



Brüssel, 12. september 2022
(OR. en)

12302/22

LIMITE

JUR 579
TELECOM 364
COSI 217
JAI 1155
ENFOPOL 451

Institutsioonidevaheline
dokument:
2021/0106(COD)

ÕIGUSTALITUSE ARVAMUS¹

Saatja: Õigustalitus

Teema: Ettepanek: Euroopa Parlamendi ja nõukogu määrus, millega nähakse ette tehisintellekti käsitlevad ühtlustatud õigusnormid

- ELi toimimise lepingu artiklite 114 ja 16 asjakohasus õigusliku alusena seoses sätetega, mida kohaldatakse õiguskaitse- ja õigusasutuste suhtes

I. SISSEJUHATUS

1. Kavandatava määrusega kehtestatakse liidus tehisintellektisüsteemide turule laskmise ja kasutuselevõtmise ühtlustatud normid (edaspidi „kavandatav määrus“)².

¹ Käesolev dokument sisaldab Euroopa Parlamendi ja nõukogu 30. mai 2001. aasta määruse (EÜ) nr 1049/2001 (üldsuse juurdepääsu kohta Euroopa Parlamendi, nõukogu ja komisjoni dokumentidele) artikli 4 lõike 2 alusel kaitstud õiguslast seisukohta, mida Euroopa Liidu Nõukogu ei ole üldsusele kättesaadavaks teinud. Loata avaldamise korral võib nõukogu kasutada kõiki seadusest tulenevaid õigusi.

² Dok 8115/21.

2. Telekommunikatsiooni ja infoühiskonna töörühma 7. aprilli 2022. aasta koosolekul võttis nõukogu õigustalituse sõna tehisintellektisüsteeme käsitleva kavandatava määruse kahe õigusliku aluse (ELi toimimise lepingu artiklid 16 ja 114) asjakohasuse küsimuses. Selgituste kohaselt on ELi toimimise lepingu artiklid 16 ja 114 (on) ettepaneku jaoks õiged õiguslikud alused ning ELi toimimise lepingu artikli 114 asemel ei ole kohane kasutada ELi toimimise lepingu artikli 87 lõiget 2. Töörühma palvel esitatakse käesolevas arvamuses kirjalikult nõukogu õigustalituse esindaja poolt nimetatud koosolekul esitatud seisukoht ning arendatakse seda edasi.
3. Tehisintellektisüsteemid on määratletud kavandatava määruse artikli 3 lõikes 1. Üldiselt vastavad need teatavat liiki tarkvarale. Kavandatud määrust kohaldatakse nii tehisintellektisüsteeme turule laskvate pakkujate kui ka tehisintellektisüsteeme kasutusele võtvate pakkujate suhtes. Lisaks kohaldatakse kavandatavat määrust ka kasutajate suhtes. Pakkuja võib olla füüsiline või juriidiline isik või ametiasutus/organ, kes töötab välja tehisintellektisüsteemi või laseb tehisintellektisüsteemi välja töötada, et see turule lasta või kasutusele võtta oma nime või kaubamärgi all. Kasutaja võib olla füüsiline või juriidiline isik, ametiasutus, ametkond või muu organ, kes kasutab tehisintellektisüsteemi oma volituste alusel.

4. Artiklis 3 esitatud määratluste kohaselt võivad õiguskaitse- ja õigusasutused kvalifitseeruda tehisintellektisüsteemi pakkujateks ja/või kasutajateks. Tehisintellektisüsteemid, mille sihtotstarve on pakkuja määratluse kohaselt õiguskaitse või õigusemõistmine, liigitatakse III lisas suure riskiga süsteemideks. Seega kohaldatakse nende suhtes olulisi nõudeid (riskijuhtimine, testimine, andmehaldus, tehniline dokumentatsioon, läbipaistvus, inimjärelvalve, täpsus, stabiilsus ja küberturvalisus) ja kohustusi (nt kvaliteedijuhtimissüsteemid, tehniline dokumentatsioon, vastavushindamine, parandusmeetmed, teabekohustus, importijate ja turustajate kohustused) ning standardeid ja vastavushindamist. Need ühtlustatud normid on inspireeritud direktiivis 2006/42/EÜ (masinad)³ ja määruses 2017/745 (meditsiiniseadmed)⁴ tooteohutuse suhtes kohaldatavatest normidest.
5. Tehisintellektisüsteemid, mis hõlmavad reaajas toimuva biomeetrilise kaugtuvastuse süsteemide kasutamist avalikult juurdepääsetavas ruumis õiguskaitse eesmärgil, kuuluvad keelatud tehisintellektisüsteemide kategooriasse. Tehisintellektisüsteemide kasutamise keelu suhtes kohaldatakse siiski erandeid. Liikmesriigid võivad või ei pruugi lubada selliste süsteemide kasutamist. Kui nende kasutamine on lubatud, kohaldatakse nende suhtes üksikasjalikke piiranguid ja kaitsemeetmeid, et nende kasutamine piirduks sellega, mis on rangelt vajalik, ning kaitsta põhiõigust isikuandmete kaitsele. Need piirangud ja kaitsemeetmed on sätestatud kavandatavas määruses Euroopa Liidu toimimise lepingu (edaspidi „ELi toimimise leping“) artikli 16 alusel ning neid tuleb täiendada siseriikliku õigusega. Kavandatava määruse artikli 5 lõike 1 punkt d ning lõiked 2, 3 ja 4 kujutavad endast ELi toimimise lepingu artikli 16 lõike 2 alusel vastu võetud direktiivi 2016/680 (õiguskaitsealase andmekaitse direktiiv) suhtes erinormi.

³ Euroopa Parlamendi ja nõukogu 17. mai 2006. aasta direktiiv 2006/42/EÜ, mis käsitleb masinaid ja millega muudetakse direktiivi 95/16/EÜ (ELT L 157, 9.6.2006, lk 24–86).

⁴ 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 1–175).

Vastavalt artikli 5 lõike 1 punktile d piirduvad nende süsteemide eesmärgid järgmisega:

- 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) Euroopa vahistamismääruse otsuse⁵ 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.

Artikli 5 lõike 3 kohaselt peab õiguskaitseasutuste poolt selliste tehnoloogiate kasutamiseks olema õigus- või haldusasutuse eelnev luba. Nõuetekohaselt põhjendatud kiireloomulistel juhtudel võib siiski hakata süsteemi kasutama ilma loata ja loa võib taotleda kasutamise ajal või pärast seda.

Artikli 5 lõike 4 kohaselt võib liikmesriik otsustada anda loa reaalajas toimuva biomeetrilise kaugtuvastuse süsteemide kasutamiseks avalikult juurdepääsetavas ruumis õiguskaitse eesmärgil ning määrata kindlaks vajalikud üksikasjalikud normid eelneva loa taotlemiseks, väljastamiseks ja kasutamiseks ning määratleda seonduvad kuriteod.

6. Kavandatava määruse õiguslikeks alusteks on ELi toimimise lepingu artikkel 16 (isikuandmete kaitse) ja ELi toimimise lepingu artikkel 114 (siseturu toimimine). Seetõttu tekib küsimus, kas need õiguslikud alused on asjakohased seoses ühtlustatud normidega, mida kohaldatakse õiguskaitse- ja õigusasutuste pakutavate või kasutatavate tehisintellektisüsteemide suhtes.

⁵ Nõukogu 13. juuni 2002. aasta raamotsus 2002/584/JSK Euroopa vahistamismääruse ja liikmesriikidevahelise üleandmiskorra kohta (EÜT L 190, 18.7.2002, lk 1).

7. Käesolevas arvamuses keskendutakse kõigepealt ELi toimimise lepingu artikli 114 kui õigusliku aluse asjakohasusele eelkõige õiguskaitseasutuste kontekstis, mida on nimetatud kavandatava määruse mitmes sättes, st seoses reaajas toimuva biomeetrilise kaugtuvastuse süsteemide kasutamisega avalikult juurdepääsetavas ruumis ja III lisa punktis 6 osutatud suure riskiga tehisintellektisüsteemidega. Seetõttu käsitletakse käesolevas arvamuses küsimust, kas ELi toimimise lepingu artikli 87 lõige 2 (politseikoostöö) oleks ELi toimimise lepingu artikli 114 asemel sobivam õiguslik alus, et hõlmata tehisintellektisüsteemide pakkumist ja kasutamist õiguskaitseasutuste poolt (II jagu). Analoogia põhjal võib käesoleva märkuse järeldust kohaldada III lisas osutatud õigusasutuste suhtes seoses suure riskiga tehisintellektisüsteemidega.
8. Käesolevas märkuses käsitletakse ka ELi toimimise lepingu artikli 16 kui täiendava õigusliku aluse asjakohasust ning protokollide nr 21 ja 22 kohaldamist seoses reaajas toimuva biomeetrilise kaugtuvastuse süsteemide kasutamisega avalikult juurdepääsetavas ruumis õiguskaitseasutuste poolt (III jagu).

II. ELI TOIMIMISE LEPINGU ARTIKLI 114 KUI ÕIGUSLIKU ALUSE

ASJAKOHASUS

9. Väljakujunenud kohtupraktika kohaselt ei olene liidu õigusakti õiguslik alus institutsiooni seisukohast kõnealuse akti taotletava eesmärgi kohta, vaid see tuleb kindlaks määrata kohtulikult kontrollitavate objektiivsete asjaolude, sealhulgas eelkõige meetme eesmärgi ja sisu alusel. Kui asjaomase õigusakti kontrollimise käigus selgub, et sellel on kaks eesmärki või et sellega reguleeritakse kahte valdkonda ning üht neist saab lugeda põhiliseks või peamiseks, samas kui teine on üksnes kõrvalise tähtsusega, siis peab õigusaktil olema vaid üks õiguslik alus, see tähendab põhilisest või peamisest eesmärgist või valdkonnast tulenev õiguslik alus. Üksnes erandkorras, kui on kindlaks tehtud, et õigusaktil on samaaegselt mitu lahutamatu eesmärki, millest üks ei ole teise suhtes teisejärguline ega kaudne, võib asjaomane õigusakt tugineda vastavatele erinevatele õiguslikele alustele, välja arvatud juhul, kui nimetatud õiguslikes alustes kirjeldatakse menetlusi, mis on omavahel vastuolus. Samuti tuleks märkida, et ELi toimimise lepingu artikli 114 lõike 1 esimeses lauses selgitatakse, et selle artikli sätteid kohaldatakse, „*kui aluslepingutes ei ole ette nähtud teisiti*“. Seega on ELi toimimise lepingu artikli 114 kasutamine õigustatud üksnes juhul, kui asjaomase õigusakti vastuvõtmiseks ei saa õigusliku alusena kasutada konkreetsemat sätet⁶. Kui aluslepingus on konkreetsem säte, mis võib olla asjaomase õigusakti õiguslik alus, tuleb selle õigusakti aluseks võtta selline säte⁷.

⁶ Nõukogu õigustalituse 17. mai 2016. aasta arvamus 9007/16, punkt 6.

⁷ 29. aprilli 2004. aasta otsus kohtuasjas C-338/01, *komisjon vs. nõukogu*, EU:C:2004:253, punkt 60.

A. KAVANDATAVA MÄÄRUSE EESMÄRK

10. Kavandatava määrusega ühtlustatakse teatavat liiki tarkvara (tehisintellektisüsteemid) turule laskmist, kasutuselevõtmist ja kasutamist. Asjaolu, et avaliku sektori asutused ja eraettevõtjad võivad olla selliste tehisintellektisüsteemide pakkujad või kasutajad, ei ole iseenesest vastuolus sellega, et ELi toimimise lepingu artikkel 114 oleks õiguslikuks aluseks⁸.
11. Asjaolu, et õiguskaitseasutused või nende nimel tegutsevad asutused võivad kuuluda selliste tehisintellektisüsteemide pakkujate või kasutajate hulka, ei ole piisav, et õigustada ELi toimimise lepingu artikli 87 kasutamist õigusliku alusena. Kavandatava määruse eesmärki ja sisu tuleb analüüsida, et teha kindlaks, kas see on vajalik.
12. Kavandatava määruse üldine eesmärk on tagada järjepidev ja kõrgetasemeline kaitse kogu liidus, sealhulgas seoses reaallajas toimuva biomeetrilise kaugtuvastuse süsteemidega avalikult juurdepääsetavas ruumis ja suure riskiga tehisintellektisüsteemidega, vältides samal ajal erinevusi, mis takistavad tehisintellektisüsteemide ning nendega seotud toodete ja teenuste vaba liikumist siseturul. Selles sätestatakse operaatoritele ühetaolised kohustused ning tagatakse kaalukate üldiste huvidega seotud põhjuste ja isikute õiguste ühetaoline kaitse kogu siseturul (põhjendus 2). Konkreetsemalt sätestatakse kavandatava määrusega 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 (põhjendus 5). Üldiselt on ettepaneku eesmärk luua sisseprojekteeritud usaldusväärne tehisintellekt, mida kohaldatakse kõigis valdkondades, koos täielike normidega tehisintellektipõhiste toodete, teenuste ja süsteemide arendamiseks, turustamiseks ja kasutamiseks. Arvestades, et tehisintellekt on juba leidnud tee paljudesse teenustesse ja toodetesse ning see suundumus jätkub ka tulevikus, järgib ettepanek siseturu loogikat, kehtestades tooteohutuse raamistiku, mis tugineb neljale riskikategooriale. Sellega kehtestatakse suure riskiga tehisintellektisüsteemide turule sisenemise ja sertifitseerimise nõuded kohustusliku CE-märgise menetluse kaudu.

⁸ Vt nõukogu õigustalituse õiguslik arvamus (ST 11395/14, punktid 39–41) ja pretsedendid, nagu direktiiv (EL) 2016/2102, direktiivid 2014/24/EL, 2014/25/EL ja 2014/23/EL.

13. Ükski kavandatava määruse eesmärk ei viita avaliku julgeoleku eesmärkide tagamisele. Isegi kui avaliku julgeoleku eesmärke tuleb saavutada kaudselt õiguskaitseasutuste poolt tehisintellektisüsteemide turule laskmise / kasutuselevõtmise / kasutamise ühtlustamise kaudu, märkis Euroopa Kohus,⁹ tõlgendades ELi toimimise lepingu artikli 87 lõiget 2 ELi toimimise lepingu artikli 67 valguses, et selleks, et liidu õigusakt põhineks selle eesmärgi ja sisu arvestades esimesena nimetatud artiklil, peab see olema otseselt seotud ELi toimimise lepingu artiklis 67 sätestatud eesmärkidega (käesoleval juhul kuritegevuse tõkestamine ja politseikoostöö). See on kavandatava määruse kontekstis välistatud, kuna ainsad ühtlustatud normid, mis reguleerivad selliste süsteemide kasutamist õiguskaitseasutuste poolt, on kas 1) tooteohutuse laadi normid, mida kohaldatakse ühetaoliselt kõigi pakkujate ja kasutajate suhtes seoses tehisintellektisüsteemide turule laskmise / kasutuselevõtmise või kasutamisega, või 2) isikuandmete kaitse normid, mille jaoks lisati õigusliku alusena ELi toimimise lepingu artikkel 16 (vt III osa allpool).
14. Ühes teises kohtuasjas¹⁰ leidis Euroopa Kohus, et kuigi tulirelvade direktiivi muutmise eesmärk oli tagada avaliku julgeoleku kõrgem tase seoses terrorismiohu ja muude kuriteoliikidega, on kaupade ohutusega seotud aspektide ühtlustamine üks siseturu nõuetekohase toimimise olulisi elemente, kuna erinevused seda valdkonda reguleerivates normides tekitavad kaubandustõkkeid¹¹.

⁹ 6. mai 2014. aasta otsus kohtuasjas C43/12, *Euroopa Komisjon vs. Euroopa Parlament ja Euroopa Liidu Nõukogu*, EU:C:2014:298.

¹⁰ 3. detsembri 2019. aasta otsus kohtuasjas C-482/17, *Tšehhi Vabariik vs. Euroopa Parlament*, EU:C:2019:1035.

¹¹ Samas, punkt 57: „Kuna aga tulirelvade eripära seisneb vastupidi sellele, mida väidab Poola Vabariik, nende ohtlikkuses mitte ainult kasutajate, vaid ka laia avalikkuse jaoks, nagu tõi välja Euroopa Kohus 23. jaanuari 2018. aasta kohtuotsuse *Buhagiar jt* (C267/16, EU:C:2018:26) punktis 54, on avaliku julgeolekuga seotud kaalutlused, mida on mainitud ka direktiivi 91/477 viiendas põhjenduses, nende kaupade omandamist ja valdamist käsitlevate õigusaktide puhul ülimalt olulised“. Vt ka 23. jaanuari 2018. aasta otsus kohtuasjas C-267/16, *Albert Buhagiar jt vs. justiitsminister*, EU:C:2018:26, punkt 54: „Sellega seoses olgu märgitud, et arvestades ohtu, mida kujutavad endast inimeste turvalisusele tulirelvad, sai nende vaba liikumise saavutada ainult sel viisil, et reguleeritakse rangelt nende ühest liikmesriigist teise liikumise tingimusi, mille hulgas esineb põhimõte, et selliste kaupade liikumisega seotud liikmesriigid peavad andma eelneva loa“.

15. Kavandatava määruse eesmärgid, sealhulgas artikli 5 lõike 1 punkt d ning lõiked 2, 3 ja 4, milles käsitletakse reaalajas toimuva biomeetrilise kaugtuvastuse süsteemide kasutamist avalikult juurdepääsetavas ruumis õiguskaitse eesmärgil, ning III lisa punktis 6 osutatud suure riskiga tehisintellektisüsteemidega seotud sätted ei ole otseselt seotud avaliku julgeoleku eesmärgiga. Vastupidi, ettepanek vastab peamistele mureküsimustele, mis on seotud sellega, kuidas tehisintellektisüsteemid mõjutavad tervist, ohutust ja põhiõigusi. Seepärast on asjaomased sätted otseselt seotud eesmärgiga tagada võrdsed tingimused tehisintellektisüsteemide turule laskmisel / kasutusele võtmisel või kasutamisel siseturul, kaitstes samal ajal kasutajate tervist, ohutust ja põhiõigusi.
16. Eespool toodut arvesse võttes on kavandatava määruse peamine eesmärk parandada siseturu toimimist ELi toimimise lepingu artikli 114 tähenduses ning ELi toimimise lepingu artiklis 67 osutatud eesmärgid on selle peamise eesmärgiga üksnes kaudselt ja juhuslikult seotud.

B. KAVANDATAVA MÄÄRUSE SISU

17. Kavandatav määrus sisaldab sisuliselt norme selle kohta, mida on vaja konkreetse toote (tehisintellekti tarkvara) turule laskmiseks (või kasutuselevõtmiseks), et tagada selle ohutus ja põhiõiguste austamine. Selles sätestatakse täielik normide kogum tehisintellektil põhinevate toodete, teenuste ja süsteemide arendamiseks, turustamiseks ja kasutamiseks. Kavandatava määrusega ei kohustata õiguskaitseasutusi kasutama seaduslikult turule lastud tehisintellektisüsteemi ega reguleerita otseselt seda, kuidas õiguskaitseasutused peaksid sellist tehisintellektisüsteemi kasutama. Selle asemel piiritletakse selgelt olukorrad, kus kavandatud kasutust peetakse suure riskiga kasutuseks lihtsalt seetõttu, et tehisintellektisüsteemi kasutavad õiguskaitse- või õigusasutused.

18. Muu hulgas sisaldab kavandatava määruse artikkel 29 norme suure riskiga tehisintellektisüsteemide kasutamise tingimuste kohta, kuid selline säte ei ole sektoripõhine, sellel on piiratud kohaldamisala (peamiselt toote kasutusjuhendid) ja see on lahutamatult seotud kavandatava määrusega tehisintellektisüsteemide arendajatele pandud kohustustega. Samuti annab see liikmesriikidele teatava vabaduse kehtestada täiendavaid norme selliste suure riskiga tehisintellektisüsteemide kasutamise kohta. Seoses reaajas toimuva biomeetrilise kaugtuvastuse süsteemidega avalikes juurdepääsetavas ruumis, mida kasutatakse õiguskaitse eesmärgil (artikkel 5), reguleeritakse kavandatava määrusega osaliselt selliste süsteemide kasutamist andmekaitse seisukohast ELi toimimise lepingu artikli 16 alusel (vt III osa allpool).
19. Lisaks võivad ainult liikmesriigid otsustada näha ette võimaluse lubada täielikult või osaliselt kasutada selliseid reaajas toimuva biomeetrilise kaugtuvastuse süsteeme. Sellise kasutamise eritingimused tuleb sätestada siseriiklikus õiguses, kuid need peavad vastama määruses sätestatud üldistele kriteeriumidele ja kaitsemeetmetele: peab olema õigus- või haldusasutuse eelnev luba, eelneva loa taotlemine, väljastamine ja kasutamine ning märke kuritegude kohta, millega seoses selliseid süsteeme võib kasutada.

20. Tehisintellektisüsteemid on erilist liiki tarkvara. Seega on tehisintellektisüsteemide turule laskmise, kasutusele võtmise / kasutamise suhtes kohaldatavate ühtlustatud normide puhul tegemist tooteohutuse laadsete ühtlustatud normidega. Neid kohaldatakse ühetaoliselt, tegemata vahet avaliku- ja erasektori kasutajate vahel. Kavandatava määruse asjakohaste põhjenduste kohaselt tuleks seetõttu tagada järjepidev ja kõrgetasemeline kaitse kogu liidus. Samal ajal tuleks vältida erinevusi, mis takistavad tehisintellektisüsteemide ning nendega seotud toodete ja teenuste vaba liikumist siseturul. See saavutatakse, sätestades operaatoritele ühetaolised kohustused ning tagades kaalukate üldiste huvidega seotud põhjuste ja isikute õiguste ühetaolise kaitse kogu siseturul, tuginedes ELi toimimise lepingu artiklile 114¹².
21. Kavandatav määrus sisaldab suure riskiga tehisintellektisüsteeme käsitlevas III lisas mitut viidet õiguskaitsele, piirikontrollihaldusele ja õigusemõistmisele (vastavalt punktid 6, 7 ja 8). Need hõlmavad artikli 6 lõikele 2 vastavat üksikasjalikku ja ammendavat loetelu lisaks muudele suure riskiga süsteemidele seoses artikli 6 lõikes 1 osutatud tooteohutusriskidega. Artikli 6 lõike 1 kohaselt tuleb mõnda tehisintellektisüsteemi käsitada määratluse kohaselt suure riskiga süsteemidena nende eeldatava ulatuslikkuse ning põhiõigustele, tervisele ja ohutusele avalduvate suurte riskide tõttu. Muud süsteemid, mida peetakse suure riskiga süsteemideks ja mis on loetletud III lisas, hõlmavad haridust, elutähtsate taristute haldamist, tööhõivet, biomeetrilist tuvastamist ja kategoriseerimist ning juurdepääsu olulistele era- ja avalik-õiguslikele teenustele.

¹² 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 (vt ettepaneku põhjendused 2 ja 5).

22. Sellised suure riskiga tehisintellektisüsteeme käsitlevad normid ei näe siiski ette, kas õiguskaitse- ja õigusasutused (või asutused, mis tegutsevad muudes kindlaksmääratud valdkondades) peaksid neid süsteeme kasutama või mitte. Kavandataval määrusel on üksnes kaudne mõju selliste tehisintellektisüsteemide tegelikule arengule, mida õiguskaitseasutused võivad kasutada, ning praegu ja tulevikus kasutatavatele tehisintellektisüsteemidele. Seega osutatakse normides tehisintellektisüsteemidele, mis on „*ette nähtud kasutamiseks*“ selliste asutuste poolt (vt nt artikli 3 lõige 12, artikli 8 lõige 2 ja III lisa). Teatava tehisintellektisüsteemi suure riskiga süsteemide loetellu kandmise tagajärg on riskijuhtimist, andmehaldust ja tehnilisi kirjeldusi käsitlevate konkreetsete normide kohaldamine. Selliste suure riskiga tehisintellektisüsteemide kasutajad peavad järgima kasutusjuhendeid, pidama logisid ja koostama andmekaitsealaseid mõjuhinnanguid.
23. Peale selle võib liidu või liikmesriigi õiguses sätestada muid kasutajakohustusi peale kasutusjuhenditega seotud kohustuste, ilma et see piiraks kasutaja kaalutlusõigust oma vahendite ja tegevuse korraldamisel, et rakendada pakkuja märgitud inimjärelevalve meetmeid (kavandatava määrase artikli 29 lõige 2). Nende normidega nähakse suure riskiga tehisintellektisüsteemide jaoks ette täiendavad põhiõiguste kaitsemeetmed.

24. Eespool toodut arvesse võttes tuleks rõhutada, et kavandatav määrus ei sisalda norme, mille eesmärk on lubada või takistada turule lastud suure riskiga tehisintellektisüsteemi kasutamist õiguskaitseasutuste poolt. Kavandatud normide kohaselt lisatakse õiguskaitseasutuste arendatud või kasutatud tehisintellektisüsteemile eraldiseisev märgis (suure riskiga tehisintellektisüsteem) vastavalt kavandatud kasutusele. Sellist kasutamist reguleeriks siseriiklik õigus ja teataval määral otsustaksid selle üle õiguskaitseasutused ise. Kavandatavas määruses sätestatakse artiklis 29 suure riskiga tehisintellektisüsteemide minimaalsed kasutustingimused (mis piirduvad kasutusjuhenditega), mis hõlmab ka III lisa punktides 6, 7 ja 8 loetletud süsteeme, mida täiendatakse siseriikliku õigusega. Seepärast tuleks kooskõlas Euroopa Kohtu praktikaga eristada ühelt poolt kavandatava määruse kavandatud eesmärki, milleks ei ole õiguskaitseasutuste poolt tehisintellektisüsteemide kasutamise reguleerimine, ja teiselt poolt mõju, mida see võib kaudselt avaldada¹³ ning mis ei ole õigusliku aluse sobivuse analüüsimisel asjakohane.
25. Punktid 6, 7 ja 8 (vastavalt õiguskaitse, ränne ja õigusemõistmine) ei ole suure riskiga tehisintellektisüsteemide puhul esmatähtsad. Kavandatava määruse kohaselt ei pruugi suure riskiga tehisintellektisüsteem olla III lisas loetletud süsteem. Enamik suure riskiga süsteeme on tegelikult kavandatava määruse artikli 6 lõike 1 punktides a ja b üldiselt loetletud süsteemid (seoses toodete ohutusega). Muud suure riskiga tehisintellektisüsteemid on loetletud III lisas, mis sisaldavad punkte 1 (biomeetiline tuvastamine), 2 (elutähtis taristu), 3 (haridus ja kutseõpe) ja 4 (tööhõive, töötajate juhtimine ja füüsilisest isikust ettevõtjana tegutsemine), mis on seotud muude valdkondadega kui justiits- ja siseküsimused. Kõigi selliste suure riskiga tehisintellektisüsteemide kasutajate suhtes kohaldatakse ühtset korda, mis ei ole kehtestatud mitte nende erilise staatuse tõttu (nt kas nad on ettevõtja või avaliku sektori asutus), vaid tervise, ohutuse ja põhiõiguste kaitse seisukohast.

¹³ Vt 21. juuni 2018. aasta otsus kohtuasjas C-5/16, *Poola Vabariik vs. Euroopa Parlament, Euroopa Liidu Nõukogu*, EU:C:2018:483, punktid 63–68, ja 22. juuni 2022. aasta otsus kohtuasjas C-534/20, *Leistriz AG vs. LH*, EU:C:2022:495, punkt 28.

26. Kavandatav määrus sisaldab seega ühtlustatud norme tehisintellektisüsteemide turule laskmise, kasutusele võtmise ja kasutamise kohta, olenemata sellest, kas neid kasutavad eraettevõtjad või avaliku sektori asutused, sealhulgas¹⁴ õiguskaitse- ja õigusasutused.
27. Jättes kõrvale reaalarajas toimuva biomeetrilise kaugtuvastuse süsteemide kasutamise avalikult juurdepääsetavas ruumis õiguskaitse eesmärgil, mille suhtes kohaldatakse isikuandmete töötlemise erinorme (vt III osa allpool), ei sisalda kavandatav määrus ühtlustatud norme suure riskiga tehisintellektisüsteemide kasutamise kohta. Nagu on selgitatud eespool punktides 18 ja 19, on viide suure riskiga tehisintellektisüsteemide kasutamisele peamiselt seotud toote kasutusjuhistega (artikkel 29) ja seotud arendajatele pandud kohustustega. Nagu on märgitud punktis 22, tehakse otsus selle kohta, kas õiguskaitse- või õigusasutused võivad kasutada kavandatava määruse alusel seaduslikult turule lastud suure riskiga tehisintellektisüsteemi või mitte, siseriikliku õiguse alusel ja riiklike asutuste poolt.
28. Seetõttu ei ole ELi toimimise lepingu artikli 87 lõige 2, eriti selle punkt a kavandatava määruse jaoks sobiv õiguslik alus. Ettepaneku normidega ei edendata ega takistata asjakohase teabe kogumist, säilitamist, töötlemist, analüüsi ega vahetamist. Lihtsalt kui selliseid toiminguid teevad õiguskaitseasutused, tuleb kasutajate õiguste kaitsmiseks järgida mitut mittekonkreetselt ühtlustatud tingimust. Samuti ei hõlma kavandatava määruse eesmärgid ühiste uurimismeetodite väljatöötamist. Suure riskiga tehisintellektisüsteemide kasutamist käsitlevad kavandatud nõuded ei ole justiits- ja siseküsimuste valdkonnale eriomased ega puuduta politseikoostööd kitsamas tähenduses, nagu see on määratletud ELi toimimise lepingus.

¹⁴ Vt Euroopa Kohtu arvamus Istanbuli konventsiooni kohta, A-1/19, EU:C:2021:198, eelkõige punktid 298 ja 301.

29. Seoses kavandatava määruse artikli 5 lõike 4 sätetega võib liikmesriik siiski otsustada lubada reaalses toimiva biomeetrilise kaugtuvastuse süsteemide kasutamist avalikult juurdepääsetavas ruumis õiguskaitse eesmärgil. Kui liikmesriik nii otsustab, on ta kohustatud kehtestama vajalikud üksikasjalikud normid eelneva loa taotlemiseks, väljastamiseks ja kasutamiseks ning selliste kuritegude määratlemiseks, mille uurimise või süüdistuse esitamise eesmärgil selline luba antakse¹⁵. Nõukogus toimunud arutelude tulemuste põhjal ei annaks need kavandatavad normid vastavatele riiklikele ametiasutustele uusi volitusi. Selle asemel nähakse ette olemasolevate või võimalike tulevaste mehhanismide kasutamine, et tagada eraelu puutumatuse ja isikuandmete kaitse.
30. Eespool toodut arvesse võttes on ELi toimimise lepingu artikkel 114 ainus sobiv õiguslik alus ühtlustatud normidele, mis käsitlevad suure riskiga tehisintellektisüsteeme, sealhulgas neid, mida kasutavad õiguskaitse- ja õigusasutused, ning ELi toimimise lepingu kolmanda osa V jaotise kohased justiits- ja siseküsimuste õiguslikud alused, näiteks ELi toimimise lepingu artikkel 87, ei ole põhjendatud ega asjakohased.

¹⁵ Väärrib märkimist, et ettepaneku artikli 5 lõikel 4 on teatavad omadused, mis sarnanevad e-kaubanduse direktiivi 2002/58 artikli 15 lõikega 1. Eelkõige nähakse sellega liikmesriikidele ette võimalus teha erandeid teatavatest liidu õiguses sätestatud keeldudest. Väljakujunenud kohtupraktika kohaselt kuuluvad sellest keelust kõrvale kalduvad siseriiklikud õigusnormid tingimata liidu õiguse kohaldamisalasse, mis omakorda toob kaasa harta kohaldamise nende suhtes.

III. ELI TOIMIMISE LEPINGU ARTIKLI 16 KUI TÄIENDAVA ÕIGUSLIKU ALUSE ASJAKOHASUS

31. Kavandatud määrus sisaldab õigusliku alusena ELi toimimise lepingu artiklit 16, mis käsitleb isikuandmete töötlemist õiguskaitse valdkonnas, ning selle põhjendused 25 ja 26 sisaldavad viidet protokolli nr 21 artiklile 6a ja protokolli nr 22 artiklile 2a, mis käsitlevad isikuandmete töötlemist kriminaalpreventsiooni valdkonnas. Komisjoni arvates on ELi toimimise lepingu artikkel 16 mõeldud olema üksnes õiguslikuks aluseks sätetele, millega piiratakse biomeetriliste isikuandmete töötlemist direktiivi 2016/680 (edaspidi „õiguskaitse direktiiv“) täiendaval viisil. Artikli 5 lõike 1 punkt c on sõnastatud põhimõttelise keeluna, mille suhtes kohaldatakse kolme erandit. Konkreetset on „reaalajas toimuv“ biomeetrilise kaugtuvastuse süsteemide kasutamine avalikult juurdepääsetavas ruumis õiguskaitse eesmärgil keelatud, välja arvatud juhul, kui see on rangelt vajalik a) võimalike kuriteoohvrite sihipäraste otsingute tegemiseks, b) vahetu terrorirünnaku või isiku füüsilist turvalisust/elu vahetult ähvardava rünnaku ärahoidmiseks, c) raske kuriteo toimepanija või selle toimepanemises kahtlustatava asukoha kindlaks tegemiseks või tuvastamiseks või talle süüdistuse esitamiseks (viitega Euroopa vahistamismäärusele). Artikli 5 lõigetes 2, 3 ja 4 sätestatud täiendavad nõuded on seotud tehisintellektisüsteemide konkreetse kasutamisega õiguskaitseasutuste poolt, eelkõige vajalikkuse ja proportsionaalsuse hindamise, eelneva loa (välja arvatud eriolukordades) ja liikmesriikide otsusega, kas anda sellises olukorras riigi tasandil luba tehisintellektivahendite konkreetseks kasutamiseks või mitte.
32. Artikkel 5 on üksikasjalik säte, millega reguleeritakse tehisintellektivahendite konkreetset kasutamist ning mille eesmärk ei ole mitte ainult täiendada kehtivat liidu õigusraamistikku (Euroopa Liidu toimimise lepingu artiklil 16 põhinev õiguskaitse direktiiv), vaid see nõuab ka riiklikku rakendusraamistikku.

33. Vaatamata sellele, et artiklis 5 sätestatud erireegel on sõnastatud keeluna, võib seda sisuliselt kirjeldada nii, et sellega sätestatakse range ja erandlik raamistik avatud ruumis olevate isikute üldiseks ja reaalselt toimuvaks jälgimiseks tehisintellektivahendite abil nende tuvastamise eesmärgil. Keeld läheb ka kaugemale lihtsast salvestamisest kaamerate abil ja viitab tehisintellektivahendite kasutamisele inимtunnuste automaatseks tuvastamiseks avalikult juurdepääsetavas ruumis (sellised tunnused nagu nägu, aga ka kõnnak, sõrmejäljed, DNA, hääl, klahvivajutused ja muud biomeetrilised või käitumuslikud signaalid). See tähendab ka isikute andmete samaaegset kogumist ja tuvastamist andmete võrdlemise/kontrollimise teel. Lisaks tuleb seda reeglit hinnata ka seoses asjaoluga, et ka erasektori kasutajatel võib olla lubatud avalikes kohtades teostada reaalselt tuvastamist (näiteks seoses jalgpallivõistlustega).
34. Komisjoni esitatud lisaselgitused näivad viitavat sellele, et praegu ei ole ükski liikmesriik seda konkreetset küsimust reguleerinud või on seda teinud väga vähesed liikmesriigid, et võimaldada õiguskaitseasutustel kasutada tehisintellektivahendeid isikute reaalselt tuvastamiseks avalikus ruumis. Kuigi praktikas ei esitatud kindlaid tõendeid selle kohta, et olemasolevaid tavasid ja vahendeid on vaja muuta, näib siiski selge, et tulevastel uurimismeetodites, kohtuekspertiisi meetodites ja tõendite kogumise eeskirjades tuleb arvesse võtta sellist keelul/eranditel põhinevat lähenemisviisi.
35. Mis puudutab õiguslikku alust, siis näib, et sätetega, millega piiratakse biomeetriliste isikuandmete töötlemist (õiguskaitse direktiivi) täiendaval viisil, püütakse kaitsta isikuandmeid, kehtestades asjakohased kaitsemeetmed. Selline eesmärk on lahutamatu seotud ELi toimimise lepingu artikli 114 kohaldamisalasse kuuluvate sätete eesmärgiga, ilma et üks neist oleks teise suhtes teisene ja kaudne. Kavandatava määruse eesmärk on kehtestada tehisintellektisüsteemide üldraamistik, järgides riskipõhist lähenemisviisi. Sellega seoses võib tehisintellektisüsteemide horisontaalne reguleerimine hõlmata rangeid kaitsemeetmeid, mida kohaldatakse selle konkreetse reaalselt toimuva tuvastamise tehisintellektisüsteemi suhtes. Selline konkreetne tehisintellektisüsteem, mis sisaldab asjakohaseid isikuandmete kaitse kaitsemeetmeid, on seetõttu lahutamatu seotud üldeesmärgiga parandada siseturu toimimist ega ole viimasega võrreldes teisene ega kaudne. Kavandataval määrusel peaks seega olema kaks õiguslikku alust vastavalt asjakohasele kohtupraktikale (vt eespool punkt 9).

36. Siiski jääb küsimus, millist õiguslikku alust tuleks kasutada isikuandmete töötlemise reguleerimiseks kavandatava määruse artikli 5 lõike 1 punktis c kuni lõikeni 4 osutatud süsteemide kasutamisel. ELi toimimise lepingu artikli 87 lõike 2 punkt a on õiguslik alus meetmetele, mida õiguskaitseasutused võtavad seoses kuritegude tõkestamise, avastamise ja uurimisega ning mis on seotud asjakohase teabe kogumise, säilitamise, töötlemise, analüüsi ja vahetamisega.
37. Nagu kohtujurist selgitas kohtuasjas *PNR Canada* esitatud arvamuses (A1/15), ei saa ühelt poolt ELi toimimise lepingu artikkel 16 ja teiselt poolt ELi toimimise lepingu artikli 87 lõike 2 punkt a ja artikli 82 lõike 1 punkt d siiski olla üksteise suhtes hierarhilises seoses „*lex generalis – lex specialis*“¹⁶. ELi toimimise lepingu artikli 16 lõige 2 on ainus säte, mida kohaldatakse normide suhtes, mis käsitlevad üksikisikute kaitset isikuandmete töötlemisel liikmesriikide õiguskaitseasutuste poolt kuritegevuse tõkestamise eesmärgil. Ainuüksi asjaolu, et artiklis 5 viidatakse Euroopa vahistamismääruse raamotsuse raskete kuritegude loetelule, ei muuda seda hinnangut: see viide ei tähenda, et raamotsus on sellisena kohaldatav¹⁷. Raskete kuritegude loetlemine on üksnes seadusloometehnika, ilma et oleks vaja koostada eraldi lisa.
38. Siiski ei ole artiklis 5 sätestatud norm kehtestatud selleks, et täiendavalt piiritleda nende justiits- ja siseküsimustega seotud meetmete kohaldamise tingimusi, vaid selle eesmärk on tagada, et tulevikus vastab tehisintellektisüsteemide poolt reaalajas toimuva biomeetrilise tuvastuse mis tahes kasutamine piisavalt põhiõigustega seotud muredele ning eelkõige vajadusele tagada, et biomeetriliste andmete kogumisel ja töötlemisel austatakse õigust eraelu puutumatusle ja isikuandmete kaitset.

Sellega seoses ei ole määruse eesmärk kehtestada uut kohustuslikku justiits- ja siseküsimustega seotud menetlust, vaid selles tuginetakse läbiproovitud menetluslikele vahenditele, et tagada põhiõiguste austamine.

¹⁶ Vt kohtujurist P. Mengozzi 8. septembri 2016. aasta aramus *Kanada ja Euroopa Liidu vaheline lepingu kavand*, aramus 1/15, EU:C:2016:656, punktid 112–120.

¹⁷ Selle raskete kuritegude loetelu rakendamise kohta liikmesriikides vt Euroopa Kohtu 21. juuni 2022. aasta otsus kohtuasjas C-817/19 *Human Rights League vs. ministrite nõukogu*, EU:C:2022:65, punktid 150–152.

39. Kui ELi toimimise lepingu artikkel 16 on asjakohane täiendav õiguslik alus, tõstatab see küsimusi vastavalt protokollide nr 21 ja 22 artiklite 6a ja 2a kohaldamise kohta. Nagu on selgitatud ettepaneku põhjendustes 25 ja 26, tähendab see, et kui Iirimaa või Taani õiguskaitseasutused kasutavad reaalses toimiva biomeetrilise kaugtuvastuse süsteeme avalikult juurdepääsetavas ruumis kuritegevuse tõkestamiseks ja kui Iirimaa või Taani ei ole seotud vastavate politseikoostöö või kriminaalasjades tehtava õiguslase koostöö normidega, ei ole kavandatava määruse artikli 5 lõike 1 punkt d ning lõiked 2 ja 3 nende kahe liikmesriigi suhtes siduvad. See ei tähenda, et artikli 5 lõike 1 punkt d ning lõiked 2 ja 3 sisaldaksid politseikoostöö norme, näiteks norme õiguskaitseasutuste vahelise teabevahetuse kohta. See tähendab lihtsalt, et kavandatava määruse artikli 5 lõike 1 punkt d ning lõiked 2 ja 3 reguleerivad sarnaselt direktiiviga 2016/680 (õiguskaitse direktiiv), mis on ELi toimimise lepingu artikli 16 alusel vastu võetud *lex generalis*, biomeetriliste isikuandmete töötlemist avalikult juurdepääsetavas ruumis reaalses toimiva biomeetrilise kaugtuvastuse süsteemide kontekstis, et tõkestada kuritegevust ja mitte midagi enam. Sellega seoses järgib komisjoni ettepanek lähenemisviisi, mille liidu seadusandja on õiguskaitse direktiivi puhul säilitanud, ning kinnitab nõnda, et ELi toimimise lepingu artikli 87 lõike 2 kasutamine selles kontekstis ei ole seega põhjendatud.
40. ELi toimimise lepingu artikli 16 lisamine ELi toimimise lepingu artiklile 114 on käesoleval juhul põhjendatud asjaoluga, et artikli 5 lõike 1 punkt d ning lõiked 2 ja 3 on ainsad juhtumid, millega reguleeritakse loa saanud tehisintellektisüsteemi kasutamist, mis riivab õigust isikuandmete kaitsele, mis on üldise andmekaitseraamistiku *lex specialis*. Selliseid *lex specialis*'e andmekaitse norme, mis mõjutavad nende tundlike tehisintellektisüsteemide kasutamist, ei saa pidada siseturu õigusliku aluse suhtes teiseseks ega kaudseks. Seetõttu on ELi toimimise lepingu artikli 16 lisamine õigusliku alusena kavandatavas määruses piisavalt põhjendatud ja ELi toimimise lepingu artikli 87 lõike 2 punktile a tuginedes ei ole asjakohane.

IV. KOKKUVÕTE

41. Eeltoodut arvestades on nõukogu õigustalitus seisukohal, et:

- a) ELi toimimise lepingu artiklite 16 ja 114 kasutamine kavandatava määruse õigusliku alusena on põhjendatud ja asjakohane;
- b) ELi toimimise lepingu artikli 87 lõikele 2 või mis tahes muule justiits- ja siseküsimuste õiguslikule alusele tuginemine ei ole põhjendatud ega asjakohane seoses ühtlustatud normidega, mida kohaldatakse tehisintellektisüsteemide suhtes, mida õiguskaitse- või õigusasutused võivad pakkuda või kasutada.
