, loetakse luba põhjendatuks.

4. Kui 15 kalendripäeva jooksul alates lõikes 2 osutatud teabe kättesaamisest esitab mõni liikmesriik vastuväiteid mõne teise liikmesriigi turujärelevalveasutuse välja antud loa kohta või kui komisjon leiab, et luba on vastuolus liidu õigusega või et lõikes 2 osutatud liikmesriikide järeldus süsteemi vastavuse kohta ei ole põhjendatud, alustab komisjon viivitamata konsultatsioone asjaomase liikmesriigiga; konsulteeritakse asjaomas(t)e operaatori(te)ga ning neil on võimalus esitada oma seisukohad. Komisjon otsustab seda arvesse võttes, kas luba on põhjendatud või ei. Komisjon adresseerib oma otsuse asjaomasele liikmesriigile ning asjaomas(t)ele operaatori(te)le.

5. Kui luba peetakse põhjendamatuks, tunnistab asjaomase liikmesriigi turujärelevalveasutus selle kehtetuks.

6. Kui tegemist on suure riskiga tehisintellektisüsteemidega, mis on mõeldud kasutamiseks toote turvakomponendina või mis on ise toode, milles suhtes kehtivad määrus (EL) 2017/745 ja määrus (EL) 2017/746, kohaldatakse määruse (EL) 2017/745 artiklit 59 ja määruse (EL) 2017/746 artiklit 54 erandina lõigetest 1–5 ka käesoleva jaotise 2. peatükis sätestatud nõuetele vastavuse hindamiseks tehtava vastavushindamise erandi suhtes.

Artikkel 48
ELi vastavusdeklaratsioon

1. Pakkuja koostab iga tehisintellektisüsteemi kohta kirjaliku ELi vastavusdeklaratsiooni ja säilitab seda riigi pädevate asutuste jaoks kättesaadavana vähemalt kümne aasta jooksul pärast tehisintellektisüsteemi turule laskmist või kasutusele võtmist. ELi vastavusdeklaratsioonis nimetatakse, millise tehisintellektisüsteemi kohta see on koostatud. Taotluse korral antakse ELi vastavusdeklaratsiooni koopia riigi asjaomastele pädevatele asutustele.

2. ELi vastavusdeklaratsioonis kinnitatakse, et kõnealune suure riskiga tehisintellektisüsteem vastab käesoleva jaotise 2. peatükis sätestatud nõuetele. ELi vastavusdeklaratsioon sisaldab V lisas sätestatud teavet ning see tõlgitakse liidu sellesse ametlikku keelde või nendesse ametlikesse keeltesse, mida nõuab liikmesriik või nõuavad liikmesriigid, kus suure riskiga tehisintellektisüsteem kättesaadavaks tehakse.

3. Kui suure riskiga tehisintellektisüsteemide suhtes kohaldatakse muid liidu ühtlustamisõigusakte, mille kohaselt on samuti nõutav ELi vastavusdeklaratsioon, koostatakse kõigi suure riskiga tehisintellektisüsteemi suhtes kohaldatavate liidu õigusaktide jaoks üks ainus ELi vastavusdeklaratsioon. Vastavusdeklaratsioon sisaldab kogu vajalikku teavet deklaratsiooniga seotud liidu ühtlustamisõigusaktide kindlakstegemiseks.

4. ELi vastavusdeklaratsiooni koostamisega võtab pakkuja vastutuse käesoleva jaotise 2. peatükis sätestatud nõuete täitmise eest. Pakkuja ajakohastab ELi vastavusdeklaratsiooni vastavalt vajadusele.

5. Komisjonil on õigus võtta kooskõlas artikliga 73 vastu delegeeritud õigusakte, et ajakohastada V lisas sätestatud ELi vastavusdeklaratsiooni sisu, et lisada sinna elemente, mis muutuvad vajalikuks tehnika arengust tulenevalt.

Artikkel 49
CE-vastavusmärgis

1. Suure riskiga tehisintellektisüsteemi CE-märgis kinnitatakse nähtaval, loetaval ja kustutamatul viisil. Kui see ei ole suure riskiga tehisintellektisüsteemi olemuse tõttu võimalik või otstarbekas, kinnitatakse märgis olenevalt asjaoludest kas pakendile või süsteemiga kaasas olevatele dokumentidele.

2. Käesoleva artikli lõikes 1 osutatud CE-märgise suhtes kohaldatakse määruse (EÜ) nr 765/2008 artiklis 30 sätestatud üldpõhimõtteid.

3. Vajaduse korral järgneb CE-märgisele artiklis 43 sätestatud vastavushindamismenetluste eest vastutava teavitatud asutuse identifitseerimisnumber. Identifitseerimisnumber esitatakse ka kõigis reklaammaterjalides, kus on öeldud, et suure riskiga tehisintellektisüsteem vastab CE-märgise nõuetele.

Artikkel 50
Dokumentide säilitamine

Pakkuja säilitab järgmisi dokumente riigi pädevate asutuste jaoks kättesaadavana kümne aasta jooksul pärast seda, kui tehisintellektisüsteem on turule lastud või kasutusele võetud:

(a) artiklis 11 osutatud tehniline dokumentatsioon;

(b) artiklis 17 osutatud kvaliteedijuhtimissüsteemi käsitlev dokumentatsioon;

(c) kui see on asjakohane, siis dokumendid muudatuste kohta, mille teavitatud asutused on heaks kiitnud;

(d) kui see on asjakohane, siis teavitatud asutuste tehtud otsused ja välja antud muud dokumendid;

(e) artiklis 48 osutatud ELi vastavusdeklaratsioon.

Artikkel 51
Registreerimine

Enne artikli 6 lõikes 2 osutatud suure riskiga tehisintellektisüsteemi turule laskmist või kasutusele võtmist registreerib pakkuja või vajaduse korral volitatud esindaja selle süsteemi artiklis 60 osutatud ELi andmebaasis.

IV JAOTIS

LÄBIPAISTVUSKOHUSTUSED TEATAVATE TEHISINTELLEKTISÜSTEEMIDE PUHUL

Artikkel 52
Läbipaistvuskohustused teatavate tehisintellektisüsteemide puhul

1. Pakkujad tagavad, et füüsiliste isikutega suhtlema mõeldud tehisintellektisüsteeme projekteeritakse ja arendatakse selliselt, et füüsilistele isikutele antakse teada, et nad suhtlevad tehisintellektisüsteemiga, välja arvatud juhul, kui see on asjaolude ja kasutamise konteksti tõttu ilmne. See kohustus ei kehti tehisintellektisüsteemide suhtes, mida on seadusega lubatud kasutada kuritegude avastamiseks, tõkestamiseks ja uurimiseks ning nende eest vastutusele võtmiseks, välja arvatud juhul, kui sellised süsteemid on üldsusele kättesaadavad, et kuritegudest teatada.

2. Emotsioonide tuvastamise süsteemi või biomeetrilise liigitamise süsteemi kasutajad annavad selle süsteemi tööst teada füüsilistele isikutele, kes selle süsteemiga kokku puutuvad. Seda kohustust ei kohaldata biomeetriliseks liigitamiseks kasutatavate tehisintellektisüsteemide suhtes, mida on seadusega lubatud kasutada kuritegude avastamiseks, tõkestamiseks ja uurimiseks.

3. Kasutaja, kes kasutab tehisintellektisüsteemi, mis loob või manipuleerib pildi-, audio-või videosisu, mis märkimisväärselt sarnaneb olemasolevate isikute, objektide, kohtade või muude olemite või sündmustega ja võib inimesele ekslikult tunduda ehtne või tõene (nn süvavõltsing), peab avalikustama, et sisu on kunstlikult loodud või seda on manipuleeritud.

   Esimest lõiku ei kohaldata siiski juhul, kui kasutamine on seadusega lubatud, et avastada, tõkestada ja uurida kuritegusid ja nende eest vastutusele võtta, või kui see on vajalik ELi põhiõiguste hartaga tagatud väljendusvabaduse ja kunsti ja teaduse vabaduse õiguse teostamiseks ning tingimusel, et kolmandate isikute õiguste ja vabaduste kaitseks kohaldatakse asjakohaseid kaitsemeetmeid.

4. Lõigete 1, 2 ja 3 kohaldamine ei mõjuta käesoleva määruse III jaotises sätestatud nõudeid ja kohustusi.

V JAOTIS

INNOVATSIOONI TOETAVAD MEETMED

Artikkel 53
Tehisintellekti regulatsiooni testkeskkonnad

1. Ühe või mitme liikmesriigi pädevate asutuste või Euroopa Andmekaitseinspektori loodud tehisintellekti regulatsiooni testkeskkondade näol on tegemist kontrollitud keskkonnaga, mis hõlbustab innovatiivsete tehisintellektisüsteemide arendamist, testimist ja valideerimist piiratud aja jooksul enne nende turule laskmist või kasutusele võtmist konkreetse kava kohaselt. See toimub pädevate asutuste otsese järelevalve ja juhendamise all, et oleks tagatud kooskõla käesoleva määruse nõuetega ja vajaduse korral muude testkeskkonnas jälgitavate liidu ja liikmesriikide õigusaktidega.

2. Liikmesriigid tagavad, et niivõrd, kuivõrd innovatiivsed tehisintellektisüsteemid on seotud isikuandmete töötlemisega või kuuluvad muul moel muude selliste riiklike asutuste või pädevate asutuste järelevalve alla, kes pakuvad või toetavad juurdepääsu andmetele, on riiklikud andmekaitseasutused ja kõnealused muud riikide asutused seotud tehisintellekti regulatsiooni testkeskkonnaga.

3. Tehisintellekti regulatsiooni testkeskkonnad ei mõjuta pädevate asutuste järelevalve- ja parandusvolitusi. Kui selliste süsteemide arendamise ja testimise käigus tehakse kindlaks oluline risk tervisele, ohutusele ja põhiõigustele, tuleb selle põhjal võtta viivitamata leevendusmeetmeid ja, kui see ei ole võimalik, arendamine ja testimine kuni riskide leevendamiseni peatada.

4. Tehisintellekti regulatsiooni testkeskkonnas osalejad vastutavad kohaldatavate liidu ja liikmesriikide vastutust käsitlevate õigusaktide alusel igasuguse kahju eest, mida testkeskkonnas toimuvad eksperimendid võivad kolmandatele isikutele põhjustada.

5. Liikmesriikide pädevad asutused, kes on loonud tehisintellekti regulatsiooni testkeskkonnad, koordineerivad oma tegevust ja teevad koostööd Euroopa tehisintellekti nõukojas. Nad esitavad nõukojale ja komisjonile igal aastal aruande nende kavade rakendamise kohta, kirjeldades muu hulgas süsteemiga seotud häid tavasid, saadud kogemusi ja soovitusi, ning, kui see on asjakohane, ka käesoleva määruse ja muude testkeskkonnas jälgitavate liidu õigusaktide kohaldamise kohta.

6. Tehisintellekti regulatsiooni testkeskkondade töökord ja -tingimused, kaasa arvatud kõlblikkuskriteeriumid ja taotluste esitamise, valiku-, osalemis- ja testkeskkonnast väljumise protseduurid ning osaliste õigused ja kohustused sätestatakse rakendusaktides. Need rakendusaktid võetakse vastu kooskõlas artikli 74 lõikes 2 osutatud kontrollimenetlusega.

Artikkel 54

Isikuandmete täiendav töötlemine tehisintellekti regulatsiooni testkeskkonnas teatavate tehisintellektisüsteemide arendamiseks avalikes huvides

1. Tehisintellekti regulatsiooni testkeskkonnas töödeldakse mujal seaduslikult kogutud isikuandmeid testkeskkonnas teatavate innovatiivsete tehisintellektisüsteemide arendamiseks ja testimiseks järgmistel tingimustel:

   (a) innovatiivseid tehisintellektisüsteeme arendatakse selleks, et kaitsta olulisi avalikke huve ühes või mitmes järgmises valdkonnas:

      i) süütegude tõkestamine, uurimine, avastamine või nende eest vastutusele võtmine või kriminaalkaristuste täitmisele pööramine, sealhulgas avalikku julgeolekut ähvardavate ohtude eest kaitsmine ja nende ennetamine, pädevate asutuste kontrolli all ja vastutusel. Töötlemine toimub liikmesriigi või liidu õiguse alusel;

      ii) avalik julgeolek ja rahvatervis, kaasa arvatud haiguste ennetamine, tõrje ja ravi;

      iii) keskkonna kvaliteedi kõrgetasemeline kaitse ja parandamine;

   (b) töödeldud andmeid on vaja, et täita üht või mitut III jaotise 2. peatükis osutatud nõuet, kui neid nõudeid ei saa tulemuslikult täita anonüümitud andmete, tehisandmete või muude isikustamata andmete töötlemisega;

(c) olemas on mõjusad seiremehhanismid, et teha kindlaks, kas testkeskkonnas toimuvate eksperimentide ajal võib tekkida riske seoses andmesubjektide põhiõigustega, ning reageerimismehhanism, mis võimaldab neid riske kiiresti leevendada ja vajaduse korral andmete töötlemise peatada;

(d) testkeskkonnas töödeldavad isikuandmed paiknevad funktsionaalselt eraldiseisvas, isoleeritud ja kaitstud andmetöötluskeskkonnas osaliste kontrolli all ning neile on juurdepääs ainult volitatud isikutel;

(e) töödeldud isikuandmeid ei tohi edastada ega üle anda ning need ei tohi olla teistele isikutele muul moel kättesaadavad;

(f) isikuandmete töötlemine testkeskkonnas ei too kaasa andmesubjekte mõjutavaid meetmeid või otsuseid;

(g) testkeskkonnas töödeldud isikuandmed kustutatakse, kui osalemine testkeskkonnas lõpeb või isikuandmete säilitamisperiood saab läbi;

(h) isikuandmete testkeskkonnas töötlemise logisid hoitakse alles testkeskkonnas osalemise ajal ja 1 aasta jooksul pärast selle lõppu üksnes selleks ja nii kaua kui on vajalik käesolevast artiklist või muudest kohaldatavatest liidu või liikmesriikide õigusaktidest tulenevate aruande- ja dokumenteerimiskohustuste täitmiseks;

(i) tehisintellektisüsteemi treenimise, testimise ja valideerimise protsessi ja põhjenduste täielikku ja üksikasjalikku kirjeldust säilitatakse koos testimistulemustega IV lisas osutatud tehnilises dokumentatsioonis;

(j) testkeskkonnas arendatud tehisintellektiprojekti, selle eesmärkide ja eeldatavate tulemuste lühiülevaade avaldatakse pädevate asutuste veebisaidil.

2. Lõige 1 ei piira liidu ega liikmesriikide õigusaktide kohaldamist, mis välistavad töötlemise muul otstarbel kui neis õigusaktides selgelt nimetatud eesmärkidel.

Artikkel 55
Meetmed väikepakkujate ja -kasutajate kohta

1. Liikmesriigid teevad järgmist:

(a) annavad väikepakkujatele ja idufirmadele eelisjuurdepääsu tehisintellekti regulatsiooni testkeskkonnale, eeldusel et nad vastavad tingimustele;

(b) korraldavad just väikepakkujate ja -kasutajate vajadustest lähtuvaid konkreetseid teadlikkuse suurendamise üritusi käesoleva määruse kohaldamise kohta;

(c) kui see on asjakohane, siis loovad spetsiaalse kanali väikepakkujate ja -kasutajate ning muude innovaatoritega suhtlemiseks, et anda juhiseid ja vastata päringutele käesoleva määruse rakendamise kohta.

2. Artikli 43 kohase vastavushindamise tasude kehtestamisel võetakse arvesse väikepakkujate erihuve ning vähendatakse neid tasusid proportsionaalselt, lähtudes väikepakkujate suurusest ja turu suurusest.

VI JAOTIS

JUHTIMINE

1. PEATÜKK

EUROOPA TEHISINTELLEKTI NÕUKODA

Artikkel 56
Euroopa tehisintellekti nõukoja loomine

1. Luuakse Euroopa tehisintellekti nõukoda (edaspidi „nõukoda“).

2. Nõukoda annab komisjonile nõu ja abi, et:

   (a) aidata kaasa riiklike järelevalveasutuste ja komisjoni tulemuslikule koostööle käesoleva määrusega hõlmatud küsimustes;

   (b) koordineerida ja toetada komisjoni ja riiklike järelevalveasutuste ja muude pädevate asutuste poolset juhendamist ja analüüsi käesoleva määruse kohaldamisalasse kuuluvates valdkondades esile kerkivates küsimustes;

   (c) abistada riiklikke järelevalveasutusi ja komisjoni käesoleva määruse järjepideva kohaldamise tagamisel.

Artikkel 57
Nõukoja ülesehitus

1. Nõukoda koosneb riiklikest järelevalveasutustest, keda esindab asutuse juht või samaväärne kõrge ametnik, ning Euroopa Andmekaitseinspektorist. Koosolekutele võib kutsuda muid riiklikke asutusi, kui arutlusel olevad küsimused on nende jaoks olulised.

2. Nõukoda võtab oma töökorra vastu liikmete lihthäälteenamusega pärast komisjoni nõusoleku saamist. Töökorras tuleb kirjeldada artiklis 58 loetletud nõukoja ülesannete täitmisega seotud tegevusalaseid aspekte. Nõukoda võib vastavalt vajadusele moodustada konkreetsete küsimuste uurimiseks alamrühmi.

3. Nõukoja eesistuja on komisjon. Komisjon kutsub kokku koosolekud ja valmistab ette päevakorra vastavalt nõukoja käesolevast määrusest tulenevatele ülesannetele ja nõukoja töökorrale. Komisjon pakub nõukoja käesoleva määruse kohaseks tegevuseks haldus- ja analüütilist tuge.

4. Nõukoda võib kutsuda koosolekutel osalema väliseksperte ja vaatlejaid ning korraldada arvamustevahetusi huvitatud kolmandate isikutega, et toetada oma tegevust asjakohases ulatuses. Selleks võib komisjon hõlbustada suhtlust nõukoja ja muude liidu organite, asutuste ja nõuanderühmade vahel.

Artikkel 58
Nõukoja ülesanded

Komisjonile artikli 56 lõike 2 kohaselt nõu ja abi andes teeb nõukoda eelkõige järgmist:

(a) kogub ja jagab eksperditeadmisi ja parimaid tavasid liikmesriikides;

(b) aitab edendada liikmesriikides ühesuguseid haldustavasid, sh artiklis 53 osutatud regulatsiooni testkeskkondade toimimise jaoks;

(c) annab välja arvamusi, soovitusi või kirjalikke seisukohti käesoleva määruse rakendamisega seotud küsimustes, eeskätt järgmise kohta:

i) III jaotise 2. peatükis sätestatud nõudeid käsitlevad tehnilised kirjeldused või olemasolevad standardid,

ii) artiklites 40 ja 41 osutatud harmoneeritud standardite või ühtsete kirjelduste kasutamine,

iii) juhenddokumentide, sh artiklis 71 osutatud haldustrahvide määramise suuniste ettevalmistamine.

2. PEATÜKK

RIIKIDE PÄDEVAD ASUTUSED

Artikkel 59
Riikide pädevate asutuste määramine

1. Iga liikmesriik asutab või määrab riigi pädevad asutused, et tagada käesoleva määruse kohaldamine ja rakendamine. Riigi pädevad asutused korraldatakse nii, et kindlustada nende tegevuse ja ülesannete objektiivsus ja erapooletus.

2. Iga liikmesriik määrab riigi pädevate asutuste hulka riikliku järelevalveasutuse. Riiklik järelevalveasutus tegutseb teavitava asutuse ja turujärelevalveasutusena, välja arvatud juhul, kui liikmesriigil on korralduslikke või halduslikke põhjuseid määrata rohkem kui üks asutus.

3. Liikmesriigid teavitavad komisjoni enda määratud asutusest või asutustest ja esitavad vajaduse korral põhjused, miks nad on määranud mitu asutust.

4. Liikmesriigid tagavad, et riigi pädevatel asutustel on käesolevast määrusest tulenevate ülesannete täitmiseks piisavad rahalised ja inimressursid. Eeskätt peab riigi pädevatele asutustele olema pidevalt kättesaadav piisavalt töötajaid, kelle pädevuste ja eksperditeadmiste hulka kuuluvad põhjalik arusaamine tehisintellekti tehnoloogiatest, andmetest ja andmetöötlusest, põhiõigustest ja tervise ja ohutusega seotud riskidest ning teadmised kehtivatest standarditest ja õiguslikest nõuetest.

5. Liikmesriigid esitavad komisjonile igal aastal aruande riigi pädevate asutuste rahaliste ja inimressursside seisu kohta, hinnates sealjuures nende piisavust. Komisjon edastab selle teabe nõukojale arutamiseks ja võimalikeks soovitusteks.

6. Komisjon hõlbustab riikide pädevate asutuste vahelist kogemuste vahetamist.

7. Riigi pädevad asutused võivad anda juhiseid ja nõu käesoleva määruse rakendamise kohta, sh väikepakkujatele. Kui riigi pädevad asutused kavatsevad anda juhiseid ja nõu tehisintellektisüsteemi kohta valdkondades, mille suhtes kehtivad ka muud liidu õigusaktid, konsulteeritakse vastavalt vajadusele nende liidu õigusaktide alusel pädevate riiklike asutustega. Liikmesriigid võivad luua operaatoritega suhtlemiseks ka ühe keskse kontaktpunkti.

8. Kui liidu institutsioonid, organid ja asutused kuuluvad käesoleva määruse kohaldamisalasse, tegutseb nende järelevalve teostamisel pädeva asutusena Euroopa Andmekaitseinspektor.

VII JAOTIS

ERALDISEISVATE SUURE RISKIGA TEHISINTELLEKTISÜSTEEMIDE ELi ANDMEBAAS

Artikkel 60
Eraldiseisvate suure riskiga tehisintellektisüsteemide ELi andmebaas

1. Komisjon loob koostöös liikmesriikidega ELi andmebaasi, mis sisaldab lõikes 2 osutatud teavet artikli 6 lõikes 2 osutatud suure riskiga tehisintellektisüsteemide kohta, mis on registreeritud vastavalt artiklile 51, ning haldab seda.

2. Pakkujad sisestavad VIII lisas loetletud andmed ELi andmebaasi. Komisjon pakub neile tehnilist ja halduslikku toetust.

3. ELi andmebaasis sisalduv teave on üldsusele juurdepääsetav.

4. ELi andmebaas sisaldab isikuandmeid ainult niivõrd, kuivõrd see on vajalik käesoleva määruse kohaseks teabe kogumiseks ja töötlemiseks. See teave hõlmab nende füüsiliste isikute nimesid ja kontaktandmeid, kes vastutavad süsteemi registreerimise eest ja on volitatud pakkujat esindama.

5. ELi andmebaasi vastutav töötleja on komisjon. Ühtlasi tagab komisjon pakkujatele piisava tehnilise ja halduslikku toetuse.

VIII JAOTIS

TURUSTAMISJÄRGNE SEIRE, TEABE JAGAMINE, TURUJÄRELEVALVE

1. PEATÜKK

TURUSTAMISJÄRGNE SEIRE

Artikkel 61
Pakkujapoolne turustamisjärgne seire ja suure riskiga tehisintellektisüsteemide turustamisjärgse seire kava

1. Pakkujad kehtestavad turustamisjärgse seire süsteemi ja dokumenteerivad selle viisil, mis on proportsionaalne tehisintellektitehnoloogiate olemuse ja suure riskiga tehisintellektisüsteemi riskidega.

2. Turustamisjärgse seire süsteem peab aktiivselt ja süstemaatiliselt koguma, dokumenteerima ja analüüsima kasutajate esitavaid või muudest allikatest kogutavaid asjakohaseid andmeid suure riskiga tehisintellektisüsteemide toimimise kohta kogu nende eluea jooksul ning võimaldama pakkujal hinnata, kas tehisintellektisüsteemid vastavad jätkuvalt III jaotise 2. peatükis sätestatud nõuetele.

3. Turustamisjärgse seire süsteem peab põhinema turustamisjärgse seire kaval. Turustamisjärgse seire kava on IV lisas osutatud tehnilise dokumentatsiooni osa. Komisjon võtab vastu rakendusakti, millega nähakse ette üksikasjalikud sätted

turustamisjärgse seire kava vormi ja kavas sisalduvate elementide loetelu kehtestamise kohta.

4. Kui tegemist on II lisas osutatud õigusaktide kohaldamisalasse kuuluva suure riskiga tehisintellektisüsteemiga, mille turustamisjärgse seire süsteem ja kava on nende õigusaktide alusel juba kehtestatud, lisatakse lõigetes 1, 2 ja 3 kirjeldatud elemendid nimetatud süsteemi ja kavasse nii, nagu on asjakohane.

Esimest lõiku kohaldatakse ka III lisa punkti 5 alapunktis b osutatud suure riskiga tehisintellektisüsteemide suhtes, mille on turule lasknud või kasutusele võtnud direktiivi 2013/36/EL kohaldamisalasse kuuluv krediidiasutus.

2. PEATÜKK

TEABE JAGAMINE INTSIDENTIDE JA TÕRGETE KOHTA

Artikkel 62
Tõsistest intsidentidest ja tõrgetest teatamine

1. Liidu turule lastud suure riskiga tehisintellektisüsteemide pakkujad teatavad igast kõnealuste süsteemide tõsisest intsidendist või tõrkest, mille puhul on tegu põhiõiguste kaitseks mõeldud liidu õiguse kohaste kohustuste rikkumisega, nende liikmesriikide turujärelevalveasutustele, kus intsident või rikkumine aset leidis.

Teatamine peab toimuma kohe pärast seda, kui pakkuja on teinud kindlaks, et tehisintellektisüsteemi ja intsidendi või tõrke vahel on põhjuslik seos või et selline seos on põhjendatult tõenäoline, ning igal juhul hiljemalt 15 päeva pärast seda, kui pakkuja sai tõsisest intsidendist või tõrkest teadlikuks.

2. Kui turujärelevalveasutus saab teate selle kohta, et rikutud on põhiõiguste kaitseks mõeldud liidu õiguse kohaseid kohustusi, teatab ta sellest artikli 64 lõikes 3 osutatud riiklikele ametiasutustele või organitele. Komisjon töötab välja eraldi juhendi, et hõlbustada lõikes 1 sätestatud kohustuste täitmist. Juhend antakse välja hiljemalt 12 kuud pärast käesoleva määruse jõustumist.

3. III lisa punkti 5 alapunktis b osutatud suure riskiga tehisintellektisüsteemide puhul, mille lasevad turule või võtavad kasutusele pakkujad, kes on direktiivi 2013/36/EL kohaldamisalasse kuuluvad krediidiasutused, ja suure riskiga tehisintellektisüsteemide puhul, mis on selliste seadmete turvakomponendid või mis on ise sellised seadmed, mille suhtes kohaldatakse määrust (EL) 2017/745 ja määrust (EL) 2017/746, piirdutakse tõsistest intsidentidest või tõrgetest teatamisel selliste intsidentide ja tõrgetega, mille korral on tegemist põhiõiguste kaitseks mõeldud liidu õiguse kohaste kohustuste rikkumisega.

3. PEATÜKK

TÄITMISE TAGAMINE

Artikkel 63
Tehisintellektisüsteemide turujärelevalve ja kontroll liidu turul

1. Käesoleva määruse kohaldamisalasse kuuluvate tehisintellektisüsteemide suhtes kohaldatakse määrust (EL) 2019/1020. Käesoleva määruse tulemusliku täitmise tagamiseks:

(a) käsitatakse kõiki määruse (EL) 2019/1020 kohaseid viiteid ettevõtjatele viidetena, mis hõlmavad kõiki käesoleva määruse III jaotise 3. peatükis kindlaks määratud operaatoreid;

(b) käsitatakse kõiki määruse (EL) 2019/1020 kohaseid viiteid toodetele viidetena, mis hõlmavad kõiki käesoleva määruse kohaldamisalasse kuuluvaid tehisintellektisüsteeme.

2. Riiklik järelevalveasutus esitab komisjonile regulaarselt aruandeid asjakohaste turujärelevalvetoimingute tulemuste kohta. Riiklik järelevalveasutus esitab komisjonile ja asjaomastele riiklikele konkurentsiasutustele viivitamata kogu turujärelevalvetoimingute käigus kindlaks tehtud teabe, mis võib pakkuda huvi liidu konkurentsiõiguse kohaldamise seisukohast.

3. Käesoleva määruse kohaldamisel on II lisa A jaos loetletud õigusaktidega reguleeritud toodetega seotud suure riskiga tehisintellektisüsteemide puhul turujärelevalveasutuseks nende õigusaktide alusel määratud ametiasutus, kes vastutab turujärelevalvetoimingute eest.

4. Käesoleva määruse kohaldamisel on finantsteenuseid käsitlevate liidu õigusaktidega reguleeritud finantsasutuste poolt turule lastud, kasutusele võetud või kasutatavate tehisintellektisüsteemide puhul turujärelevalveasutuseks asjaomane ametiasutus, kes vastutab kõnealuste õigusaktide kohaselt nende asutuste finantsjärelevalve eest.

5. Tehisintellektisüsteemide puhul, mis on loetletud III lisa punkti 1 alapunktis a (niivõrd, kuivõrd neid süsteeme kasutatakse õiguskaitse eesmärgil) ning punktides 6 ja 7, määravad liikmesriigid käesoleva määruse kohaldamisel turujärelevalveasutuseks kas direktiivi (EL) 2016/680 või määruse 2016/679 kohaselt pädeva andmekaitse järelevalveasutuse või riigi pädeva asutuse, kes tegeleb selliste õiguskaitse-, rände- või varjupaigaasutuste tegevuse järelevalvega, kes võtavad selliseid süsteeme kasutusele või kasutavad neid.

6. Kui liidu institutsioonid, organid ja asutused kuuluvad käesoleva määruse kohaldamisalasse, tegutseb nende turujärelevalveasutusena Euroopa Andmekaitseinspektor.

7. Liikmesriigid hõlbustavad koordineerimist käesoleva määruse alusel määratud turujärelevalveasutuste ja muude asjaomaste riiklike asutuste või organite vahel, kes teevad järelevalvet II lisas loetletud liidu ühtlustamisõigusaktide või muude III lisas osutatud suure riskiga tehisintellektisüsteemide seisukohast oluliste liidu õigusaktide kohaldamise üle.

Artikkel 64
Juurdepääs andmetele ja dokumentatsioonile

1. Turujärelevalveasutustele antakse seoses nende tegevusega täielik juurdepääs pakkuja kasutatud treenimis-, valideerimis- ja testimisandmestikele, muu hulgas rakendusliideste (APIde) või muude sobivate kaugjuurdepääsu võimaldavate tehniliste vahendite ja tööriistade kaudu.

2. Kui see on vajalik, et hinnata suure riskiga tehisintellektisüsteemi vastavust III jaotise 2. peatükis sätestatud nõuetele, ja põhjendatud taotluse alusel antakse turujärelevalveasutustele juurdepääs tehisintellektisüsteemi lähtekoodile.

3. Riiklikel ametiasutustel või organitel, kes tegelevad põhiõiguste kaitse alastest liidu õigusaktidest tulenevate kohustuste täitmise järelevalve või tagamisega seoses

III lisas osutatud suure riskiga tehisintellektisüsteemide kasutamisega, on õigus taotleda mis tahes dokumentatsiooni, mis on loodud või mida hoitakse käesoleva määruse alusel, ja saada sellele juurdepääs, kui juurdepääs sellisele dokumentatsioonile on vajalik nende ülesannetest tulenevate kohustuste täitmiseks nende jurisdiktsiooni piires. Asjaomane avaliku sektori asutus või organ teatab igast sellisest taotlusest asjaomase liikmesriigi turujärelevalveasutusele.

4. Hiljemalt kolm kuud pärast käesoleva määruse jõustumist nimetab iga liikmesriik lõikes 3 osutatud ametiasutused või organid ning teeb nende loetelu riikliku järelevalveasutuse veebisaidil üldsusele kättesaadavaks. Liikmesriigid teavitavad loetelust komisjoni ja teisi liikmesriike ning ajakohastavad seda.

5. Kui lõikes 3 osutatud dokumentatsioon ei ole piisav, et teha kindlaks, kas põhiõiguste kaitseks mõeldud liidu õiguse kohaseid kohustusi on rikutud, võib lõikes 3 osutatud ametiasutus või organ esitada turujärelevalveasutusele põhjendatud taotluse korraldada suure riskiga tehisintellektisüsteemi testimine tehniliste vahendite abil. Turujärelevalveasutus korraldab testimise mõistliku aja jooksul pärast taotluse esitamist tihedas koostöös taotluse esitanud ametiasutuse või organiga.

6. Lõikes 3 osutatud riiklike ametiasutuste või organite poolt käesoleva artikli sätete kohaselt saadud teabe ja dokumentatsiooni käsitlemisel täidetakse artiklis 70 sätestatud konfidentsiaalsuskohustusi.

Artikkel 65

Riiklikul tasemel riski tekitava tehisintellektisüsteemiga tegelemise menetlus

1. Riski tekitavat tehisintellektisüsteemi käsitatakse määruse (EL) 2019/1020 artikli 3 punktis 19 määratletud ohtliku tootena niivõrd, kuivõrd tegemist on tervise või ohutuse või isikute põhiõiguste kaitsega seotud riskidega.

2. Kui liikmesriigi turujärelevalveasutusel on piisavalt põhjust uskuda, et tehisintellektisüsteem tekitab lõikes 1 osutatud riski, korraldab ta asjaomase tehisintellektisüsteemi hindamise, et selgitada välja, kas süsteem vastab käesolevas määruses sätestatud nõuetele ja kohustustele. Kui esineb põhiõiguste kaitsega seotud risk, teavitab turujärelevalveasutus sellest ka artikli 64 lõikes 3 osutatud asjaomaseid riiklikke ametiasutusi või organeid. Asjaomased operaatorid teevad vastavalt vajadusele koostööd turujärelevalveasutuste ja muude artikli 64 lõikes 3 osutatud riiklike ametiasutuste või organitega.

   Kui turujärelevalveasutus leiab nimetatud hindamise käigus, et tehisintellektisüsteem ei vasta käesolevas määruses sätestatud nõuetele ja kohustustele, nõuab ta viivitamata, et asjaomane operaator võtaks vastavalt tema ettekirjutusele kõik vajalikud parandusmeetmed, et tehisintellektisüsteem nimetatud nõuetega vastavusse viia, turult kõrvaldada või tagasi nõuda mõistliku aja jooksul, mis vastab riski olemusele.

   Turujärelevalveasutus teavitab sellest asjaomast teavitatud asutust. Teises lõigus osutatud meetmete suhtes kohaldatakse määruse (EL) nr 2019/1020 artiklit 18.

3. Kui turujärelevalveasutus on seisukohal, et nõuetele mittevastavus ei piirdu üksnes tema liikmesriigi territooriumiga, teavitab ta komisjoni ja teisi liikmesriike hindamistulemustest ja meetmetest, mille võtmist ta on operaatorilt nõudnud.

4. Operaator tagab, et kõigi asjaomaste, tema poolt liidu turul kättesaadavaks tehtud tehisintellektisüsteemide suhtes võetakse kõik vajalikud parandusmeetmed.

5. Kui tehisintellektisüsteemi operaator ei võta lõikes 2 osutatud ajavahemiku jooksul piisavaid parandusmeetmeid, võtab turujärelevalveasutus kõik sobivad ajutised meetmed, et keelata või piirata tehisintellektisüsteemi kättesaadavaks tegemist oma siseriiklikul turul, toode turult kõrvaldada või tagasi nõuda. See asutus teavitab komisjoni ja teisi liikmesriike nimetatud meetmetest viivitamata.

6. Lõikes 5 osutatud teave sisaldab kõiki kättesaadavaid üksikasju, eelkõige nõuetele mittevastava tehisintellektisüsteemi identifitseerimiseks vajalikke andmeid, tehisintellektisüsteemi päritolu, väidetava mittevastavuse ja riski olemust, võetud riiklike meetmete olemust ja kestust ning asjaomase operaatori esitatud seisukohti. Turujärelevalveasutused märgivad eelkõige ära, kas nõuetele mittevastavus on tingitud ühest või mitmest järgmisest asjaolust:

   (a) tehisintellektisüsteemi mittevastavus III jaotise 2. peatükis sätestatud nõuetele;

   (b) puudused artiklites 40 ja 41 osutatud harmoneeritud standardites või ühtsetes kirjeldustes, mille alusel vastavust eeldatakse.

7. Muude liikmesriikide kui menetluse algatanud liikmesriigi turujärelevalveasutused teavitavad komisjoni ja teisi liikmesriike viivitamata kõigist võetud meetmetest ja muust nende käsutuses olevast täiendavast teabest seoses asjaomase tehisintellektisüsteemi mittevastavusega ning, kui nad ei ole teadaantud riigisisese meetmega nõus, siis ka oma vastuväidetest.

8. Kui kolme kuu jooksul alates lõikes 5 osutatud teabe kättesaamisest ei ole teised liikmesriigid ega komisjon esitanud vastuväiteid liikmesriigi ajutise meetme suhtes, loetakse meede põhjendatuks. See ei piira asjaomase operaatori määruse (EL) 2019/1020 artikli 18 kohaseid menetlusõigusi.

9. Kõigi liikmesriikide turujärelevalveasutused tagavad, et asjaomase toote suhtes võetakse viivitamata asjakohased piiravad meetmed, näiteks kõrvaldatakse toode liikmesriigi turult.

Artikkel 66
Liidu kaitsemeetmete menetlus

1. Kui kolme kuu jooksul alates artikli 65 lõikes 5 osutatud teavituse kättesaamisest esitab mõni liikmesriik vastuväite teise liikmesriigi võetud meetme suhtes või kui komisjon leiab, et meede on liidu õigusega vastuolus, alustab komisjon viivitamata konsultatsioone asjaomase liikmesriigi ja operaatori või operaatoritega ning hindab riiklikku meedet. Selle hindamise tulemuste põhjal otsustab komisjon 9 kuu jooksul alates artikli 65 lõikes 5 osutatud teate saamisest, kas riiklik meede on põhjendatud või ei, ning teatab oma otsuse asjaomasele liikmesriigile.

2. Kui riiklik meede loetakse põhjendatuks, siis võtavad kõik liikmesriigid vajalikud meetmed, et tagada mittevastava tehisintellektisüsteemi kõrvaldamine oma turgudelt, ja teavitavad sellest komisjoni. Kui riiklik meede loetakse põhjendamatuks, tunnistab asjaomane liikmesriik selle kehtetuks.

3. Kui riiklik meede loetakse põhjendatuks ja tehisintellektisüsteemi nõuetele mittevastavus tuleneb puudustest käesoleva määruse artiklites 40 ja 41 osutatud harmoneeritud standardites või ühtsetes kirjeldustes, kohaldab komisjon määruse (EL) nr 1025/2012 artiklis 11 sätestatud menetlust.

Artikkel 67
Nõuetele vastavad tehisintellektisüsteemid, mis põhjustavad riski

1. Kui liikmesriigi turujärelevalveasutus leiab pärast artikli 65 kohast hindamist, et tehisintellektisüsteem, mis on kooskõlas käesoleva määruse nõuetega, põhjustab sellest hoolimata riski isikute tervisele või ohutusele, põhiõiguste kaitseks mõeldud liidu õiguse kohaste kohustuste täitmisele või avalike huvide kaitsmise muudele aspektidele, nõuab ta, et asjaomane operaator võtaks vastavalt tema ettekirjutusele kõik vajalikud meetmed tagamaks, et asjaomane tehisintellektisüsteem ei põhjusta turule laskmise või kasutusele võtmise korral enam sellist riski, kõrvaldaks asjaomase tehisintellektisüsteemi turult või nõuaks selle tagasi mõistliku aja jooksul, mis vastab riski olemusele.

2. Pakkuja või muud asjaomased operaatorid tagavad, et parandusmeetmed võetakse kõigi asjaomaste tehisintellektisüsteemide suhtes, mille nad on liidu turul kättesaadavaks teinud, lõikes 1 osutatud liikmesriigi turujärelevalveasutuse ettekirjutuse kohase tähtaja jooksul.

3. Liikmesriik teavitab sellest viivitamata komisjoni ja teisi liikmesriike. Teave peab sisaldama kõiki teadaolevaid üksikasju, eelkõige asjaomase tehisintellektisüsteemi tuvastamiseks vajalikke andmeid, tehisintellektisüsteemi päritolu ja tarneahelat, kaasneva riski olemust ning liikmesriigi võetud meetmete olemust ja kestust.

4. Komisjon alustab viivitamata konsulteerimist liikmesriikidega ja asjaomas(t)e operaatori(te)ga ning hindab võetud riiklikke meetmeid. Nimetatud hinnangu tulemuste põhjal otsustab komisjon, kas meede on põhjendatud või mitte, ning teeb vajaduse korral ettepaneku sobivate meetmete kohta.

5. Komisjon adresseerib oma otsuse liikmesriikidele.

Artikkel 68
Formaalne mittevastavus

1. Kui mõne liikmesriigi turujärelevalveasutus on avastanud ühe järgmistest asjaoludest, nõuab ta, et asjaomane pakkuja lõpetaks asjaomase mittevastavuse:

   (a) vastavusmärgise kinnitamisel ei ole järgitud artikli 49 nõudeid;

   (b) vastavusmärgist ei ole kinnitatud;

   (c) ELi vastavusdeklaratsiooni ei ole koostatud;

   (d) ELi vastavusdeklaratsioon ei ole koostatud õigesti;

   (e) vastavushindamises osaleva teavitatud asutuse identifitseerimisnumbrit ei ole kinnitatud, kui see on asjakohane.

2. Kui lõikes 1 osutatud mittevastavust ei kõrvaldata, võtab asjaomane liikmesriik kõik vajalikud meetmed tehisintellektisüsteemi turul kättesaadavaks tegemise piiramiseks või keelamiseks või tagab selle tagasinõudmise või kõrvaldamise turult.

IX JAOTIS

KÄITUMISJUHENDID

Artikkel 69
Käitumisjuhendid

1. Komisjon ja liikmesriigid edendavad ja hõlbustavad selliste käitumisjuhendite koostamist, mille eesmärk on soodustada III jaotise 2. peatükis sätestatud nõuete vabatahtlikku kohaldamist tehisintellektisüsteemide suhtes, mis ei ole suure riskiga tehisintellektisüsteemid, toetudes tehnilistele kirjeldustele ja lahendustele, mille abil saab otstarbekalt tagada selliste nõuete täitmise, arvestades nende süsteemide sihtotstarvet.

2. Komisjon ja nõukoda edendavad ja hõlbustavad selliste käitumisjuhendite koostamist, mille eesmärk on soodustada selliste nõuete vabatahtlikku kohaldamist tehisintellektisüsteemide suhtes, mis on seotud näiteks keskkonnasäästlikkusega, puuetega inimestele juurdepääsetavusega, sidusrühmade osalemisega tehisintellektisüsteemide projekteerimises ja arendamises ning arendusmeeskondade mitmekesisusega, lähtudes selgetest eesmärkidest ja põhilistest tulemusnäitajatest, millega mõõta kirjeldatud eesmärkide saavutamist.

3. Käitumisjuhendeid võivad koostada üksikud tehisintellektisüsteemide pakkujad või nende esindusorganisatsioonid või mõlemad ning sellesse tegevusse võib kaasata ka kasutajaid ja huvitatud sidusrühmi ning nende esindusorganisatsioone. Käitumisjuhendid võivad käia ühe või mitme tehisintellektisüsteemi kohta, võttes arvesse asjaomaste süsteemide sihtotstarbe sarnasusi.

4. Käitumisjuhendite koostamist edendades ja hõlbustades võtavad komisjon ja nõukoda arvesse väikepakkujate ja idufirmade erihuve ja vajadusi.

X JAOTIS

KONFIDENTSIAALSUS JA KARISTUSED

Artikkel 70
Konfidentsiaalsus

1. Käesoleva määruse kohaldamises osalevad riigi pädevad asutused ja teavitatud asutused austavad oma ülesannete täitmisel ja tegevuse käigus saadud teabe ja andmete konfidentsiaalsust, et kaitsta eeskätt järgmist:

   (a) intellektuaalomandiõigused ning füüsilise või juriidilise isiku konfidentsiaalne äriteave või ärisaladused, kaasa arvatud lähtekood, välja arvatud juhtudel, millele on viidatud direktiivi 2016/943 (milles käsitletakse avalikustamata oskusteabe ja äriteabe (ärisaladuste) ebaseadusliku omandamise, kasutamise ja avalikustamise vastast kaitset) artiklis 5;

   (b) käesoleva määruse tulemuslik rakendamine, eelkõige inspekteerimise, uurimise ja auditite eesmärgil; c) avaliku ja riigi julgeolekuga seotud huvid;

   (c) kriminaal- või haldusmenetluste usaldusväärsus.

2. Ilma et see piiraks lõike 1 kohaldamist, ei avaldata riikide pädevate asutuste ning riikide pädevate asutuste ja komisjoni vahel konfidentsiaalselt vahetatud teavet ilma, et oleks eelnevalt konsulteeritud riigi pädevad asutusega, kust teave pärit on, ja kasutajaga, kui III lisa punktides 1, 6 ja 7 osutatud suure riskiga tehisintellektisüsteeme kasutavad õiguskaitse-, rände- või varjupaigaasutused ja kui selline avaldamine seaks ohtu avaliku ja riigi julgeolekuga seotud huvid.

   Kui õiguskaitse-, rände- või varjupaigaasutused on III lisa punktides 1, 6 ja 7 osutatud suure riskiga tehisintellektisüsteemide pakkujad, peab IV lisas osutatud tehniline dokumentatsioon jääma nende asutuste ruumidesse. Need asutused peavad tagama, et olenevalt asjaoludest võivad artikli 63 lõigetes 5 ja 6 osutatud turujärelevalveasutused taotluse alusel viivitamata tutvuda dokumentatsiooniga või saada selle koopia. Dokumentide ja nende koopiatega on lubatud tutvuda ainult neil turujärelevalveasutuse töötajatel, kellel on asjakohasel tasemel salastatud teabele juurdepääsu luba.

3. Lõiked 1 ja 2 ei mõjuta komisjoni, liikmesriikide ja teavitatud asutuste õigusi ja kohustusi vahetada teavet ja edastada hoiatusi ega asjaosaliste kohustusi anda teavet liikmesriikide kriminaalõiguse kohaselt.

4. Komisjon ja liikmesriigid võivad vajaduse korral vahetada konfidentsiaalset teavet nende kolmandate riikide reguleerivate asutustega, kellega nad on sõlminud kahe- või mitmepoolsed konfidentsiaalsuse kokkulepped, mis tagavad konfidentsiaalsuse piisava taseme.

Artikkel 71
Karistused

1. Liikmesriigid kehtestavad kooskõlas käesolevas määruses sätestatud tingimustega õigusnormid karistuste, kaasa arvatud haldustrahvide kohta, mida kohaldatakse käesoleva määruse rikkumise korral, ning võtavad kõik vajalikud meetmed, et tagada nende nõuetekohane ja mõjus rakendamine. Kehtestatud karistused peavad olema mõjusad, proportsionaalsed ja hoiatavad. Neis tuleb eriti arvesse võtta väikepakkujate ja idufirmade huve ja nende majanduslikku elujõulisust.

2. Liikmesriigid teavitavad komisjoni nimetatud normidest ja meetmetest ning teavitavad teda viivitamata nende hilisematest muudatustest.

3. Järgmiste rikkumiste korral kohaldatakse haldustrahvi kuni 30 000 000 eurot või, kui rikkuja on ettevõte, kuni 6 % tema eelmise majandusaasta ülemaailmsest kogukäibest olenevalt sellest, kumb on suurem:

   (a) artiklis 5 osutatud tehisintellekti kasutusviiside keelu rikkumine;

   (b) tehisintellektisüsteemi mittevastavus artiklis 10 sätestatud nõuetele.

4. Kui tehisintellektisüsteem ei vasta ükskõik millisele käesolevast määrusest tulenevale nõudele või kohustusele, välja arvatud need, mis on sätestatud artiklites 5 ja 10, kohaldatakse haldustrahvi kuni 20 000 000 eurot või, kui rikkuja on ettevõte, kuni 4 % tema eelmise majandusaasta ülemaailmsest kogukäibest olenevalt sellest, kumb on suurem.

5. Kui teavitatud asutustele ja riigi pädevatele asutustele on taotluse peale esitatud vale, ebatäielikku või eksitavat teavet, kohaldatakse haldustrahve kuni 10 000 000 eurot või, kui rikkuja on ettevõte, kuni 2 % tema eelmise majandusaasta ülemaailmsest kogukäibest olenevalt sellest, kumb on suurem.

6. Kui otsustatakse igal konkreetsel juhul kohaldatava haldustrahvi suuruse üle, võetakse arvesse iga konkreetse olukorra kõiki asjaomaseid asjaolusid ning pööratakse asjakohast tähelepanu järgmisele:

   (a) rikkumise olemus, raskusaste ja kestus ning selle tagajärjed;

   (b) kas muud turujärelevalveasutused on juba kohaldanud sama operaatori suhtes sama rikkumise eest haldustrahve;

   (c) rikkumise toime pannud operaatori suurus ja turuosa.

7. Iga liikmesriik kehtestab õigusnormid selle kohta, kas ja millisel määral võib haldustrahve määrata selles liikmesriigis asutatud avaliku sektori asutustele ja organitele.

8. Olenevalt liikmesriikide õigussüsteemidest võib haldustrahve käsitlevaid õigusnorme kohaldada selliselt, et trahve määravad riigi pädevad kohtud või muud asutused, nii nagu neis liikmesriikides asjakohane. Selliste õigusnormide kohaldamisel neis liikmesriikides on samaväärne mõju.

Artikkel 72

Liidu institutsioonide, asutuste ja organite suhtes kohaldatavad haldustrahvid

1. Euroopa Andmekaitseinspektor võib määrata haldustrahve käesoleva määruse kohaldamisalasse kuuluvatele liidu institutsioonidele, asutustele ja organitele. Kui otsustatakse haldustrahvi määramise ja selle konkreetsel juhul kohaldatava suuruse üle, võetakse arvesse iga konkreetse olukorra kõiki asjaomaseid asjaolusid ning pööratakse asjakohast tähelepanu järgmisele:

   (a) rikkumise olemus, raskusaste ja kestus ning selle tagajärjed;

   (b) Euroopa Andmekaitseinspektoriga rikkumise heastamiseks ja rikkumise võimaliku kahjuliku mõju leevendamiseks tehtav koostöö, kaasa arvatud Euroopa Andmekaitseinspektori poolt varem asjaomase liidu institutsiooni, asutuse või organi suhtes samas küsimuses määratud meetmete järgimine:

   (c) liidu institutsiooni, asutuse või organi varasemad sarnased rikkumised.

2. Järgmiste rikkumiste korral kohaldatakse haldustrahve kuni 500 000 eurot:

   (a) artiklis 5 osutatud tehisintellekti kasutusviiside keelu rikkumine;

   (b) tehisintellektisüsteemi mittevastavus artiklis 10 sätestatud nõuetele.

3. Kui tehisintellektisüsteem ei vasta ükskõik millisele käesolevast määrusest tulenevale nõudele või kohustusele, välja arvatud need, mis on sätestatud artiklites 5 ja 10, kohaldatakse haldustrahvi kuni 250 000 eurot.

4. Enne käesoleva artikli alusel otsuse tegemist annab Euroopa Andmekaitseinspektor liidu institutsioonile, asutusele või organile, kelle suhtes Euroopa Andmekaitseinspektor on menetluse algatanud, võimaluse olla võimaliku rikkumisega seotud küsimuses ära kuulatud. Euroopa Andmekaitseinspektori otsused toetuvad üksnes sellistele elementidele ja asjaoludele, mille kohta asjaomastel isikutel on olnud võimalik esitada oma seisukoht. Kaebuste esitajate olemasolu korral kaasatakse nad aktiivselt menetlusse.

5. Menetluse käigus tagatakse täielikult asjaomaste isikute õigus kaitsele. Neil on õigus tutvuda Euroopa Andmekaitseinspektori toimikuga tingimusel, et võetakse arvesse üksikisikute ja ettevõtjate õigustatud huvi kaitsta oma isikuandmeid ja ärisaladusi.

6. Käesoleva artikli alusel määratud trahvidega kogutud summad kantakse liidu üldeelarvesse.

XI JAOTIS

VOLITUSTE DELEGEERIMINE JA KOMITEEMENETLUS

Artikkel 73
Delegeeritud volituste rakendamine

1. Komisjonile antakse õigus võtta vastu delegeeritud õigusakte käesolevas artiklis sätestatud tingimustel.

2. Artiklis 4, artikli 7 lõikes 1, artikli 11 lõikes 3, artikli 43 lõigetes 5 ja 6 ning artikli 48 lõikes 5 osutatud õigus võtta vastu delegeeritud õigusakte antakse komisjonile määramata ajaks alates [*käesoleva määruse jõustumise kuupäev*].

3. Euroopa Parlament ja nõukogu võivad artiklis 4, artikli 7 lõikes 1, artikli 11 lõikes 3, artikli 43 lõigetes 5 ja 6 ning artikli 48 lõikes 5 osutatud volituste delegeerimise igal ajal tagasi võtta. Tagasivõtmise otsusega lõpetatakse otsuses nimetatud volituste delegeerimine. Otsus jõustub järgmisel päeval pärast selle avaldamist *Euroopa Liidu Teatajas* või otsuses nimetatud hilisemal kuupäeval. See ei mõjuta juba jõustunud delegeeritud õigusaktide kehtivust.

4. Niipea kui komisjon on delegeeritud õigusakti vastu võtnud, teeb ta selle samal ajal teatavaks Euroopa Parlamendile ja nõukogule.

5. Artikli 4, artikli 7 lõike 1, artikli 11 lõike 3, artikli 43 lõigete 5 ja 6 ning artikli 48 lõike 5 alusel vastu võetud delegeeritud õigusakt jõustub üksnes juhul, kui Euroopa Parlament ega nõukogu ei ole kolme kuu jooksul pärast õigusakti teatavakstegemist Euroopa Parlamendile ja nõukogule esitanud selle kohta vastuväiteid või kui Euroopa Parlament ja nõukogu on enne selle tähtaja möödumist komisjonile teatanud, et nad ei esita vastuväiteid. Euroopa Parlamendi või nõukogu algatusel pikendatakse seda tähtaega kolme kuu võrra.

Artikkel 74
Komiteemenetlus

1. Komisjoni abistab komitee. Nimetatud komitee on komitee määruse (EL) nr 182/2011 tähenduses.

2. Käesolevale lõikele viitamise korral kohaldatakse määruse (EL) nr 182/2011 artiklit 5.

XII JAOTIS

LÕPPSÄTTED

Artikkel 75
Määruse (EÜ) nr 300/2008 muutmine

Määruse (EÜ) nr 300/2008 artikli 4 lõikesse 3 lisatakse järgmine lõik:

„Võttes vastu üksikasjalikke meetmeid julgestusseadmete tehniliste kirjelduste ning nende heakskiitmise ja kasutamise korra kohta, mis on seotud tehisintellektisüsteemidega Euroopa

Parlamendi ja nõukogu määruse (EL) YYY/XX [tehisintellekti kohta]* tähenduses, võetakse arvesse selle määruse III jaotise 2. peatükis sätestatud nõudeid.“

_____

* Määrus (EL) YYY/XX [tehisintellekti kohta] (ELT …).”

Artikkel 76
Määruse (EL) nr 167/2013 muutmine

Määruse (EL) nr 167/2013 artikli 17 lõikesse 5 lisatakse järgmine lõik:

„Võttes vastu esimese lõigu kohaseid delegeeritud õigusakte, mis käsitlevad tehisintellektisüsteeme, mis on turvakomponendid Euroopa Parlamendi ja nõukogu määruse (EL) YYY/XX [tehisintellekti kohta]* tähenduses, võetakse arvesse selle määruse III jaotise 2. peatükis sätestatud nõudeid.

_____

* Määrus (EL) YYY/XX [tehisintellekti kohta] (ELT …).”

Artikkel 77
Määruse (EL) nr 168/2013 muutmine

Määruse (EL) nr 168/2013 artikli 22 lõikesse 5 lisatakse järgmine lõik:

„Võttes vastu esimese lõigu kohaseid delegeeritud õigusakte, mis käsitlevad tehisintellektisüsteeme, mis on turvakomponendid Euroopa Parlamendi ja nõukogu määruse (EL) YYY/XX [tehisintellekti kohta]* tähenduses, võetakse arvesse selle määruse III jaotise 2. peatükis sätestatud nõudeid.

_____

* Määrus (EL) YYY/XX [tehisintellekti kohta] (ELT …).”

Artikkel 78
Direktiivi 2014/90/EL muutmine

Direktiivi 2014/90/EL artiklisse 8 lisatakse järgmine lõige:

„4. Tegutsedes vastavalt lõikele 1 ning võttes vastu tehnilisi kirjeldusi ja testimisstandardeid vastavalt lõigetele 2 ja 3 seoses tehisintellektisüsteemidega, mis on turvakomponendid Euroopa Parlamendi ja nõukogu määruse (EL) YYY/XX [tehisintellekti kohta]* tähenduses, võtab komisjon arvesse selle määruse III jaotise 2. peatükis sätestatud nõudeid.

_____

* Määrus (EL) YYY/XX [tehisintellekti kohta] (ELT …).”.

Artikkel 79
Direktiivi (EL) 2016/797 muutmine

Direktiivi (EL) 2016/797 artiklisse 5 lisatakse järgmine lõige:

„12. „Võttes vastu lõike 1 kohaseid delegeeritud õigusakte ja lõike 11 kohaseid rakendusakte, mis käsitlevad tehisintellektisüsteeme, mis on turvakomponendid Euroopa Parlamendi ja nõukogu määruse (EL) YYY/XX [tehisintellekti kohta]* tähenduses, võetakse arvesse selle määruse III jaotise 2. peatükis sätestatud nõudeid.

_____

* Määrus (EL) YYY/XX [tehisintellekti kohta] (ELT …).”.

Artikkel 80
Määruse (EL) 2018/858 muutmine

Määruse (EL) 2018/858 artiklisse 5 lisatakse järgmine lõige:

„4. „Võttes vastu lõike 3 kohaseid delegeeritud õigusakte, mis käsitlevad tehisintellektisüsteeme, mis on turvakomponendid Euroopa Parlamendi ja nõukogu määruse (EL) YYY/XX [tehisintellekti kohta]* tähenduses, võetakse arvesse selle määruse III jaotise 2. peatükis sätestatud nõudeid.

_____

* Määrus (EL) YYY/XX [tehisintellekti kohta] (ELT …).”.

Artikkel 81
Määruse (EL) 2018/1139 muutmine

Määrust (EL) 2018/1139 muudetakse järgmiselt.

1) Artiklisse 17 lisatakse järgmine lõige:

„3. „Võttes vastu lõike 1 kohaseid rakendusakte, mis käsitlevad tehisintellektisüsteeme, mis on turvakomponendid Euroopa Parlamendi ja nõukogu määruse (EL) YYY/XX [*tehisintellekti kohta*]* tähenduses, võetakse arvesse selle määruse III jaotise 2. peatükis sätestatud nõudeid, ilma et see piiraks lõike 2 kohaldamist.

_____

* Määrus (EL) YYY/XX [tehisintellekti kohta] (ELT …).”

2) Artiklisse 19 lisatakse järgmine lõige:

„4. „Võttes vastu lõigete 1 ja 2 kohaseid delegeeritud õigusakte, mis käsitlevad tehisintellektisüsteeme, mis on turvakomponendid määruse (EL) YYY/XX [tehisintellekti kohta] tähenduses, võetakse arvesse selle määruse III jaotise 2. peatükis sätestatud nõudeid.“

3) Artiklisse 43 lisatakse järgmine lõige:

„4. „Võttes vastu lõike 1 kohaseid rakendusakte, mis käsitlevad tehisintellektisüsteeme, mis on turvakomponendid määruse (EL) YYY/XX [tehisintellekti kohta] tähenduses, võetakse arvesse selle määruse III jaotise 2. peatükis sätestatud nõudeid.“

4) Artiklisse 47 lisatakse järgmine lõige:

„3. „Võttes vastu lõigete 1 ja 2 kohaseid delegeeritud õigusakte, mis käsitlevad tehisintellektisüsteeme, mis on turvakomponendid määruse (EL) YYY/XX [tehisintellekti kohta] tähenduses, võetakse arvesse selle määruse III jaotise 2. peatükis sätestatud nõudeid.“

5) Artiklisse 57 lisatakse järgmine lõige:

„Võttes vastu kõnealuseid rakendusakte, mis käsitlevad tehisintellektisüsteeme, mis on turvakomponendid määruse (EL) YYY/XX [tehisintellekti kohta] tähenduses, võetakse arvesse selle määruse III jaotise 2. peatükis sätestatud nõudeid.“

6) Artiklisse 58 lisatakse järgmine lõige:

„3. „Võttes vastu lõigete 1 ja 2 kohaseid delegeeritud õigusakte, mis käsitlevad tehisintellektisüsteeme, mis on turvakomponendid määruse (EL) YYY/XX [tehisintellekti kohta] tähenduses, võetakse arvesse selle määruse III jaotise 2. peatükis sätestatud nõudeid.“.

Artikkel 82
Määruse (EL) 2019/2144 muutmine

Määruse (EL) 2019/2144 artiklisse 11 lisatakse järgmine lõige:

„3. „Võttes vastu lõike 2 kohaseid rakendusakte, mis käsitlevad tehisintellektisüsteeme, mis on turvakomponendid Euroopa Parlamendi ja nõukogu määruse (EL) YYY/XX [tehisintellekti kohta]* tähenduses, võetakse arvesse selle määruse III jaotise 2. peatükis sätestatud nõudeid.

_____

* Määrus (EL) YYY/XX [tehisintellekti kohta] (ELT …).”.

Artikkel 83
Juba turule lastud või kasutusele võetud tehisintellektisüsteemid

1. Käesolevat määrust ei kohaldata tehisintellektisüsteemide suhtes, mis on selliste IX lisas loetletud õigusaktidega loodud suuremahuliste IT-süsteemide komponendid, mis on turule lastud või kasutusele võetud enne [*12 kuud pärast artikli 85 lõikes 2 osutatud kuupäeva, mil käesolevat määrust hakatakse kohaldama*], välja arvatud juhul, kui nende õigusaktide asendamise või muutmise tulemusena tehakse oluline muudatus asjaomase tehisintellektisüsteemi või asjaomaste tehisintellektisüsteemide projektis või sihtotstarbes.

   Kui see on asjakohane, võetakse käesolevas määruses sätestatud nõudeid arvesse, kui hinnatakse IX lisas loetletud õigusaktidega loodud suuremahulisi IT-süsteeme neis õigusaktides sätestatud korra kohaselt.

2. Käesolevat määrust kohaldatakse suure riskiga tehisintellektisüsteemide suhtes, välja arvatud lõikes 1 osutatud süsteemide suhtes, mis on turule lastud või kasutusele võetud enne [*artikli 85 lõikes 2 osutatud kuupäev, mil käesolevat määrust hakatakse kohaldama*], ainult juhul, kui pärast nimetatud kuupäeva muudetakse oluliselt nende projekti või sihtotstarvet.

Artikkel 84
Hindamine ja läbivaatamine

1. Komisjon annab pärast käesoleva määruse jõustumist kord aastas hinnangu sellele, kas III lisas esitatud loetelu on vaja muuta.

2. Komisjon esitab Euroopa Parlamendile ja nõukogule hiljemalt [*kolm aastat pärast artikli 85 lõikes 2 osutatud kuupäeva, mil käesolevat määrust hakatakse kohaldama,*] ning pärast seda iga nelja aasta järel aruande käesoleva määruse hindamise ja läbivaatamise kohta. Aruanded avalikustatakse.

3. Lõikes 2 osutatud aruannetes pööratakse erilist tähelepanu järgmisele:

   (a) riigi pädevate asutuste rahaliste ja inimressursside olukord, et nad saaksid tulemuslikult täita neile käesoleva määruse alusel määratud ülesandeid;

(b) olukord seoses artikli 71 lõikes 1 osutatud karistuste ja eriti haldustrahvidega, mida liikmesriigid kohaldavad käesoleva määruse sätete rikkumise korral.

4. Komisjon hindab [*kolme aasta jooksul alates artikli 85 lõikes 2 osutatud kuupäevast, mil käesolevat määrust hakatakse kohaldama,*] ja pärast seda iga nelja aasta järel, kui mõjusalt ja tulemuslikult on käitumisjuhendid edendanud III jaotise 2. peatükis sätestatud nõuete ja võimaluse korral muude kui suure riskiga tehisintellektisüsteemide suhtes kehtivate täiendavate nõuete kohaldamist.

5. Lõigete 1–4 kohaldamisel esitavad nõukoda, liikmesriigid ja riikide pädevad asutused komisjonile tema taotluse korral teavet.

6. Lõigetes 1 ja 4 osutatud hindamiste ja läbivaatamiste käigus võtab komisjon arvesse nõukoja, Euroopa Parlamendi, nõukogu ning muude asjaomaste organite ja allikate seisukohti ja tähelepanekuid.

7. Komisjon esitab vajaduse korral asjakohased ettepanekud käesoleva määruse muutmiseks, eelkõige võttes arvesse tehnika ja infoühiskonna arengut.

Artikkel 85
Jõustumine ja kohaldamine

1. Käesolev määrus jõustub kahekümnendal päeval pärast selle avaldamist *Euroopa Liidu Teatajas*.

2. Käesolevat määrust kohaldatakse alates [*24 kuud pärast määruse jõustumist]*.

3. Erandina lõikest 2 kohaldatakse:

(a) III jaotise 4. peatükki ja VI jaotist alates [*kolm kuud pärast käesoleva määruse jõustumist*];

(b) artiklit 71 alates [12 kuud pärast määruse jõustumist].

Käesolev määrus on tervikuna siduv ja vahetult kohaldatav kõikides liikmesriikides.

Brüssel,

Euroopa Parlamendi nimel	*Nõukogu nimel*
president	*eesistuja*

FINANTSSELGITUS

1. ETTEPANEKU/ALGATUSE RAAMISTIK

1.1. Ettepaneku/algatuse nimetus

1.2. Asjaomased poliitikavaldkonnad

1.3. Ettepanek/algatus käsitleb

1.4. Eesmärgid

1.4.1. Üldeesmärgid

1.4.2. Erieesmärgid

1.4.3. Oodatavad tulemused ja mõju

1.4.4. Tulemusnäitajad

1.5. Ettepaneku/algatuse põhjendused

1.5.1. Lühi- või pikaajalises perspektiivis täidetavad vajadused, sealhulgas algatuse rakendamise üksikasjalik ajakava

1.5.2. ELi meetme lisaväärtus (see võib tuleneda eri teguritest, nagu kooskõlastamisest saadav kasu, õiguskindlus, suurem tõhusus või vastastikune täiendavus). Käesoleva punkti kohaldamisel tähendab „ELi meetme lisaväärtus“ väärtust, mis tuleneb liidu sekkumisest ja lisandub väärtusele, mille liikmesriigid oleksid muidu üksi loonud.

1.5.3. Samalaadsetest kogemustest saadud õppetunnid

1.5.4. Kooskõla mitmeaastase finantsraamistikuga ja võimalik koostoime muude asjaomaste meetmetega

1.5.5. Erinevate kasutada olevate rahastamisvõimaluste, sealhulgas vahendite ümberpaigutamise võimaluste hinnang

1.6. Ettepaneku/algatuse kestus ja finantsmõju

1.7. Ettenähtud eelarve täitmise viisid

2. HALDUSMEETMED

2.1. Järelevalve ja aruandluse eeskirjad

2.2. Haldus- ja kontrollisüsteem(id)

2.2.1. Eelarve täitmise viisi(de), rahastamise rakendamise mehhanismi(de), maksete tegemise korra ja kavandatava kontrollistrateegia selgitus

2.2.2. Teave kindlakstehtud riskide ja nende vähendamiseks kasutusele võetud sisekontrollisüsteemi(de) kohta

2.2.3. Kontrollide kulutõhususe (kontrollikulude suhe hallatavate vahendite väärtusse) hinnang ja põhjendus ning prognoositav veariski tase (maksete tegemise ja sulgemise ajal).

2.3. Pettuse ja eeskirjade eiramise ärahoidmise meetmed

3. ETTEPANEKU/ALGATUSE HINNANGULINE FINANTSMÕJU

3.1. Mitmeaastase finantsraamistiku rubriigid ja kulude eelarveread, millele mõju avaldub

3.2. Ettepaneku hinnanguline finantsmõju assigneeringutele

3.2.1. Hinnanguline mõju tegevusassigneeringutele – ülevaade

3.2.2. Tegevusassigneeringutest rahastatav väljund (hinnang)

3.2.3. Hinnanguline mõju haldusassigneeringutele – ülevaade

3.2.4. Kooskõla kehtiva mitmeaastase finantsraamistikuga

3.2.5. Kolmandate isikute rahaline osalus

3.3. Hinnanguline mõju tuludele

FINANTSSELGITUS

1. ETTEPANEKU/ALGATUSE RAAMISTIK

1.1. Ettepaneku/algatuse nimetus

Euroopa Parlamendi ja nõukogu määrus, millega sätestatakse tehisintellekti käsitlevad harmoneeritud eeskirjad (tehisintellekti käsitlev õigusakt) ja muudetakse teatavaid liidu õigusakte

1.2. Asjaomased poliitikavaldkonnad

Sidevõrgud, sisu ja tehnoloogia

Siseturg, tööstus, ettevõtlus ja VKEd

Mõju eelarvele on seotud komisjonile usaldatud uute ülesannetega, sealhulgas ELi tehisintellekti nõukoja toetamisega.

Tegevus: Euroopa digituleviku kujundamine

1.3. Ettepanek/algatus käsitleb

X **uut meedet**

☐ **uut meedet, mis tuleneb katseprojektist / ettevalmistavast meetmest**[64]

☐ **olemasoleva meetme pikendamist**

☐ **ümbersuunatud meedet**

1.4. Eesmärgid

1.4.1. Üldeesmärgid

Sekkumise üldeesmärk on tagada ühtse turu nõuetekohane toimimine, luues tingimused usaldusväärse tehisintellekti arendamiseks ja kasutamiseks liidus.

1.4.2. Erieesmärgid

Erieesmärk nr 1

Sätestada tehisintellektisüsteemide erinõuded ja kõigi väärtusahelas osalejate kohustused, et turule lastavad ja kasutatavad tehisintellektisüsteemid oleksid ohutud ja kooskõlas kehtiva põhiõigusi käsitleva õigusega ning liidu väärtustega.

Erieesmärk nr 2

Tagada õiguskindlus, et soodustada tehisintellektialaseid investeeringuid ja innovatsiooni, tehes selgeks, milliseid olulisi nõudeid, kohustusi ja vastavusmenetlusi tuleb järgida tehisintellektisüsteemi liidu turule laskmiseks ja seal kasutamiseks.

Erieesmärk nr 3

Tugevdada juhtimist ja tõhustada põhiõigusi käsitleva kehtiva õiguse ja tehisintellektisüsteemidele kohalduvate ohutusnõuete täitmise tagamist, andes asjaomastele asutustele vastavushindamise, järelkontrollimenetluste ning riigi ja ELi

[64] Vastavalt finantsmääruse artikli 54 lõike 2 punktile a või b.

tasandi vahel juhtimis- ja järelevalveülesannete jagamisega seotud uued volitused, vahendid ja selged eeskirjad.

Erieesmärk nr 4

Aidata arendada õiguspäraste, ohutute ja usaldusväärsete tehisintellektirakenduste ühtset turgu ning vältida turu killustumist, võttes ELi meetmed, millega sätestada liidu turule lastavatele ja seal kasutatavatele tehisintellektisüsteemidele miinimumnõuded kooskõlas põhiõigusi ja ohutust käsitleva kehtiva õigusega.

1.4.3. Oodatavad tulemused ja mõju

Märkige, milline peaks olema ettepaneku/algatuse oodatav mõju toetusesaajatele/sihtrühmale.

Tehisintellektisüsteemide pakkujatele peaksid kehtima minimaalsed, kuid selged nõuded, mis loovad õiguskindlust ja tagavad juurdepääsu kogu ühtsele turule.

Tehisintellekti kasutajatel peaks olema õiguskindlus, et nende ostetavad suure riskiga tehisintellektisüsteemid vastavad Euroopa seadustele ja väärtustele.

Tuleks vähendada tarbijate ohutuse vähendamise või põhiõiguste rikkumise riski.

1.4.4. Tulemusnäitajad

Täpsustage, milliste näitajate alusel hinnatakse ettepaneku/algatuse elluviimist.

Näitaja 1

Tõsiste intsidentide või tehisintellekti selliste toimimiste arv, mis kujutavad endast tõsist intsidenti või põhiõigustega seotud kohustuste rikkumist (poolaasta kohta) kasutusalade lõikes ja mis on arvutatud a) absoluutväärtusena, b) kasutatud rakenduste osakaaluna ja c) asjaomaste kodanike osakaaluna.

Näitaja 2

a) Tehisintellekti tehtavad investeeringud ELis (aasta)

b) Tehisintellekti tehtavad investeeringud liikmesriigiti (aasta)

c) Tehisintellekti kasutavate ettevõtete osakaal (aasta)

d) Tehisintellekti kasutavate ettevõtete osakaal (aasta)

a) ja b) arvutamisel lähtutakse ametlikest allikatest ja võrreldakse neid erasektori hinnanguliste arvutustega.

c) ja d) kogutakse tavapäraste ettevõtjate küsitluste kaudu.

1.5. Ettepaneku/algatuse põhjendused

1.5.1. Lühi- või pikaajalises perspektiivis täidetavad vajadused, sealhulgas algatuse rakendamise üksikasjalik ajakava

Määrus peaks olema täielikult kohaldatav poolteist aastat pärast selle vastuvõtmist, kuid juhtimisstruktuurid peaksid enne seda paigas olema. Eelkõige peavad liikmesriikidel olema nimetatud olemasolevad asutused ja/või loodud uued asutused varem õigusaktides sätestatud ülesannete täitmiseks ning luua tuleks tõhus ELi tehisintellekti nõukoda. Kohaldamise ajaks peaks Euroopa tehisintellektisüsteemide andmebaas täielikult toimima. Seetõttu tuleb andmebaas välja töötada vastuvõtmisprotsessiga paralleelselt, et see oleks määruse jõustumise ajaks valmis.

1.5.2. ELi meetme lisaväärtus (see võib tuleneda eri teguritest, nagu kooskõlastamisest saadav kasu, õiguskindlus, suurem tõhusus või vastastikune täiendavus). Käesoleva punkti kohaldamisel tähendab „ELi meetme lisaväärtus“ väärtust, mis tuleneb liidu sekkumisest ja lisandub väärtusele, mille liikmesriigid oleksid muidu üksi loonud.

Tekkiv lahkneda võivate riiklike eeskirjade segu takistab tehisintellektisüsteemide sujuvat pakkumist ELis ega suuda eri liikmesriikides tõhusalt tagada ohutust ega põhiõiguste ja liidu väärtuste kaitset. ELi ühised õiguslikud meetmed tehisintellekti valdkonnas võivad hoogustada siseturgu ja anda Euroopa tööstusele maailmas konkurentsieelise ja mastaabisäästu, mida liikmesriigid ei suuda üksi saavutada.

1.5.3. Samalaadsetest kogemustest saadud õppetunnid

E-kaubanduse direktiivis 2000/31/EÜ on sätestatud ühtse turu toimimise ja digiteenuste järelevalve põhiraamistik ning liikmesriikidevahelise üldise koostöömehhanismi põhistruktuur, mis põhimõtteliselt hõlmab kõiki digiteenuste suhtes kohaldatavaid nõudeid. Direktiivi hindamisel juhiti tähelepanu puudustele selle koostöömehhanismi mitmes aspektis, sealhulgas olulistes menetluslikes aspektides, näiteks liikmesriikide vastamise selgete tähtaegade puudumine ning üldine suutmatus reageerida partnerite taotlustele. See on toonud aastate jooksul liikmesriikide vahel kaasa usaldamatuse piiriüleste digiteenuste pakkujatega seotud probleemide lahendamise valdkonnas. Direktiivi hindamisest ilmnes vajadus määratleda Euroopa tasandil kindlapiirilised eeskirjad ja nõuded. Sellel põhjusel eeldaks käesolevas määruses sätestatud erikohustuste rakendamine ELi tasandi spetsiifilist koostöömehhanismi, mille juhtimisstruktuur tagab ELi tasandi vastutavate organite koordineerituse.

1.5.4. Kooskõla mitmeaastase finantsraamistikuga ja võimalik koostoime muude asjaomaste meetmetega

Määruses, millega sätestatakse tehisintellekti käsitlevad harmoneeritud eeskirjad ja muudetakse teatavaid liidu õigusakte, määratletakse tehisintellektisüsteemidele kohaldatavate nõuete uus ühtne raamistik, mis läheb palju kaugemale olemasolevates õigusaktides ettenähtust. Seepärast tuleb käesoleva ettepanekuga kehtestada uus riiklik ja Euroopa reguleerimis- ja koordineerimisfunktsioon.

Seoses võimaliku koostoimega muude asjakohaste õigusaktidega võivad riigi tasandi teavitavate asutuste rolli täita riikide ametiasutused, mis täidavad muude ELi õigusaktide alusel sarnaseid ülesandeid.

Tehisintellekti vastu usalduse suurendamisega ja seega tehisintellekti arendamisse ja vastuvõtmisse investeerimise soodustamisega täiendab see programmi „Digitaalne Euroopa“, mille viiest prioriteedist üks on soodustada tehisintellekti levikut.

1.5.5. Erinevate kasutada olevate rahastamisvõimaluste, sealhulgas vahendite ümberpaigutamise võimaluste hinnang

Töötajad paigutatakse ümber. Muud kulud kaetakse programmi „Digitaalne Euroopa“ eelarvest, sest käesoleva määruse eesmärk tagada usaldusväärne tehisintellekt aitab otseselt täita programmi „Digitaalne Euroopa“ üht põhieesmärki, milleks on kiirendada tehisintellekti arendamist ja juurutamist Euroopas.

1.6. Ettepaneku/algatuse kestus ja finantsmõju

☐ **Piiratud kestusega**

– ☐ hõlmab ajavahemikku [PP/KK]AAAA–[PP/KK]AAAA

– ☐ finantsmõju kulukohustuste assigneeringutele avaldub ajavahemikul AAAA–AAAA ja maksete assigneeringutele ajavahemikul AAAA–AAAA.

X **Piiramatu kestusega**

– rakendamise käivitumisperiood hõlmab üht/kaht (kinnitamisel) aastat,

– millele järgneb täieulatuslik rakendamine

1.7. Ettenähtud eelarve täitmise viisid[65]

X **Eelarve otsene täitmine** komisjoni poolt

– ☐ oma talituste kaudu, sealhulgas kasutades liidu delegatsioonides töötavat komisjoni personali;

– ☐ rakendusametite kaudu

☐ **Eelarve jagatud täitmine** koostöös liikmesriikidega

☐ **Eelarve kaudne täitmine**, mille puhul eelarve täitmise ülesanded on delegeeritud:

– ☐ kolmandatele riikidele või nende määratud asutustele;

– ☐ rahvusvahelistele organisatsioonidele ja nende allasutustele (nimetage);

– ☐ Euroopa Investeerimispangale ja Euroopa Investeerimisfondile;

– ☐ finantsmääruse artiklites 70 ja 71 osutatud asutustele;

– ☐ avalik-õiguslikele asutustele;

– ☐ avalikke teenuseid osutavatele eraõiguslikele asutustele, kuivõrd nad esitavad piisavad finantstagatised;

– ☐ liikmesriigi eraõigusega reguleeritud asutustele, kellele on delegeeritud avaliku ja erasektori partnerluse rakendamine ja kes esitavad piisavad finantstagatised;

– ☐ isikutele, kellele on delegeeritud Euroopa Liidu lepingu V jaotise kohaste ühise välis- ja julgeolekupoliitika erimeetmete rakendamine ja kes on kindlaks määratud asjaomases alusaktis.

– *Mitme eelarve täitmise viisi valimise korral esitage üksikasjad rubriigis „Märkused“.*

Märkused

[65] Eelarve täitmise viise koos viidetega finantsmäärusele on selgitatud veebisaidil http://www.cc.cec/budg/man/budgmanag/budgmanag_en.html

2. HALDUSMEETMED

2.1. Järelevalve ja aruandluse eeskirjad

Märkige sagedus ja tingimused.

Määrus vaadatakse läbi ja seda hinnatakse viis aastat pärast määruse jõustumist. Komisjon esitab Euroopa Parlamendile, nõukogule ning Euroopa Majandus- ja Sotsiaalkomiteele aruande määruse hindamise tulemuste kohta.

2.2. Haldus- ja kontrollisüsteem(id)

2.2.1. Eelarve täitmise viisi(de), rahastamise rakendamise mehhanismi(de), maksete tegemise korra ja kavandatava kontrollistrateegia selgitus

Määrusega kehtestatakse uued põhimõtted seoses siseturul tehisintellektisüsteemide pakkumise harmoneeritud eeskirjadega ning tagatakse samal ajal ohutus ja põhiõiguste austamine. Nende uute eeskirjade jaoks ja käesolevast määrusest tulenevate kohustuste piiriüleseks kohaldamiseks on vaja järjepidevust tagavat uut nõuanderühma, mis koordineerib riiklike asutuste tegevust.

Nende uute ülesannete täitma asumiseks tuleb asjakohaselt rahastada komisjoni talitusi. Uue määruse täitmise tagamiseks on hinnanguliselt tarvis 10 täistööaja ekvivalenti (5 täistööaja ekvivalenti nõukoja tegevuse toetuseks ja 5 täistööaja ekvivalenti Euroopa Andmekaitseinspektorile, kes tegutseb Euroopa Liidu organite juurutatavate tehisintellektisüsteemide valdkonnas teavitava asutusena).

2.2.2. Teave kindlakstehtud riskide ja nende vähendamiseks kasutusele võetud sisekontrollisüsteemi(de) kohta

Selleks et nõukoja liikmetel oleks võimalus teha faktidel põhinevaid teadlikke analüüse, nähakse ette, et nõukoda peaks selle tegevuses toetama komisjoni haldusstruktuur ja et luuakse eksperdirühm, mis jagab vajaduse korral täiendavat oskusteavet.

2.2.3. Kontrollide kulutõhususe (kontrollikulude suhe hallatavate vahendite väärtusse) hinnang ja põhjendus ning prognoositav veariski tase (maksete tegemise ja sulgemise ajal)

Kuna ühe tehingu (nt koosolekul osaleva delegaadi reisikulude hüvitamine) väärtus on väike, näib koosolekukuludega seoses piisavat standardsest kontrollikorrast. Sidevõrkude, sisu ja tehnoloogia peadirektoraadis on andmebaasi arendamisega seotud lepingute määramiseks olemas kindel sisekontrollisüsteem, mida rakendatakse tsentraliseeritud hanketegevuse kaudu.

2.3. Pettuse ja eeskirjade eiramise ärahoidmise meetmed

Nimetage rakendatavad või kavandatud ennetus- ja kaitsemeetmed, nt pettustevastase võitluse strateegias esitatud meetmed.

Komisjonile kohalduvad olemasolevad pettuste ennetamise meetmed hõlmavad käesoleva määruse täitmiseks vajalikke lisaassigneeringuid.

3. ETTEPANEKU/ALGATUSE HINNANGULINE FINANTSMÕJU

3.1. Mitmeaastase finantsraamistiku rubriigid ja kulude eelarveread, millele mõju avaldub

- Olemasolevad eelarveread

Järjestage mitmeaastase finantsraamistiku rubriigiti ja iga rubriigi sees eelarveridade kaupa

Mitmeaastase finantsraamistiku rubriik	Eelarverida	Assigneeringute liik	Rahaline osalus			
	Nr	Liigendatud/liigendamata[66]	EFTA riigid[67]	kandidaatriigid[68]	kolmandad riigid	finantsmääruse artikli 21 lõike 2 punkti b tähenduses
7	20 02 06 Halduskulud	Liigendamata	EI	EI	EI	EI
1	02 04 03 Programm „Digitaalne Euroopa“, tehisintellekt	Liigendatud	JAH	EI	EI	EI
1	02 01 30 01 Programmi „Digitaalne Euroopa“ toetuskulud	Liigendamata	JAH	EI	EI	EI

3.2. Ettepaneku hinnanguline finantsmõju assigneeringutele

3.2.1. Hinnanguline mõju tegevusassigneeringute kuludele – ülevaade

– ☐ Ettepanek/algatus ei hõlma tegevusassigneeringute kasutamist

– X Ettepanek/algatus hõlmab tegevusassigneeringute kasutamist, mis toimub järgmiselt:

miljonites eurodes (kolm kohta pärast koma)

66 Liigendatud = liigendatud assigneeringud / liigendamata = liigendamata assigneeringud.
67 EFTA: Euroopa Vabakaubanduse Assotsiatsioon.
68 Kandidaatriigid ja vajaduse korral Lääne-Balkani potentsiaalsed kandidaatriigid.

Mitmeaastase finantsraamistiku rubriik	1	

Sidevõrkude, sisu ja tehnoloogia peadirektoraat				Aasta **2022**	Aasta **2023**	Aasta **2024**	Aasta **2025**	Aasta **2026**	Aasta **2027**[69]	**KOKKU**	
•Tegevusassigneeringud											
Eelarverida[70] 02 04 03		Kulukohustused	(1a)		1,000						**1,000**
		Maksed	(2a)		0,600	0,100	0,100	0,100	0,100		**1,000**
Eelarverida		Kulukohustused	(1b)								
		Maksed	(2b)								
Eriprogrammide vahenditest rahastatavad haldusassigneeringud[71]											
Eelarverida 02 01 30 01			(3)		0,240	0,240	0,240	0,240	0,240		**1,200**
Sidevõrkude, sisu ja tehnoloogia peadirektoraadi assigneeringud KOKKU		Kulukohustused	= 1a + 1b + 3		**1,240**		**0,240**	**0,240**	**0,240**		**2,200**
		Maksed	= 2a + 2b +3).		**0,840**	**0,340**	**0,340**	**0,340**	**0,340**		**2,200**

69 Esialgne ja oleneb eelarvest.

70 Eelarve ametliku liigenduse kohaselt.

71 Tehniline ja/või haldusabi ning ELi programmide ja/või meetmete rakendamiseks antava toetusega seotud kulud (endised BA read), kaudne teadustegevus, otsene teadustegevus.

•Tegevusassigneeringud KOKKU	Kulukohustused	(4)		1,000						**1,000**
	Maksed	(5)		0,600	0,100	0,100	0,100	0,100		**1,000**
•Eriprogrammide vahenditest rahastatavad haldusassigneeringud KOKKU		(6)		**0,240**	**0,240**	**0,240**	**0,240**	**0,240**		**1,200**
Mitmeaastase finantsraamistiku **RUBRIIGI 1 assigneeringud KOKKU**	Kulukohustused	= 4 + 6		1,240	0,240	0,240	0,240	0,240		**2,200**
	Maksed	= 5 + 6		0,840	0,340	0,340	0,340	0,340		**2,200**

Juhul kui ettepanek/algatus mõjutab mitut rubriiki, tuleb eelmist jaotist korrata

•Tegevusassigneeringud KOKKU (kõik rubriigid)	Kulukohustused	(4)								
	Maksed	(5)								
•Eriprogrammide vahenditest rahastatavad haldusassigneeringud KOKKU (kõik rubriigid)		(6)								
Mitmeaastase finantsraamistiku **RUBRIIKIDE 1–6 assigneeringud KOKKU** (Sihtsumma)	Kulukohustused	= 4 + 6								
	Maksed	= 5 + 6								

Mitmeaastase finantsraamistiku rubriik	7	„Halduskulud“

Selle punkti täitmisel tuleks kasutada haldusalaste eelarveandmete tabelit, mis on esitatud õigusaktile lisatava finantsselgituse lisas (sisekorraeeskirjade V lisa), ja laadida see üles DECIDE'i talitustevahelise konsulteerimise eesmärgil.

miljonites eurodes (kolm kohta pärast koma)

		Aasta **2023**	Aasta **2024**	Aasta **2025**	Aasta **2026**	Aasta **2027**	**Pärast 2027. aastat**[72]	**KOKKU**
Sidevõrkude, sisu ja tehnoloogia peadirektoraat								
•Personalikulud		0,760	0,760	0,760	0,760	0,760	0,760	**3,800**
•Muud halduskulud		**0,010**	**0,010**	**0,010**	**0,010**	**0,010**	**0,010**	**0,050**
Sidevõrkude, sisu ja tehnoloogia peadirektoraat KOKKU	**Assigneeringud**	**0,760**	**0,760**	**0,760**	**0,760**	**0,760**	**0,760**	**3,850**
Euroopa Andmekaitseinspektor								
•Personalikulud		0,760	0,760	0,760	0,760	0,760	0,760	**3,800**
•Muud halduskulud								
Euroopa Andmekaitseinspektor KOKKU	**Assigneeringud**	**0,760**	**0,760**	**0,760**	**0,760**	**0,760**	**0,760**	**3,800**
Mitmeaastase finantsraamistiku **RUBRIIGI 7 assigneeringud KOKKU**	(Kulukohustuste kogusumma = maksete kogusumma)	1,530	1,530	1,530	1,530	1,530	1,530	**7,650**

miljonites eurodes (kolm kohta pärast koma)

	Aasta	Aasta	Aasta	Aasta	Aasta **2026**	Aasta **2027**		**KOKKU**

[72] Kõik selle veeru arvud on esialgsed ja olenevad programmide jätkumisest ning assigneeringute saadavusest.

		2022	2023	2024	2025				
Mitmeaastase finantsraamistiku **RUBRIIKIDE 1–7 assigneeringud KOKKU**	Kulukohustused		2,770	1,770	1,770	1,770	1,770		**9,850**
	Maksed		2,370	1,870	1,870	1,870	1,870		**9,850**

3.2.2. Tegevusassigneeringutest rahastatav väljund (hinnang)

kulukohustuste assigneeringud miljonites eurodes (kolm kohta pärast koma)

Märkige eesmärgid ja väljundid ⇩			Aasta **2022**		Aasta **2023**		Aasta **2024**		Aasta **2025**		Aasta **2026**		Aasta **2027**		Pärast **2027. aastat** [73]		**KOKKU**	
	VÄLJUNDID																	
	Liik	Keskmine kulu	Arv	Kulu	Arv	Kulu	Arv	Kulu	Arv	Kulu	Arv	Kulu	Arv	Kulu	Arv	Kulu	Väljundite arv kokku	Kulud kokku
ERIEESMÄRK nr 1[74] ...																		
Andmebaas					1	1,000	1		1		1		1		1	0,100	1	1,000
Koosolekud – väljund					10	0,200	10	0,200	10	0,200	10	0,200	10	0,200	10	0,200	50	1,000
Teavitustegevus					2	0,040	2	0,040	2	0,040	2	0,040	2	0,040	2	0,040	10	0,040
Erieesmärk nr 1 kokku																		
ERIEESMÄRK nr 2 ...																		
- Väljund																		
Erieesmärk nr 2 kokku																		
KOKKU					13	0,240	13	0,240	13	0,240	13	0,240	13	0,240	13	0,100	65	2,200

[73] Kõik selle veeru arvud on esialgsed ja olenevad programmide jätkumisest ning assigneeringute saadavusest.

[74] Vastavalt punktile 1.4.2. „Erieesmärgid ...“

3.2.3. Hinnanguline mõju haldusassigneeringutele – ülevaade

– ☐ Ettepanek/algatus ei hõlma haldusassigneeringute kasutamist

– X Ettepanek/algatus hõlmab haldusassigneeringute kasutamist, mis toimub järgmiselt:

miljonites eurodes (kolm kohta pärast koma)

	Aasta **2022**	Aasta **2023**	Aasta **2024**	Aasta **2025**	Aasta **2026**	Aasta **2027**	**Kord aastas pärast 2027. aastat**[75]	**KOKKU**
Mitmeaastase finantsraamistiku RUBRIIK 7								
Personalikulud		1,520	1,520	1,520	1,520	1,520	**1,520**	**7,600**
Muud halduskulud		0,010	0,010	0,010	0,010	0,010	**0,010**	**0,050**
Mitmeaastase finantsraamistiku RUBRIIGI 7 kulud kokku		1,530	1,530	1,530	1,530	1,530	**1,530**	**7,650**

Mitmeaastase finantsraamistiku RUBRIIGIST 7 välja jäävad kulud[76]								
Personalikulud								
Muud halduskulud		0,240	0,240	0,240	0,240	0,240	**0,240**	**1,20**
Mitmeaastase finantsraamistiku RUBRIIGIST 7 välja jäävad kulud kokku		0,240	0,240	0,240	0,240	0,240	**0,240**	**1,20**

KOKKU		**1,770**	**1,770**	**1,770**	**1,770**	**1,770**	**1,770**	**8,850**

Personali ja muude halduskuludega seotud assigneeringute vajadused kaetakse asjaomase peadirektoraadi poolt kõnealuse meetme haldamiseks juba antud ja/või peadirektoraadi siseselt ümberpaigutatud assigneeringutest, mida vajaduse korral võidakse täiendada nendest lisaassigneeringutest, mis haldavale peadirektoraadile eraldatakse iga-aastase vahendite eraldamise menetluse käigus, arvestades eelarvepiirangutega.

75 Kõik selle veeru arvud on esialgsed ja olenevad programmide jätkumisest ning assigneeringute saadavusest.

76 Tehniline ja/või haldusabi ning ELi programmide ja/või meetmete rakendamiseks antava toetusega seotud kulud (endised BA read), kaudne teadustegevus, otsene teadustegevus.

3.2.3.1. Hinnanguline personalivajadus

– ☐ Ettepanek/algatus ei hõlma personali kasutamist

– X Ettepanek/algatus hõlmab personali kasutamist, mis toimub järgmiselt:

Hinnanguline väärtus täistööaja ekvivalendina

.		Aasta **2023**	Aasta **2024**	Aasta **2025**	**2026**	**2027**	**Pärast 2027. aastat** [77]	
•Ametikohtade loeteluga ette nähtud ametikohad (ametnikud ja ajutised töötajad)								
20 01 02 01 (komisjoni peakorteris ja esindustes)		10	10	10	10	10	10	
20 01 02 03 (delegatsioonides)								
01 01 01 01 (kaudne teadustegevus)								
01 01 01 11 (otsene teadustegevus)								
Muud eelarveread (märkige)								
• Koosseisuväline personal (täistööajale taandatud töötajad) [78]								
20 02 01 (üldvahenditest rahastatavad lepingulised töötajad, riikide lähetatud eksperdid ja renditööjõud)								
20 02 03 (lepingulised töötajad, kohalikud töötajad, riikide lähetatud eksperdid, renditööjõud ja noored eksperdid delegatsioonides)								
XX 01 xx **yy zz** [79]	- peakorteris							
	- delegatsioonides							
01 01 01 02 (lepingulised töötajad, riikide lähetatud eksperdid ja renditööjõud kaudse teadustegevuse valdkonnas)								
01 01 01 12 (lepingulised töötajad, riikide lähetatud eksperdid ja renditööjõud otsese teadustegevuse valdkonnas)								
Muud eelarveread (märkige)								
KOKKU		**10**	**10**	**10**	**10**	**10**	**10**	

XX tähistab asjaomast poliitikavaldkonda või eelarvejaotist.

Personalivajadused kaetakse juba meedet haldavate peadirektoraadi töötajatega ja/või töötajate peadirektoraadisisese ümberpaigutamise teel. Vajaduse korral võidakse personali täiendada iga-aastase vahendite eraldamise menetluse käigus, arvestades olemasolevate eelarvepiirangutega.

Eeldatavasti katab Euroopa Andmekaitseinspektor poole vajalikest vahenditest.

Ametnikud ja ajutised töötajad	Neli AD täistööaja ekvivalenti ja üks AST täistööaja ekvivalent kulub kuni 13–16 koosoleku ettevalmistamiseks, aruannete projektide koostamiseks, poliitikaalase töö jätkamiseks, näiteks seoses suure riskiga tehisintellektirakenduste loetelu tulevaste muudatustega, ning suhete säilitamiseks liikmesriikide ametiasutustega.

[77] Kõik selle veeru arvud on esialgsed ja olenevad programmide jätkumisest ning assigneeringute saadavusest.

[78] Lepingulised töötajad, kohalikud töötajad, riikide lähetatud eksperdid, renditööjõud, noored spetsialistid delegatsioonides.

[79] Tegevusassigneeringutest rahastatavate koosseisuväliste töötajate ülempiiri arvestades (endised BA read).

	ELi asutuste arendatud tehisintellektisüsteemide eest vastutab Euroopa Andmekaitseinspektor. Varasema kogemuse põhjal võib hinnata, et õigusakti ettepanekust tulenevate Euroopa Andmekaitseinspektori ülesannete täitmiseks on vaja viis AD täistööaja ekvivalenti.
Koosseisuvälised töötajad	

Ülesannete kirjeldus:

3.2.4. Kooskõla kehtiva mitmeaastase finantsraamistikuga

Ettepanek/algatus:

– X on täielikult rahastatav mitmeaastase finantsraamistiku asjaomase rubriigi sisese vahendite ümberpaigutamise kaudu.

Ümberkavandamist ei ole vaja.

– ☐ tingib mitmeaastase finantsraamistiku asjaomases rubriigi mittesihtotstarbelise varu ja/või mitmeaastase finantsraamistiku määruses sätestatud erivahendite kasutuselevõtu.

Selgitage, millised toimingud on vajalikud, osutades asjaomastele rubriikidele, eelarveridadele ja summadele ning nimetades kasutatavad rahastamisvahendid.

– ☐ nõuab mitmeaastase finantsraamistiku muutmist.

Selgitage, millised toimingud on vajalikud, osutades asjaomastele rubriikidele, eelarveridadele ja summadele.

3.2.5. Kolmandate isikute rahaline osalus

Ettepanek/algatus:

– X ei hõlma kolmandate isikute poolset kaasrahastamist

– ☐ hõlmab kaasrahastamist, mille hinnanguline summa on järgmine:

assigneeringud miljonites eurodes (kolm kohta pärast koma)

	Aasta **N**[80]	Aasta **N + 1**	Aasta **N + 2**	Aasta **N + 3**	Lisage vajalik arv aastaid, et kajastada kogu finantsmõju kestust (vt punkt 1.6)			Kokku
Nimetage kaasrahastav asutus								
Kaasrahastatavad assigneeringud KOKKU								

[80] N on aasta, mil alustatakse ettepaneku/algatuse rakendamist. „N“ asemel tuleb märkida esimene eeldatav rakendamise aasta (näiteks 2021). Sama tuleb teha ka järgnevate aastate puhul.

3.3. Hinnanguline mõju tuludele

– ☐ Ettepanekul/algatusel on järgmine finantsmõju:

– ☐ Ettepanekul/algatusel on järgmine finantsmõju:

  – ☐ muudele tuludele

  – ☐ muudele tuludele

  – Palun märkige, kas see on kulude eelarveridasid mõjutav sihtotstarbeline tulu ☐

miljonites eurodes (kolm kohta pärast koma)

Tulude eelarverida	Jooksva aasta eelarves kättesaadavad assigneeringud	Ettepaneku/algatuse mõju[81]						
		Aasta **N**	Aasta **N + 1**	Aasta **N + 2**	Aasta **N + 3**	Lisage vajalik arv aastaid, et kajastada kogu finantsmõju kestust (vt punkt 1.6)		
Artikkel ….								

Sihtotstarbeliste tulude puhul märkige, milliseid kulude eelarveridasid ettepanek mõjutab.

Muud märkused (nt tuludele avaldatava mõju arvutamise meetod/valem või muu teave).

[81] Traditsiooniliste omavahendite (tollimaksud ja suhkrumaksud) korral tuleb märkida netosummad, st brutosumma pärast 20 % sissenõudmiskulude mahaarvamist.