



**Euroopa
Andmekaitse nõukogu ja Euroopa
Andmekaitseinspektori**

ühisarvamus 5/2021

**ettepaneku kohta võtta
vastu Euroopa Parlamendi ja
nõukogu määrus, millega
nähaakse ette tehisintellekti
käsitlevad ühtlustatud
õigusnormid (tehisintellekti
käsitlev õigusakt)**

18. juuni 2021

Kommenteeritud kokkuvõte

Euroopa Komisjon esitas 21. aprillil 2021. aastal ettepaneku võtta vastu Euroopa Parlamendi ja nõukogu määrus, millega nähakse ette tehisintellekti käsitlevad ühtlustatud õigusnormid (edaspidi „ettepanek“). Euroopa Andmekaitseinspektor ja Euroopa Andmekaitseinspektor jagavad seadusandja muret tehisintellekti kasutamise kohta Euroopa Liidus (EL) ning rõhutavad, et ettepanekul on eriti oluline **mõju andmekaitsele**.

Euroopa Andmekaitseinspektor ja Euroopa Andmekaitseinspektor märgivad, et ettepaneku **õiguslik alus** on eelkõige ELi toimimise lepingu artikkel 114. Lisaks põhineb ettepanek ka ELi toimimise lepingu artiklil 16, kuivõrd see sisaldab erieeskirju üksikisikute kaitse kohta isikuandmete töötlemisel, eelkõige piiranguid tehisintellektisüsteemide kasutamisel õiguskaitse eesmärgil reaalses toimuvaks biomeetriliseks kaugtuvastamiseks avalikult juurdepääsetavates ruumides. Euroopa Andmekaitseinspektor ja Euroopa Andmekaitseinspektor tuletavad meelde, et koosõlas Euroopa Liidu Kohtu praktikaga on ELi toimimise lepingu artikkel 16 asjakohane õiguslik alus juhtudel, kui isikuandmete kaitse on ELi seadusandja vastuvõetud eeskirjade üks peamisi eesmärke või komponente. ELi toimimise lepingu artikli 16 kohaldamine eeldab ka **vajadust tagada** isikuandmete töötlemise **nõuete täitmise sõltumatu järelevalve**, nagu on nõutud ka ELi põhiõiguste harta artiklis 8.

Ettepaneku reguleerimisalaga seoses väljendavad Euroopa Andmekaitseinspektor ja Euroopa andmekaitseinspektor suurt heameelt asjaolu üle, et see laieneb tehisintellektisüsteemide pakkumisele ja kasutamisele ELi institutsioonides, asutustes või ametites. **Rahvusvahelise õiguskaitsekoostöö väljajätmine ettepaneku reguleerimisalast** tekitab aga Euroopa Andmekaitseinspektorile ja Euroopa andmekaitseinspektorile tõsist muret, sest selline väljajätmine toob kaasa märkimisväärse kõrvalehoidmise riski (nt kolmandad riigid või rahvusvahelised organisatsioonid, kes käitavad suure riskiga rakendusi, millele ELi ametiasutused tuginevad).

Euroopa Andmekaitseinspektor ja Euroopa Andmekaitseinspektor on rahul ettepaneku aluseks oleva **riskipõhise käsitlemusega**. Seda käsitlemist tuleks siiski selgitada ja mõiste „oht põhiõigustele“ tuleks viia koosõlla isikuandmete kaitse üldmääruse ja määrusega (EL) 2018/1725, sest mängu tulevad isikuandmete kaitsega seotud aspektid.

Euroopa Andmekaitseinspektor ja Euroopa Andmekaitseinspektor nõustuvad ettepanekuga, kui selles sätestatakse, et **tehisintellektisüsteemi suure riskiga süsteemiks liigitamine ei tähenda tingimata, et süsteem on iseenesest seaduslik** ja kasutaja võib selle sellisena kasutusele võtta. Võimalik, et vastutav töötleja peab **täitma ELi andmekaitsealastest õigusaktidest tulenevaid lisanõudeid**. Lisaks peaks liidu õigusaktidest (sealhulgas isikuandmete kaitse õigusaktidest) tulenevate juriidiliste kohustuste täitmine olema eeltingimuseks, et saada CE-märgisega tootena Euroopa turule sisenemise luba. Selles kontekstis leiavad Euroopa Andmekaitseinspektor ja Euroopa Andmekaitseinspektor, et **III jaotise 2. peatükki tuleks lisada nõue tagada vastavus isikuandmete kaitse üldmäärusega ning ELi institutsioonide, ametite, organite ja asutuste andmekaitsemäärusega**. Lisaks peavad Euroopa Andmekaitseinspektor ja Euroopa Andmekaitseinspektor vajalikuks kohandada ettepanekus esitatud vastavushindamismenetlust nii, et suure riskiga tehisintellektisüsteemide *ex-ante* vastavushindamist teeksid alati kolmandad isikud.

Võttes arvesse suurt diskrimineerimise ohtu, keelatakse ettepanekus „sotsiaalne hindamine“, kui see toimub „teatud aja jooksul“ või „ametiasutuste poolt või nende nimel“. Ka eraettevõtted, nt sotsiaalmeedia- ja pilveteenuste pakkujad, võivad töödelda tohutul hulgal isikuandmeid ja teha sotsiaalset hindamist. Sellest tulenevalt **peaks tulevane tehisintellekti määrus keelama igasuguse sotsiaalse hindamise**.

Füüsiliste isikute biomeetriline kaugtuvastamine avalikkusele juurdepääsetavates ruumides kujutab endast füüsiliste isikute eraellu sekkumise suurt ohtu, millel on oluline mõju elanikkonna ootusele olla avalikes ruumides anonüümne. Neil põhjustel nõuavad Euroopa Andmekaitseinspektor ja Euroopa

Andmekaitseinspektor **avalikult juurdepääsetavates ruumides viibivate inimeste tunnusjoonte** (nt nägude, aga ka kõnnaku, sõrmejälgede, DNA, hääle, klahvivajutuste ja muude biomeetriliste tunnuste või käitumissignaalide) **automaatsel tuvastamisel tehisintellekti kasutamise üldist keeldu** mis tahes kontekstis. **Keeld** on samuti soovitatav kehtestada **tehisintellektisüsteemidele, mis liigitavad üksikisikuid biomeetrilist tuvastamist kasutades rühmadesse** rahvuse, soo, poliitilise või seksuaalse sättumuse või harta artikliga 21 keelatud diskrimineerimise muude põhjuste alusel. Lisaks leiavad Euroopa Andmekaitseinspektor ja Euroopa Andmekaitseinspektor, et tehisintellekti kasutamine **füüsilise isiku emotsioonide tuletamiseks on väga ebasoovitav ja see tuleks keelata**.

Euroopa Andmekaitseinspektor ja Euroopa Andmekaitseinspektor tervitavad **Euroopa Andmekaitseinspektori nimetamist liidu institutsioonide, asutuste ja organite järelevalve pädevaks asutuseks ja turujärelevalveasutuseks**. Siiski tuleks Euroopa Andmekaitseinspektori tähtsust ja ülesandeid täpsemalt selgitada, eriti mis puudutab tema rolli turujärelevalveasutusena. Lisaks peaks tulevane tehisintellekti määrus selgelt kehtestama **järelevalveasutuste sõltumatuse** järelevalve- ja jõustamisülesannete täitmisel.

Andmekaitseasutuste määramine riiklikeks järelevalveasutusteks tagaks ühtlustatuma regulatiivse käsitlemise, soodustaks andmetöötlussätete järjepidevat tõlgendamist ja väldiks liikmesriikide vahelisi jõustamise vastuolusid. Seetõttu leiavad Euroopa Andmekaitseinspektor ja Euroopa Andmekaitseinspektor, et **andmekaitseasutused tuleks määrata riiklikeks järelevalveasutusteks vastavalt ettepaneku artiklile 59**.

Ettepanekuga antakse Euroopa tehisintellekti nõukojas komisjonile põhiroll. Selline roll on vastuolus vajadusega, et tehisintellektiga tegelev Euroopa asjaomane asutus oleks igasugusest poliitilisest mõjust sõltumatu. Sõltumatuse tagamiseks peaks tulevane tehisintellekti määrus andma **Euroopa tehisintellekti nõukojale rohkem autonoomiat** ja tagama, et see saaks tegutseda omal algatusel.

Arvestades tehisintellektisüsteemide levikut ühtsel turul ja piiriüleste juhtumite tõenäosust, on ühtlustatud jõustamine ja pädevuste nõuetekohane jaotamine riiklike järelevalveasutuste vahel äärmiselt oluline. Euroopa Andmekaitseinspektor ja Euroopa Andmekaitseinspektor soovivad kavandada **mehhanismi, mis tagaks iga tehisintellektisüsteemi jaoks nii õigusaktiga hõlmatud üksikisikute kui ka ettevõtete ühtse kontaktpunkti**.

Testkeskkondadega seoses soovivad Euroopa Andmekaitseinspektor ja Euroopa Andmekaitseinspektor **täpsustada nende ulatust ja eesmärke**. Ettepanekus tuleks samuti selgelt sätestada, et selliste testkeskkondade õiguslik alus peaks vastama kehtivas andmekaitse õigusraamistikus sätestatud nõuetele.

Ettepanekus kirjeldatud **sertifitseerimissüsteemil puudub selge seos ELi andmekaitsealaste õigusaktide ning ELi ja liikmesriikide muude õigusaktidega**, mida kohaldatakse suure riskiga tehisintellektisüsteemide eri valdkondades, ning see ei võta arvesse **võimalikult vähete andmete kogumise ja lõimitud andmekaitse põhimõtteid**, mis on üks aspekte, mida tuleb arvestada **enne CE-vastavusmäärgise saamist**. Seetõttu soovivad Euroopa Andmekaitseinspektor ja Euroopa Andmekaitseinspektor ettepanekut muuta, et selgitada seost nimetatud määruse alusel väljastatud sertifikaatide ning andmekaitseertifikaatide, -pitserite ja -määrgiste vahel. Andmekaitseasutused peaksid osalema ühtlustatud standardite ja ühtsete tehniliste kirjelduste koostamisel ja kehtestamisel.

Mis puudutab **toimimisjuhendeid**, siis Euroopa Andmekaitseinspektor ja Euroopa Andmekaitseinspektor peavad **vajalikuks selgitada**, kas isikuandmete kaitset tuleks käsitleda toimimisjuhenditega hõlmatavate „lisanõuete” hulgas, ja tagada, et „tehnilised kirjeldused ja lahendused” ei oleks vastuolus kehtiva ELi andmekaitse õigusraamistiku reeglite ja põhimõtetega.

SISUKORD

| | | |
|-------|--|----|
| 1 | SISSEJUHATUS | 5 |
| 2 | ETTEPANEKU KESKSETE PÕHIMÕTETE ANALÜÜS..... | 7 |
| 2.1 | Ettepaneku reguleerimisala ja seos kehtiva õigusraamistikuga | 7 |
| 2.2 | Riskipõhine käsitlus | 8 |
| 2.3 | Tehisintellekti keelatud kasutusviisid | 11 |
| 2.4 | Suure riskiga tehisintellektisüsteemid | 13 |
| 2.4.1 | Kolmandate isikute <i>ex-ante</i> vastavushindamise vajadus | 13 |
| 2.4.2 | Reguleerimisala peab hõlmama ka juba kasutusel olevaid tehisintellektisüsteeme | 13 |
| 2.5 | Juhtimine ja Euroopa tehisintellekti nõukogu | 14 |
| 2.5.1 | Juhtimine | 14 |
| 2.5.2 | Euroopa tehisintellekti nõukoda | 16 |
| 3 | KOOSTOIME andmekaitse õigusraamistikuga | 17 |
| 3.1 | Ettepaneku koostoime ELi kehtivate andmekaitse õigusaktidega | 17 |
| 3.2 | Testkeskkond ja täiendav töötlemine (ettepaneku artiklid 53 ja 54)..... | 18 |
| 3.3 | Läbipaistvus | 20 |
| 3.4 | Andmete eriliikide ja kuritegudega seotud andmete töötlemine | 21 |
| 3.5 | Vastavusmehhanismid..... | 21 |
| 3.5.1 | Sertifitseerimine | 21 |
| 3.5.2 | Tegevusjuhendid | 22 |
| 4 | JÄRELDUSED | 24 |

Euroopa Andmekaitse nõukogu ja Euroopa Andmekaitseinspektor,

võttes arvesse 23. oktoobri 2018. aasta määruse (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/EÜ¹) artikli 42 lõiget 2,

võttes arvesse Euroopa Majanduspiirkonna (EMP) lepingut, eriti selle XI lisa ja protokollid nr 37, mida on muudetud EMP ühiskomitee 6. juuli 2018. aasta otsusega nr 154/2018²,

võttes arvesse 22. aprilli 2021. aasta taotlust Euroopa Andmekaitseinspektori ja Euroopa Andmekaitse nõukogu ühisarvamuseks ettepaneku kohta võtta vastu Euroopa Parlamendi ja nõukogu määrus, millega nähakse ette tehisintellekti käsitlevad ühtlustatud õigusnormid (tehisintellekti käsitlev õigusakt),

ON VASTU VÕTNUD JÄRGMISE ÜHISARVAMUSE

1 SISSEJUHATUS

1. Tehisintellektisüsteemide tulek on väga oluline samm tehnoloogia arengus ja viisis, kuidas inimesed tehnoloogiaga suhtlevad. Tehisintellekt on oluliste tehnoloogiate kogum, mis muudab põhjalikult meie igapäeva elu, nii ühiskondlikust kui ka majanduslikust vaatepunktist. Lähiaastatel on tehisintellekti vallas oodata otsustavaid otsuseid, sest see aitab meil ületada teatud suuri probleeme, millega täna paljudes valdkondades silmitsi seisame (nt tervishoid, liikuvus, avalik haldus või haridus).
2. Lubatud edusammud ei tule aga riskideta. Riskid on väga olulised, sest me pole tehisintellektisüsteemide individuaalsete ja ühiskondlike tagajärgedega suurel määral varem kokku puutunud. Sisu loomine, prognooside tegemine või otsuste langetamine automatiseeritud viisil, nagu seda teevad tehisintellektisüsteemid masinõppetehnikate või loogika- ja tõenäosustõlgenduse reeglite abil, ei ole sama, kui seda teevad loominguliste või teoreetiliste mõttekäikude abil inimesed, kandes tagajärgede eest täielikku vastutust.
3. Tehisintellekt suurendab paljudes valdkondades tehtavate prognooside hulka, alates inimsilmale nähtamatutest (kuid masinatele nähtavatest) mõõdetavatest andmekorrelatsioonidest, muutes meie elu lihtsamaks ja lahendades mitmeid probleeme, kuid samas õõnestab meie suutlikkust tulemusi põhjuslikult tõlgendada, nii et läbipaistvuse, inimkontrolli, aruandekohustuse ja tulemuste eest vastutamise mõisted satuvad tõsisesse ohtu.

¹ ELT L 295, 21.11.2018, lk 39–98.

² Kõiki käesoleva dokumendi viiteid liikmesriikidele tuleb mõista kui viiteid EMP liikmesriikidele.

4. Tehisintellekti (isiklikud ja isikustamata) andmed on paljudel juhtudel autonoomse otsustusprotsessi põhieeldus, mis paratamatult mõjutab eri tasanditel üksikisikute elu. Seetõttu rõhutavad Euroopa Andmekaitsekoogu ja Euroopa Andmekaitseinspektor juba praegu, et määruse ettepanekul, millega nähakse ette tehisintellekti käsitlevad ühtlustatud õigusnormid (tehisintellekti käsitlev õigusakt; edaspidi „ettepanek”)³, on **oluline mõju andmekaitsele**.
5. Andmete põhjal otsuste tegemise ülesande andmine masinatele ohustab üksikisikute õigusi ja vabadusi, mõjutab nende eraelu ja võib kahjustada rühmi või isegi ühiskondi tervikuna. Euroopa Andmekaitsekoogu ja Euroopa Andmekaitseinspektor rõhutavad, et inimõiguste ülddeklaratsioonis (artikkel 12), Euroopa inimõiguste konventsioonis (artikkel 8) ja ELi põhiõiguste hartas (edaspidi „harta”) (artiklid 7 ja 8) tunnustatud ELi väärtuste sambaks on õigus eraelule ja isikuandmete kaitsele, mis on tehisintellekti mõiste aluseks oleva masinate otsustusautonoomia eeldusega vastuolus. Tehisintellekti rakenduste pakutava kasvuperspektiivi ning inimkesksuse ja inimese ülimuslikkuse ühitamine masinatega on väga ambitsioonikas, kuid siiski vajalik eesmärk.
6. Euroopa Andmekaitsekoogu ja Euroopa Andmekaitseinspektor tervitavad kõigi sidusrühmade kaasamist tehisintellekti väärtusahela reguleerimisse ja erinõuete kehtestamist lahenduste pakkujatele, sest need on selliseid süsteeme kasutavate toodete puhul ülimalt olulised. Siiski tuleb eri osaliste – tehisintellektisüsteemi kasutaja, pakkuja, importija või turustaja – kohustused selgelt piiritleda ja kindlaks määrata. Eelkõige tuleks isikuandmete töötlemisel pöörata erilist tähelepanu nende ülesannete ja kohustuste kooskõlale andmekaitse õigusraamistiku vastutava töötleja ja volitatud töötleja mõistetega, sest mõlemad normid ei ole kooskõlas.
7. Ettepanekus on oluline koht inimjärelvalve mõistel (artikkel 14), mida Euroopa Andmekaitsekoogu ja Euroopa Andmekaitseinspektor tunnustavad. Kuid nagu eespool öeldud, peaks teatavate tehisintellektisüsteemide tugeva potentsiaalse mõju tõttu üksikisikutele või rühmadele tegelik inimkesksus põhinema pädeval inimjärelvalvel ja seaduslikul töötlemisel, juhul kui sellised süsteemid põhinevad isikuandmete töötlemisel või töötlevad isikuandmeid oma ülesande täitmiseks, et järgitaks õigust, mille kohaselt füüsilise isiku kohta ei tohi teha otsust, mis põhineb üksnes automatiseeritud töötlusel.
8. Lisaks peaks ettepanek paljude tehisintellekti rakenduste andmemahukuse tõttu soodustama lõimitud ja vaikimisi andmekaitse põhimõtte järgimist igal tasandil, julgustades andmekaitse põhimõtete (nagu on ette nähtud isikuandmete kaitse üldmääruse artiklis 25 ning ELi institutsioonide, ametite, organite ja asutuste andmekaitsemääruse artiklis 27) tõhusat rakendamist kaasaegse tehnoloogia abil.
9. Lõpetuseks rõhutavad Euroopa Andmekaitsekoogu ja Euroopa Andmekaitseinspektor, et käesolev ühisarvamus esitatakse ainult ettepaneku esialgse analüüsina, ilma et see mõjutaks ettepaneku mõju edasist hindamist ja analüüsimist ning selle kooskõla ELi andmekaitsealaste õigusaktidega.

³ COM(2021) 206 final

2 ETTEPANEKU KESKSETE PÕHIMÕTETE ANALÜÜS

2.1 Ettepaneku reguleerimisala ja seos kehtiva õigusraamistikuga

10. Seletuskirja kohaselt on ettepaneku **õiguslik alus** eelkõige ELi toimimise lepingu artikkel 114, mis näeb ette siseturu loomise ja toimimise tagamiseks vajalike meetmete vastuvõtmise⁴. Lisaks põhineb ettepanek ka ELi toimimise lepingu artiklil 16, *kuivõrd see sisaldab erieeskirju üksikisikute kaitse kohta isikuandmete töötlemisel, eelkõige piiranguid tehisintellektisüsteemide kasutamisel õiguskaitse eesmärgil reaalses toimuvaks biomeetriliseks kaugtuvastamiseks avalikult juurdepääsetavates ruumides*⁵.
11. Euroopa Andmekaitseinspektor ja Euroopa Andmekaitseinspektor tuletavad meelde, et kooskõlas Euroopa Liidu Kohtu praktikaga on ELi toimimise lepingu artikkel 16 asjakohane õiguslik alus juhtudel, kui isikuandmete kaitse on ELi seadusandja vastu võetud eeskirjade üks peamisi eesmärke või komponente⁶. ELi toimimise lepingu artikli 16 kohaldamine eeldab ka vajadust tagada isikuandmete töötlemise nõuete täitmise sõltumatu järelevalve, nagu on nõutud ka harta artiklis 8.
12. Euroopa Andmekaitseinspektor ja Euroopa Andmekaitseinspektor tuletavad meelde, et ELi toimimise lepingu artikli 16 alusel vastu võetud terviklik andmekaitse õigusraamistik on juba olemas ja koosneb andmekaitse üldmäärusest⁷, ELi institutsioonide, ametite, organite ja asutuste andmekaitsemäärusest⁸ ning õiguskaitse direktiivist⁹. Ettepaneku kohaselt võib ELi toimimise lepingu artiklile 16 tuginevaks ja seega isikuandmete kaitse üldmääruse, ELi institutsioonide, ametite, organite ja asutuste andmekaitsemääruse ning õiguskaitse direktiiviga sama õiguslikku alust omavaks pidada ainult biomeetriliste andmete töötlemise täiendavaid piiranguid. Sellel on oluline mõju ettepaneku koostoimele isikuandmete kaitse üldmääruse, ELi institutsioonide, ametite, organite ja asutuste andmekaitsemääruse ning õiguskaitse direktiiviga üldiselt, nagu on allpool kirjeldatud.
13. Mis puudutab **ettepaneku reguleerimisala**, siis on Euroopa Andmekaitseinspektor ja Euroopa andmekaitseinspektor väga rahul asjaoluga, et see laieneb tehisintellektisüsteemide kasutamisele ELi institutsioonide, asutuste või ametite poolt. Et sarnaselt ELi liikmesriikides kasutamisele võib nendes üksustes tehisintellektisüsteemide kasutamine samuti oluliselt

⁴ Seletuskiri, lk 5.

⁵ Seletuskiri, lk 6. Vt ettepaneku põhjendus 2.

⁶ 26. juuli 2017. aasta arvamus, *PNR Canada*, arvamusmenetlus 1/15, ECLI:EU:C:2017:592, punkt 96.

⁷ 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 1–88).

⁸ 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 39–98).

⁹ 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 (ELT L 119, 4.5.2016, lk 89–131).

mõjutada üksikisikute põhiõigusi, on hädavajalik, et tehisintellekti reguleerivat uut raamistikku kohaldataks nii ELi liikmesriikide kui ka ELi institutsioonide, ametite, organite ja asutuste suhtes, et tagada kogu liidus ühtne lähenemine. Kuna ELi institutsioonid, ametid, organid ja asutused võivad tegutseda nii tehisintellektisüsteemide pakkujate kui ka kasutajatena, peavad Euroopa Andmekaitseinspektor ja Euroopa Andmekaitsekoostöö igati asjakohaseks kaasata need üksused ELi toimimise lepingu artikli 114 alusel ettepaneku reguleerimisalasse.

14. Euroopa Andmekaitsekoostöö ja Euroopa Andmekaitseinspektor on siiski tõsiselt mures rahvusvahelise õiguskaitsealase koostöö väljajätmise pärast ettepaneku artikli 2 lõikes 4 sätestatud reguleerimisalast. See väljajätmine toob kaasa märkimisväärse kõrvalehoidmise riski (nt kolmandad riigid või rahvusvahelised organisatsioonid, kes haldavad suure riskiga rakendusi, millele ELi ametiasutused tuginevad).
15. Tehisintellektisüsteemide väljatöötamine ja kasutamine hõlmab paljudel juhtudel isikuandmete töötlemist. Selgus käesoleva ettepaneku ja ELi andmekaitsealaste olemasolevate õigusaktide vahel on äärmiselt oluline. Ettepanek ei ole piirav ja täiendab isikuandmete kaitse üldmäärust, ELi institutsioonide, ametite, organite ja asutuste andmekaitsemäärust ning õiguskaitse direktiivi. Kuigi ettepaneku põhjendustes selgitatakse, et tehisintellektisüsteemide kasutamine peaks siiski vastama andmekaitsealastele õigusaktidele, **soovitavad Euroopa Andmekaitsekoostöö ja Euroopa Andmekaitseinspektor tungivalt selgitada ettepaneku artiklis 1, et isikuandmete kaitset käsitlevaid liidu õigusakte**, eelkõige isikuandmete kaitse üldmäärust, ELi institutsioonide, ametite, organite ja asutuste andmekaitsemäärust, e-privatsuse direktiivi¹⁰ ning õiguskaitse direktiivi, kohaldatakse ettepaneku reguleerimisalasse kuuluva mis tahes isikuandmete töötlemistoimingu suhtes. Vastavas põhjenduses tuleks samuti selgitada, et ettepanekuga ei püüta mõjutada isikuandmete töötlemist reguleerivate ELi olemasolevate õigusaktide kohaldamist, sh nende õigusaktide täitmist kontrollivate sõltumatute järelevalveasutuste ülesandeid ja volitusi.

2.2 Riskipõhine käsitlus

16. Euroopa Andmekaitsekoostöö ja Euroopa Andmekaitseinspektor **tervitavad** ettepaneku aluseks olevat **riskipõhist käsitlust**. Ettepanek käsitleb kõiki tehisintellektisüsteeme, sealhulgas neid, mis ei hõlma isikuandmete töötlemist, kuid võivad siiski mõjutada huve või põhiõigusi ja -vabadusi.
17. Euroopa Andmekaitsekoostöö ja Euroopa Andmekaitseinspektor märgivad, et ettepaneku teatud sätetest on jäetud välja üksikisikute rühmadele või ühiskonnale tervikuna avalduvad riskid (nt erilise tähtsusega kollektiivsed mõjud nagu rühmade diskrimineerimine või poliitiliste arvamuste avaldamine avalikes kohtades). Euroopa Andmekaitsekoostöö ja Euroopa Andmekaitseinspektor soovitavad tehisintellektisüsteemidest tulenevaid ühiskonna/rühmade riske võrdselt hinnata ja leevendada.

¹⁰ Euroopa Parlamendi ja nõukogu 12. juuli 2002. aasta direktiiv 2002/58/EÜ, milles käsitletakse isikuandmete töötlemist ja eraelu puutumatuse kaitset elektroonilise side sektoris (eraelu puutumatust ja elektroonilist sidet käsitlev direktiiv), mida on muudetud direktiiviga 2006/24/EÜ ja direktiiviga 2009/136/EÜ.

18. Euroopa Andmekaitseenõukogu ja Euroopa Andmekaitseinspektor on seisukohal, et ettepaneku riskipõhist käsitlemist tuleks selgitada ja isikuandmete kaitsega seotud aspektide kontekstis tuleks mõiste „oht põhiõigustele” viia **koosõlla isikuandmete kaitse üldmäärusega**. Olenemata sellest, kas tegemist on lõppkasutajate, lihtsalt andmesubjektide või muude isikutega, keda tehisintellektisüsteem puudutab, on ettepaneku nõrk külge viite puudumine tehisintellektisüsteemist mõjutatud üksikisikule. Mõjutatud isikute kontekstis osalejatele seatud kohustused peaksid tulenema konkreetsemalt üksikisiku ja tema õiguste kaitsest. Seega soovivad Euroopa Andmekaitseenõukogu ja Euroopa Andmekaitseinspektor seadusandjatele tungivalt, et nad käsitleksid ettepanekus selgesõnaliselt tehisintellektisüsteemi subjektiks olevate **üksikisikute õigusi ja õiguskaitsevahendeid**.
19. Euroopa Andmekaitseenõukogu ja Euroopa Andmekaitseinspektor võtavad teadmiseks, et otsustati koostada **suure riskiga tehisintellektisüsteemide** täielik loetelu. See otsus võib suure riskiga olukordade vähese köitvuse tõttu tekitada mustvalge efekti, kahjustades ettepaneku aluseks olevat üldist riskipõhist käsitlemist. Samuti puuduvad ettepaneku II ja III lisas esitatud suure riskiga tehisintellektisüsteemide üksikasjalikus loetelus teatud liiki kasutusmallid, millega kaasnevad olulised riskid, näiteks tehisintellekti kasutamine kindlustusmakse kindlaksmääramisel, ravi hindamisel või terviseuuringutes. Euroopa Andmekaitseenõukogu ja Euroopa Andmekaitseinspektor rõhutavad samuti, et neid lisasid tuleb korrapäraselt ajakohastada, et tagada nende kohaldamisala asjakohasus.
20. Ettepanekuga nõutakse tehisintellektisüsteemi **pakkujatelt** riskihindamist, kuid enamasti on (andmete) vastutavad töötajad pigem tehisintellektisüsteemide **kasutajad** kui pakkujad (nt näotuvastussüsteemi kasutaja on „vastutav töötaja“ ja seetõttu ei kehti talle suure riskiga tehisintellektisüsteemide pakkujatele ettepanekus kehtestatud nõuded).
21. Lisaks ei ole **pakkujal alati võimalik hinnata tehisintellektisüsteemi kõiki kasutusviise**. Seega on esialgne riskihindamine üldisem kui see, mille teeb tehisintellektisüsteemi kasutaja. Isegi kui pakkuja esialgne riskihindamine ei näita, et tehisintellektisüsteem on ettepaneku alusel „suure riskiga”, ei tohiks see välistada **hilisemat (üksikasjalikumalt) hindamist** (andmekaitsealane mõjuhinnang isikuandmete kaitse üldmääruse artikli 35, ELi institutsioonide, ametite, organite ja asutuste andmekaitsemääruse artikli 39 või õiguskaitse direktiivi artikli 27 alusel), **mille peaks tegema süsteemi kasutaja**, võttes arvesse kasutamise konteksti ja konkreetseid kasutusmalle. Ettepanekust sõltumatult tuleb tõlgendada seda, kas isikuandmete kaitse üldmääruse, ELi institutsioonide, ametite, organite ja asutuste andmekaitsemääruse ning õiguskaitse direktiivi alusel võib teatud tüüpi töötlemisega tõenäoliselt kaasneda suur risk. Tehisintellektisüsteemi liigitamine põhiõigustele avalduva mõju tõttu „suure riskiga” süsteemiks¹¹ **tekitab isikuandmete kaitse üldmääruse, ELi**

¹¹Euroopa Liidu Põhiõiguste Amet (FRA) on tehisintellekti või sellega seotud tehnoloogia kasutamisel põhiõiguste mõju hindamise vajadust juba käsitlenud. 2020. aasta aruandes „[Toimigem tulevikus õigesti. Tehisintellekt ja põhiõigused](#)“ tuvastas FRA „puudusi tehisintellekti kasutamises, näiteks ennetava politseitegevuse, meditsiinidiagnostika, sotsiaalteenuste ja suunatud reklaami valdkonnas“, ning rõhutas, et üksikisikutele avalduva negatiivse mõju vähendamiseks „peaksid era- ja avalikud organisatsioonid hindama, kuidas võib tehisintellekt põhiõigusi kahjustada”.

institutsioonide, ametite, organite ja asutuste andmekaitsemääruse ning õiguskaitsse direktiivi alusel siiski „suure riski” eelduse, kuivõrd töödeldakse isikuandmeid.

22. **Euroopa Andmekaitsekoostöö ja Euroopa Andmekaitseinspektor nõustuvad ettepanekuga, kui selles täpsustatakse, et tehisintellektisüsteemi suure riskiga süsteemiks liigitamine ei tähenda tingimata, et süsteem on iseenesest seaduslik ja kasutaja võib selle sellisena kasutusele võtta. On võimalik, et vastutav töötaja peab täitma ELi andmekaitsealastest õigusaktidest tulenevaid lisanõudeid.** Lisaks tuleb ettepanekus käsitleda ja lahendada ettepaneku artikli 5 aluspõhjendusi, mille kohaselt erinevalt keelatud süsteemidest võivad suure riskiga süsteemid olla põhimõtteliselt lubatud, sest eelkõige kavandatav CE-vastavusmäärus ei tähenda, et sellega seotud isikuandmete töötlemine on seaduslik.
23. Liidu õigusaktidest (sealhulgas isikuandmete kaitse õigusaktidest) tulenevate juriidiliste kohustuste täitmine peaks siiski olema eeltingimus, et saada CE-märgisega tootena Euroopa turule sisenemise luba. Selles kontekstis soovivad Euroopa Andmekaitsekoostöö ja Euroopa Andmekaitseinspektor **lisada ettepaneku III jaotise 2. peatükki nõue tagada vastavus isikuandmete kaitse üldmäärusega ning ELi institutsioonide, ametite, organite ja asutuste andmekaitsemäärusega.** Enne CE-vastavusmääruse andmist neid nõudeid auditeeritakse (kolmanda poole auditi kaudu) kooskõlas aruandluspõhimõttega. Kolmanda poole hinnangu kontekstis on teenuseosutaja tehtav esialgne mõjuhindang eriti asjakohane.
24. Tehisintellektisüsteemide arendamise keerukust arvestades tuleb märkida, et tehisintellektisüsteemide tehnilised omadused (nt tehisintellekti tüübipõhine käsitus) võivad kaasa tuua suuremaid riske. Seetõttu tuleks tehisintellektisüsteemi riskihindamises arvestada selle **tehnilisi omadusi, konkreetseid kasutusviise** ja süsteemi toimimise **konteksti**.
25. Eelöeldut silmas pidades soovivad Euroopa Andmekaitsekoostöö ja Euroopa Andmekaitseinspektor ettepanekus täpsustada, et **pakkuja** teeb asjaomase tehisintellektisüsteemi esialgse riskihindamise, **võttes arvesse kasutusmalle** (täpsustatakse ettepanekus, näiteks täiendades III lisa lõike 1 punkti a, kus tehisintellekti biomeetriliste süsteemide kasutusmalle ei mainita), ja et tehisintellektisüsteemi **kasutaja** peab andmekaitsealaste õigusaktide kohase vastutava töötajana (kui asjakohane) tegema andmekaitsealase mõjuhindangu, mida on üksikasjalikult kirjeldatud isikuandmete kaitse üldmääruse artiklis 35, ELi institutsioonide, ametite, organite ja asutuste andmekaitsemääruse artiklis 39 ning õiguskaitsse direktiivi artiklis 27, võttes arvesse mitte üksnes tehnilisi omadusi ja **kasutusmalli**, vaid ka **konkreetsed konteksti**, milles tehisintellekt töötab.
26. Lisaks tuleks selgitada ettepaneku III lisa nimetatud teatud termineid (nt „olulised erateenused” või „väikepakkujad, kes kasutavad krediitvõimelisuse hindamise tehisintellekti oma tarbeks“).

2.3 Tehisintellekti keelatud kasutusviisid

27. Euroopa Andmekaitseinspektor ja Euroopa Andmekaitseinspektor leiavad, et **tehisintellekti sekkuvaid vorme** – eriti neid, mis võivad mõjutada inimväärikust – tuleb käsitleda ettepaneku artikli 5 kohaselt keelatud tehisintellektisüsteemidena, selmet liigitada need ettepaneku III lisa punktis 6 „suure riskiga“ süsteemideks. See kehtib eelkõige andmete võrdlemise kohta, mis mõjutab suuresti ka isikuid, kes ei ole andnud politseivaatluseks mingit põhjust või on seda andnud vaid vähesel määral, või andmekaitsealaste õigusaktide eesmärgi piiramise põhimõtet kahjustavat töötlemist. Tehisintellekti kasutamine politsei- ja õiguskaitse valdkonnas nõuab valdkonnapõhiseid, täpseid, etteaimatavaid ja proportsionaalseid eeskirju, mis peavad arvestama asjaomaste isikute huvidega ja mõjuga demokraatliku ühiskonna toimimisele.
28. Ettepaneku artikliga 5 kaasneb risk, et „väärtuste” kohta antakse tühje lubadusi ja neile mittevastavad tehisintellektisüsteemid keelustatakse. Artiklis 5 osutatud kriteeriumid, mille alusel „kvalifitseeritakse“ tehisintellektisüsteemid keelatuks, **piiravad keelu ulatust** sellisel määral, et see võib praktikas osutada mõttetuks (nt „põhjustab või tõenäoliselt põhjustab [...] füüsilist või psühholoogilist kahju” artikli 5 lõike 1 punktides a ja b; piirangud ametiasutustele artikli 5 lõike 1 punktis c; ebamäärane sõnastus punkti c alapunktides i ja ii; reaalses toimiva biomeetrilise kaugtuvastamise piiramine ilma selge määratluseta jne).
29. Eelkõige võib tehisintellekti kasutamine „sotsiaalse hindamise“ jaoks, nagu on ette nähtud ettepaneku artikli 5 lõike 1 punktis c, põhjustada diskrimineerimist ja see on vastuolus ELi põhiväärtustega. Ettepanekus keelatakse vaid need tegevused, mis viiakse läbi „teatud aja jooksul“ või „ametiasutuste poolt või nende nimel“. Eraettevõtted, eelkõige sotsiaalmeedia- ja pilveteenuste pakkujad, võivad töödelda tohtul hulgal isikuandmeid ja teha sotsiaalset hindamist. Sellest tulenevalt **peaks ettepanek keelama igasuguse sotsiaalse hindamise**. Tuleb märkida, et õiguskaitse kontekstis piirab õiguskaitse direktiivi artikkel 4 seda tüüpi tegevusi juba märkimisväärselt (praktiliselt keelustab).
30. Üksikisikute **biomeetrilise kaugtuvastamisega** avalikult juurdepääsetavates ruumides kaasneb üksikisikute eraellu tungimise suur risk. Seetõttu leiavad Euroopa Andmekaitseinspektor ja Euroopa Andmekaitseinspektor, et on **vaja rangemat käsitlust**. Tehisintellektisüsteemide kasutamine võib tekitada suuri probleeme seoses proportsionaalsuse põhimõttega, sest see võib hõlmata valimatute ja ebaproportsionaalselt paljude andmesubjektide andmete töötlemist, et tuvastada vaid mõned üksikisikud (nt reisijad lennujaamades ja rongijaamades). Biomeetrilise kaugtuvastamise süsteemide **haardumatus** tekitab ka läbipaistvuse probleeme ja küsimusi, mis on seotud ELi õiguse kohase töötlemise õigusliku alusega (õiguskaitse direktiiv, isikuandmete kaitse üldmäärus, ELi institutsioonide, ametite, organite ja asutuste andmekaitsemäärus ja muud kohaldatavad õigusaktid). Endiselt on lahendamata probleem, kuidas füüsilisi isikuid sellisest töötlemisest nõuetekohaselt teavitada, samuti üksikisikute õiguste tõhusa ja õigeaegse kasutamise probleem. Sama kehtib **avalikes kohtades elanikkonna anonüümseks jäämise** (mõistlikule) **eeldusele avalduva pöördumatu ja olulise mõju kohta**, mille tulemuseks on otsene negatiivne mõju sõna-, kogunemis-, ühinemis- ja liikumisvabaduse kasutamisele.

31. Ettepaneku artikli 5 lõike 1 punktis d on esitatud ulatuslik **erandjuhtude loetelu**, mille korral on avalikult juurdepääsetavates ruumides reaajas toimuva biomeetrilise kaugtuvastamise süsteemide kasutamine õiguskaitses kontekstis lubatud. Euroopa Andmekaitseinspektoori ja Euroopa Andmekaitseinspektor peavad **seda käsitlemist** mitmes aspektis **vigaseks**. Esiteks on ebaselge, mida tuleks mõista „märkimisväärse viivituse” all ja kuidas seda pidada kergendavaks teguriks, arvestades, et massilise identifitseerimise süsteem suudab tuvastada tuhandeid isikuid vaid mõne tunniga. Lisaks ei sõltu töötlemise sekkumise ulatus alati sellest, kas tuvastamine toimub reaajas või mitte. Poliitilise protesti kontekstis tehtav biomeetriline kaugtuvastamine avaldab tõenäoliselt olulist heidutavat mõju põhiõiguste ja -vabaduste, nt kogunemis- ja ühinemisvabaduse ning üldiste demokraatia aluspõhimõtete teostamisele. Teiseks ei sõltu töötlemise sekkumise ulatus tingimata selle eesmärgist. Sellise süsteemi kasutamine muudel eesmärkidel, näiteks eraturvateenuse osutamiseks, kujutab samasugust ohtu era- ja pereelu austamise ning isikuandmete kaitses põhiõigustele. Lõpetuseks – isegi ettenähtud piirangute korral on kuritegudes kahtlustatavate või kuriteo toimepanijate potentsiaalne arv peaaegu alati „piisavalt suur“, et õigustada tehisintellektisüsteemide pidevat kasutamist kahtlustatavate tuvastamiseks, hoolimata artikli 5 lõikes 2–4 sätestatud lisatingimustest. Näib, et ettepaneku põhjendustes ei mainita, et avatud alade jälgimisel tuleb täita ELi andmekaitsealastest õigusaktidest tulenevaid kohustusi mitte ainult kahtlustatavate, vaid ka kõikide muude tegelikult jälgitavate isikute puhul.
32. Kõikidel nimetatud põhjustel **nõuavad** Euroopa Andmekaitseinspektoori ja Euroopa Andmekaitseinspektor **avalikult juurdepääsetavates ruumides viibivate inimeste tunnusoonte (nt nägude, aga ka kõnnaku, sõrmejälgede, DNA, hääle, klahvivajutuste ja muude biomeetriliste tunnuste või käitumissignaali) automaatsel tuvastamisel tehisintellekti kasutamise üldist keeldu mis tahes kontekstis**. Ettepaneku praegune käsitus on tuvastada ja loetleda kõik tehisintellektisüsteemid, mis tuleks keelata. Seega tuleks järjepidevuse huvides ettepaneku artikli 5 kohaselt keelata **küberryuumis toimuva laiaulatusliku kaugtuvastamise tehisintellektisüsteemid**. Võttes arvesse õiguskaitses direktiivi, ELi institutsioonide, ametite, organite ja asutuste andmekaitsemäärust ja isikuandmete kaitses üldmäärust, ei suuda Euroopa Andmekaitseinspektor ega Euroopa Andmekaitseinspektoori aru saada, kuidas seda tüüpi tegevused saaksid täita vajalikkuse ja proportsionaalsuse nõudeid, lähtuvalt sellest, mida Euroopa Kohus ja Euroopa Inimõiguste Kohus peavad vastuvõetavaks sekkumiseks põhiõigustesse.
33. Lisaks **soovitavad** Euroopa Andmekaitseinspektoori ja Euroopa Andmekaitseinspektor **keelata** nii ametiasutuste kui ka eraõiguslike üksuste puhul **tehisintellektisüsteemid, mis liigitavad üksikisikuid biomeetrilist tuvastust (nt näotuvastust) kasutades rühmadesse rahvuse, soo, poliitilise või seksuaalse sättumuse või harta artikliga 21 keelatud muude diskrimineerimise põhjuste alusel, või tehisintellektisüsteemid, mille teaduslik kehtivus ei ole tõestatud või mis on otseselt ELi alusväärtustega vastuolus (nt valedetektor, III lisa lõike 6 punkt b ja lõike 7 punkt a)**. Seetõttu tuleks **artikliga 5 keelata „biomeetriline liigitamine”**.

34. See mõjutab ka inimväärikust, kui arvuti määrab kindlaks või liigitab tulevase käitumise sõltumatult isiku vabast tahtest. Tehisintellektisüsteemid, mis on ette nähtud õiguskaitseasutustele füüsiliste isikutega seotud individuaalsete riskide hindamiseks, et hinnata, milline on risk, et füüsiline isik (taas)rikub seadust, vt III lisa lõike 6 punkt a, või tegeliku või potentsiaalse kuriteo esinemise või kordumise prognoosimiseks füüsiliste isikute profiilianalüüsi põhjal või isikuomaduste, iseloomujoonte või varasema kuritegeliku käitumise hindamiseks, vt III lisa lõike 6 punkt e, ja mida kasutatakse ettenähtud otstarbel, toovad kaasa politsei- ja kohtuotsusele allutamise, objektistades seeläbi mõjutatud inimese. Sellised tehisintellektisüsteemid, mis kahjustavad õigust inimväärikusele, tuleks artikli 5 alusel keelata.
35. Lisaks leiavad Euroopa Andmekaitseõukogu ja Euroopa Andmekaitseinspektor, et tehisintellekti kasutamine **füüsilise isiku emotsioonide tuletamiseks on väga ebasoovitav ja see tuleks keelata**, v.a teatud täpselt määratletud kasutusjuhud, näiteks tervishoiu või uurimistöe eesmärgil (nt patsiendid, kelle emotsioonide tuvastamine on oluline), kuid alati koos kohaldatavate asjakohaste kaitsemeetmetega ja muidugi arvestades kõiki muid andmekaitsetingimusi ja -piiranguid, sealhulgas eesmärgi piiramist.

2.4 Suure riskiga tehisintellektisüsteemid

2.4.1 Kolmandate isikute *ex-ante* vastavushindamise vajadus

36. Euroopa Andmekaitseõukogu ja Euroopa Andmekaitseinspektor tervitavad asjaolu, et suure riskiga tehisintellektisüsteemid peavad enne nende turulelaskmist või muul viisil ELis kasutuselevõttu läbima eelneva vastavushindamise. Põhimõtteliselt on see regulatiivne mudel teretulnud, sest see pakub innovatsioonisõbralikkuse ja põhiõiguste suure ennetava kaitse vahel head tasakaalu. Et seda saaks kasutada konkreetsetes keskkondades (nt avalikke teenuseid pakkuvate asutuste otsustusprotsessid või elutähtsad taristud), tuleb ette näha täieliku lähtekoodi uurimise viisid.
37. Euroopa Andmekaitseõukogu ja Euroopa Andmekaitseinspektor pooldavad siiski ettepaneku artiklis 43 sätestatud vastavushindamise menetluse kohandamist selliselt, et **suure riskiga tehisintellektisüsteemide jaoks tuleb üldjuhul teha kolmandate isikute *ex-ante* vastavushindamine**. Kuigi suure riskiga isikuandmete töötlemise kolmandate isikute vastavushindamine ei ole isikuandmete kaitse üldmääruses ega ELi institutsioonide, ametite, organite ja asutuste andmekaitsemääruses nõutav, ei ole tehisintellektisüsteemide riskid veel täielikult teada. Seepärast tugevdaks kolmandate isikute vastavushindamise kohustuse üldine lisamine kõigi suure riskiga tehisintellektisüsteemide õiguskindlust ja usaldust.

2.4.2 Reguleerimisala peab hõlmama ka juba kasutusel olevaid tehisintellektisüsteeme

38. Ettepaneku artikli 43 lõike 4 kohaselt tuleb suure riskiga tehisintellektisüsteemidele teha uus vastavushindamine alati, kui neid oluliselt muudetakse. On õige tagada, et tehisintellektisüsteemid vastaksid kogu elutsükli jooksul tehisintellekti määruse nõuetele. Enne kavandatava määruse kohaldamist (või 12 kuud pärast seda, kui tegemist on IX lisas loetletud suuremahuliste IT-süsteemidega) turule lastud või kasutusele võetud tehisintellektisüsteemid

jäetakse selle reguleerimisalast välja, v.a juhul, kui tehakse „oluline muudatus“ nende süsteemide projektis või sihtotstarbes (artikkel 83).

39. Siiski on „oluliste muudatuste“ lävi ebaselge. Ettepaneku põhjenduses 66 on sätestatud madalam vastavushindamise lävi: „iga kord, kui aset leiab muutus, mis võib mõjutada süsteemi vastavust käeoleva määruse nõuetele“. Samalaadne lävi oleks asjakohane artiklis 83 vähemalt suure riskiga tehisintellektisüsteemide puhul. Lisaks on kaitselünkade kõrvaldamiseks vaja, et juba loodud ja toimivad tehisintellektisüsteemid vastaksid pärast teatud rakendamisetappi samuti tehisintellekti määruse nõuetele.
40. Isikuandmete töötlemise mitmekülgsed võimalused ja välisriskid mõjutavad ka tehisintellektisüsteemide turvalisust. Artikli 83 keskendumine „olulisele muudatusele projektis või sihtotstarbes“ ei sisalda viidet väliste riskide muutustele. Ettepaneku artiklisse 83 tuleks seetõttu lisada viide välistest riskidest (nt küberrünnakud, vastaste rünnakud ja tarbijate põhjendatud kaebused) tuleneva ohustsenaariumi muutustele.
41. Kuivõrd kohaldamine algab 24 kuud pärast tulevase määruse jõustumist, ei pea Euroopa Andmekaitseinspektor ja Euroopa Andmekaitseinspektsiooni ka juba pikemat aega turul olnud tehisintellektisüsteemide erandi tegemist asjakohaseks. Kuigi ettepanekus nähakse ette, et määruse nõudeid võetakse iga suuremahulise IT-süsteemi hindamisel arvesse IX lisas loetletud õigusaktides sätestatud viisil, on Euroopa Andmekaitseinspektsiooni ja Euroopa Andmekaitseinspektor seisukohal, et tehisintellektisüsteemide kasutuselevõtu nõudeid tuleks kohaldada tulevase määruse kohaldamise kuupäevast.

2.5 Juhtimine ja Euroopa tehisintellekti nõukogu

2.5.1 Juhtimine

42. Euroopa Andmekaitseinspektsiooni ja Euroopa Andmekaitseinspektor tervitavad Euroopa Andmekaitseinspektori nimetamist liidu institutsioonide, asutuste ja organite järelevalve pädevaks asutuseks ja turujärelevalveasutuseks, kui need kuuluvad käesoleva ettepaneku reguleerimisalasse. Euroopa Andmekaitseinspektor on valmis täitma oma uut ülesannet ELi avaliku halduse tehisintellekti reguleerimisasutusena. Euroopa Andmekaitseinspektori tähtsus ja ülesandeid ei ole aga piisavalt üksikasjalikult kirjeldatud ning neid tuleks ettepanekus veelgi täpsustada, eriti mis puudutab asutuse rolli turujärelevalveasutusena.
43. Euroopa Andmekaitseinspektsiooni ja Euroopa Andmekaitseinspektor on teadlikud rahaliste vahendite eraldamisest nõukogule ja Euroopa Andmekaitseinspektorile, kes tegutseb ettepanekus teavitava asutusena. Euroopa Andmekaitseinspektorile ettenähtud uute ülesannete täitmine, olenemata sellest, kas ta tegutseb teavitatud asutusena, nõuaks aga oluliselt suuremaid rahalisi vahendeid ja inimressursse.
44. Esiteks seetõttu, et artikli 63 lõikes 6 on sätestatud, et Euroopa Andmekaitseinspektor „tegutseb turujärelevalveasutusena“ ettepaneku reguleerimisalasse kuuluvate liidu institutsioonide, asutuste ja organite jaoks, kuid selles ei selgitata, kas Euroopa Andmekaitseinspektorit tuleb täiel määral pidada „turujärelevalveasutuseks“, nagu on ette nähtud määruses (EL) 2019/1020. See tekitab küsimusi Euroopa Andmekaitseinspektori

praktiliste ülesannete ja volituste kohta. Teiseks (ja eeldusel, et esimesele küsimusele vastatakse jaatavalt) on ebaselge, kuidas suudab ELi institutsioonide, ametite, organite ja asutuste andmekaitsemääruses sätestatud Euroopa Andmekaitseinspektori ametikoht täita määruse (EL) 2019/1020 artiklis 11 sätestatud ülesannet, mis hõlmab „oma territooriumil tõhusat turujärelevalvet internetis kättesaadavaks tehtud toodete üle“ või „esindusliku valimi alusel füüsilisi või laboratoorseid kontrole“. Esineb oht, et ettepanekus täpsustamata uute ülesannete tegelemine võib ohustada tema kohustuste täitmist andmekaitseinspektorina.

45. Euroopa Andmekaitsekoostöögrupp ja Euroopa Andmekaitseinspektor rõhutavad siiski, et ettepaneku mõned sätted, milles määratletakse tehisintellekti määrusest tulenevad eri pädevate asutuste ülesanded ja volitused, nende suhted, olemus ja sõltumatuse tagatis, tunduvad praeguses etapis ebaselged. Määruses (EL) 2019/1020 on sätestatud, et turujärelevalveasutus peab olema sõltumatu, kuid määruse eelnõus ei nõuta järelevalveasutustelt sõltumatust ja isegi nõutakse, et nad esitaksid komisjonile turujärelevalveasutuste (kes võivad olla erinevad institutsioonid) täidetavate teatud ülesannete kohta aruandeid. Kuivõrd ettepanekus sätestatakse ka, et andmekaitseasutused on õiguskaitse eesmärgil kasutatavate tehisintellektisüsteemide turujärelevalveasutused (artikli 63 lõige 5), tähendab see ka seda, et neile võib kohalduda riikliku järelevalveasutuse kaudu komisjonile aruannete esitamise kohustus (artikli 63 lõige 2), mis näib olevat vastuolus nende sõltumatusega.
46. Seetõttu on Euroopa Andmekaitsekoostöögrupp ja Euroopa Andmekaitseinspektor seisukohal, et neid sätteid tuleb selgitada, et need oleksid kooskõlas määrusega (EL) 2019/1020, ELi institutsioonide, ametite, organite ja asutuste andmekaitsemäärusega ja isikuandmete kaitse üldmäärusega, ning ettepanekus tuleks selgelt sätestada, et tehisintellekti määruse kohased järelevalveasutused peavad oma ülesannete täitmisel olema täielikult sõltumatud, sest see oleks tulevase määruse nõuetekohase järelevalve ja jõustamise oluline tagatis.
47. Samuti soovivad Euroopa Andmekaitsekoostöögrupp ja Euroopa Andmekaitseinspektor meelde tuletada, et andmekaitseasutused jõustavad isikuandmeid hõlmavate tehisintellektisüsteemide valdkonnas juba isikuandmete kaitse üldmäärust, ELi institutsioonide, ametite, organite ja asutuste andmekaitsemäärust ning õiguskaitse direktiivi, et tagada põhiõiguste ja täpsemalt andmekaitse õiguse kaitse. Seetõttu on andmekaitseasutustel, nagu on ettepanekus nõutud riiklikelt järelevalveasutustelt, juba mõningad teadmised tehisintellekti tehnoloogiast, andmetest, andmetöötlusest ja põhiõigustest ning eksperditeadmised uue tehnoloogiaga kaasnevate põhiõigustega seotud riskide hindamisest. Juhtudel, kus tehisintellektisüsteemid põhinevad isikuandmete töötlemisel või töötlevad isikuandmeid, on ettepaneku sätted lisaks otseselt lõimunud andmekaitse õigusraamistikuga, mis kehtib määruse reguleerimisalasse kuuluvate enamike tehisintellektisüsteemide kohta. Seetõttu on ettepanekuga hõlmatud järelevalveasutuste ja andmekaitseasutuste pädevused omavahel seotud.
48. Seega tagaks andmekaitseasutuste määramine riiklikeks järelevalveasutusteks ühtlustatuma regulatiivse käsitluse, aitaks kaasa andmetöötlussätete järjepidevale tõlgendamisele ja väldiks vastuolusid selle jõustamisel liikmesriikides. Samuti oleks ettepaneku reguleerimisalasse kuuluvate isikuandmete töötlemise kõikides toimingutes tehisintellekti väärtusahela kõikide sidusrühmade jaoks kasulik luua ühtne kontaktpunkt ning piirata kahe erineva töötlemisega tegeleva reguleeriva (ettepaneku ja isikuandmete kaitse üldmäärusega hõlmatud) asutuse

vahelist suhtlust. Sellest tulenevalt leiavad Euroopa Andmekaitseenõukogu ja Euroopa Andmekaitseinspektor, et **andmekaitseasutused tuleks vastavalt ettepaneku artiklile 59 määrata riiklikeks järelevalveasutusteks.**

49. Igal juhul, kuivõrd ettepanek sisaldab ELi toimimise lepingu artikli 16 alusel vastu võetud erieeskirju üksikisikute kaitse kohta isikuandmete töötlemisel, peab nende eeskirjade järgimine (eeskätt avalikult juurdepääsetavates ruumides õiguskaitse kontekstis reaalses toimuva biomeetrilise kaugtuvastamise süsteemide kasutamise piirangute puhul) **olema sõltumatute asutuste kontrolli all.**
50. Ettepanekus puudub aga selgesõnaline säte, mis annaks sõltumatutele asutustele nende eeskirjade järgimise tagamise pädevuse. Ainus viide isikuandmete kaitse üldmääruses või õiguskaitse direktiivis nimetatud pädevatele andmekaitse järelevalveasutustele on ettepaneku artikli 63 lõikes 5, kuid ainult „turujärelevalveasutustena“ ja mõne muu asutuse alternatiivina. Euroopa Andmekaitseenõukogu ja Euroopa Andmekaitseinspektor leiavad, et asjade selline korraldus ei taga ELi toimimise lepingu artikli 16 lõikes 2 ja harta artiklis 8 sätestatud sõltumatu kontrolli nõude täitmist.

2.5.2 Euroopa tehisintellekti nõukoda

51. Ettepanekuga luuakse Euroopa tehisintellekti nõukoda (EAIB). Euroopa Andmekaitseenõukogu ja Euroopa Andmekaitseinspektor tunnistavad vajadust kavandatava õigusraamistiku järjepideva ja ühtlustatud kohaldamise järele, samuti ELi tehisintellekti käsitlevate õigusaktide väljatöötamisse sõltumatute ekspertide kaasamise järele. Samas nähakse ettepanekuga ette komisjoni põhiroll. Viimane ei oleks mitte ainult EAIB osa, vaid ka selle eesistuja ning tal oleks EAIB kodukorra vastuvõtmisel vetoõigus. See on vastuolus vajadusega, et Euroopa tehisintellekti nõukoda oleks igasugusest poliitilisest mõjust sõltumatu. Seetõttu leiavad Euroopa Andmekaitseenõukogu ja Euroopa Andmekaitseinspektor, et tulevane tehisintellekti määrus peaks andma **EAIB-le rohkem autonoomiat**, et võimaldada tal tagada ühtsel turul määruse järjepidev kohaldamine.
52. Euroopa Andmekaitseenõukogu ja Euroopa Andmekaitseinspektor märgivad samuti, et EAIB-le ei anta volitusi kavandatava määruse jõustamiseks. Arvestades aga tehisintellektisüsteemide levikut ühtsel turul ja piiriüleste juhtumite tõenäosust, on ühtlustatud jõustamine ja pädevuste nõuetekohane jaotamine riiklike järelevalveasutuste vahel äärmiselt oluline. Seetõttu soovivad Euroopa Andmekaitseenõukogu ja Euroopa Andmekaitseinspektor tulevases tehisintellekti määramises täpsustada riiklike järelevalveasutuste koostöömehhanisme. Euroopa Andmekaitseenõukogu ja Euroopa Andmekaitseinspektor soovivad kehtestada mehhanismi, mis garanteeriks iga tehisintellektisüsteemi jaoks ühtse kontaktpunkti nii õigusaktidest mõjutatud üksikisikutele kui ka ettevõtetele, ning organisatsioonidele, kelle tegevus hõlmab rohkem kui pooli ELi liikmesriike, võib EAIB määrata riikliku asutuse, kes vastutab asjakohase tehisintellektisüsteemiga seoses tehisintellekti määruse jõustamise eest.

53. Võttes arvesse nõukoda moodustavate asutuste sõltumatust, on nõukojal lisaks õigus tegutseda omal algatusel, mitte ainult pakkuda komisjonile nõu ja abi. Seepärast rõhutavad Euroopa Andmekaitseinspektoori ja Euroopa Andmekaitseinspektor vajadust laiendada nõukojale määratud ülesannet nii, et see ei kattuks ettepanekus loetletud ülesannetega.
54. Nende eesmärkide saavutamiseks **peavad EAIB-l olema piisavad ja asjakohased volitused** ning nõukoja õiguslikku seisundit tuleks selgitada. Et tulevase määruse sisuline kohaldamisala oleks jätkuvalt asjakohane, tundub eelkõige vajalik kaasata selle väljatöötamise määruse kohaldamise eest vastutavad ametiasutused. Seetõttu soovivad Euroopa Andmekaitseinspektoori ja Euroopa Andmekaitseinspektor anda EAIB-le volitused teha komisjonile I lisa (milles määratletakse tehisintellekti tehnoloogiad ja käsitlused) ja III lisa (milles on loetletud artikli 6 lõikes 2 osutatud suure riskiga tehisintellektisüsteemid) kohta muutmissettepanekuid. Enne nende lisade muutmist peaks komisjon ka EAIB-ga konsulteerima.
55. Ettepaneku artikli 57 lõikega 4 nähakse ette teabevahetus nõukoja ja muude liidu organite, asutuste, ametite ja nõuanderühmade vahel. Võttes arvesse nende varasemat tööd tehisintellekti valdkonnas ja inimõiguste alaseid teadmisi, soovivad Euroopa Andmekaitseinspektoori ja Euroopa Andmekaitseinspektor kaaluda põhiõiguste ameti määramist nõukoja üheks vaatlejaks.

3 KOOSTOIME ANDMEKAITSE ÕIGUSRAAMISTIKUGA

3.1 Ettepaneku koostoime ELi kehtivate andmekaitse õigusaktidega

56. Selgelt määratletud seos ettepaneku ja kehtivate andmekaitsealaste õigusaktide vahel on oluline eeltingimus, et tagada isikuandmete kaitse valdkonnas ELi õigustiku järgimine ja kohaldamine (ja see säilitada). Selliseid ELi õigusakte (eelkõige isikuandmete kaitse üldmäärust, ELi institutsioonide, ametite, organite ja asutuste andmekaitsemäärust ning õiguskaitse direktiivi) tuleb pidada eelduseks, millele võivad tugineda edasised seadusandlikud ettepanekud, ilma et see mõjutaks või segaks kehtivaid sätteid, sealhulgas kui see puudutab järelevalveasutuste pädevust ja juhtimist.
57. Euroopa Andmekaitseinspektoori ja Euroopa Andmekaitseinspektori arvates on seetõttu oluline ettepanekus selgelt vältida mis tahes järjepidevusetust ja võimalikke vastuolusid isikuandmete kaitse üldmääruse, ELi institutsioonide, ametite, organite ja asutuste andmekaitsemääruse ning õiguskaitse direktiiviga. Seda mitte ainult õiguskindluse tagamiseks, vaid ka selleks, et vältida ettepaneku otsest või kaudset ohtu ELi toimimise lepingu artiklis 16 ja harta artiklis 8 sätestatud isikuandmete kaitse põhiõigusele.
58. Iseõppivad masinad saavad füüsiliste isikute isikuandmeid kaitsta ainult siis, kui see on kontseptsiooni integreeritud. Samuti on hädavajalik kohene võimalus kasutada isikuandmete kaitse üldmääruse artikli 22 (automatiseeritud töötlusel põhinevate üksikotsuste tegemine, sealhulgas profiilialüüs) või ELi institutsioonide, ametite, organite ja asutuste andmekaitsemääruse artikli 23 kohaseid õigusi, olenemata töötlemise eesmärkidest. Seepärast tuleb tehisintellektisüsteemides algusest peale sätestada muud andmesubjektide õigused, mis

on seotud andmekaitse õigusaktidele vastava kustutamise- ja parandusõigusega, olenemata valitud tehisintellekti käsitlesest või tehnilisest ülesehitusest.

59. Isikuandmete kasutamine tehisintellektisüsteemide õpetamiseks võib viia tehisintellektisüsteemi kallutatud otsustusmustrite loomiseni. Seega tuleks sellistes protsessides nõuda mitmesuguseid kaitsemeetmeid ja eelkõige kvalifitseeritud inimjärelevalvet, et tagada andmesubjektide õiguste austamine ja tagamine ning vältida igasugust negatiivset mõju üksikisikutele. Pädevatel asutustel peaks olema ka võimalus esitada suuniseid, et hinnata tehisintellektisüsteemide eelarvamusi ja toetada inimjärelevalvet.
60. Kui nende andmeid kasutatakse tehisintellekti koolitamiseks ja/või prognoosideks, tuleks andmesubjekte alati teavitada õiguslikust alusest ning tehisintellektisüsteemi loogikat (menetlust) ja ulatust üldiselt kirjeldada. Seetõttu tuleks neil juhtudel alati tagada üksikisikute õigus töötlemist piirata (isikuandmete kaitse üldmääruse artikkel 18 ja ELi institutsioonide, ametite, organite ja asutuste andmekaitsemääruse artikkel 20) ning andmeid kustutada/eemaldada (isikuandmete kaitse üldmääruse artikkel 16 ja ELi institutsioonide, ametite, organite ja asutuste andmekaitsemääruse artikkel 19). Lisaks peaks vastutaval töötlejal olema selgesõnaline kohustus teavitada andmesubjekti vastuväidete esitamise, piiramise, andmete kustutamise jms tähtaegadest. Tehisintellektisüsteem peab suutma piisavate tehniliste ja korralduslike meetmete abil täita kõiki andmekaitseenõudeid. Õigus selgitustele peaks tagama täiendava läbipaistvuse.

3.2 Testkeskkond ja täiendav töötlemine (ettepaneku artiklid 53 ja 54)

61. Olemasolevaid õiguslikke ja moraalseid piire arvesse võttes on oluline edendada Euroopa innovatsiooni, kasutades selliseid vahendeid nagu testkeskkond. Testkeskkond annab võimaluse tagada kaitsemeetmed, mis on tehisintellektisüsteemide usaldusväärsuse ja töökindluse loomiseks vajalikud. Keerulises keskkonnas võib tehisintellekti katsetajatel olla raske kõiki huve nõuetekohaselt kaaluda. Reguleeritud testkeskkonnas tegutsemine võib eriti piiratud ressursidega väikeste ja keskmise suurusega ettevõtete puhul anda kiiremat teavet ja seega soodustada innovatsiooni.
62. Ettepaneku artikli 53 lõikes 3 on sätestatud, et testkeskkond ei mõjuta järelevalve- ega parandusvolitusi. Kui see selgitus on kasulik, on vaja koostada ka suunised või juhised, kuidas saavutada hea tasakaal ühelt poolt järelevalveasutusena tegutsemise ja teisalt testkeskkonna kaudu üksikasjaliku juhendamise vahel.
63. Artikli 53 lõikes 6 kirjeldatakse, et testkeskkondade töökord ja -tingimused sätestatakse rakendusaktides. Oluline on koostada konkreetsed suunised, et testkeskkondade loomisel ja kasutamisel tagada järjepidevus ja toetus. Siduvad rakendusaktid võivad aga piirata iga liikmesriigi võimalust kohandada testkeskkonda oma vajadustele ja kohalikele tavadele. Seega soovivad Euroopa Andmekaitseõukogu ja Euroopa Andmekaitseinspektor EAIB-l tagada testkeskkondade suunised.

64. Ettepaneku artikli 54 eesmärk on luua tehisintellekti reguleeritud testkeskkonnas avalikes huvides teatud tehisintellektisüsteemide arendamiseks isikuandmete täiendava töötlemise õiguslik alus. Ettepaneku artikli 54 lõike 1 seos ettepaneku artikli 54 lõikega 2 ja põhjendusega 41 ning seega ka kehtivate ELi andmekaitsealaste õigusaktidega on jätkuvalt ebaselge. Isikuandmete kaitse üldmääruses ja ELi institutsioonide, ametite, organite ja asutuste andmekaitsemääruses on aga „täiendava töötlemise“ alus juba loodud. Eriti nende juhtumite kontekstis, kus täiendava töötlemise lubamine on avalikes huvides, ei pea vastutava töötleja ja andmesubjekti huvide tasakaalustamine takistama innovatsiooni. Praegu ei käsitle ettepaneku artikkel 54 kahte olulist küsimust: i) mis asjaoludel, milliste (lisa-) kriteeriumide alusel kaalutakse andmesubjektide huve ja ii) kas neid tehisintellektisüsteeme kasutatakse ainult testkeskkonnas. Euroopa Andmekaitsekoostöögrupi ja Euroopa Andmekaitseinspektor tervitavad liidu või liikmesriigi õigusaktide kohaldamise nõuet õiguskaitse direktiivi alusel testkeskkonnas kogutud isikuandmete töötlemiseks, kuid soovivad kavandatavat eesmärki täpsustada viisil, mis on kooskõlas isikuandmete kaitse üldmääruse ja ELi institutsioonide, ametite, organite ja asutuste andmekaitsemäärusega, peamiselt selgitades, et selliste testkeskkondade õiguslik alus peaks vastama isikuandmete kaitse üldmääruse artikli 23 lõikes 2 ja ELi institutsioonide, ametite, organite ja asutuste andmekaitsemääruse artiklis 25 sätestatud nõuetele, ja täpsustades, et testkeskkonna iga kasutus tuleb põhjalikult hinnata. See kehtib ka artikli 54 lõike 1 punktides b–j esitatud tingimuste täieliku loetelu kohta.
65. Ettepaneku artiklis 54 esitatud andmete taaskasutamisega seotud lisakaalutlused näitavad, et testkeskkonna kasutamine on ressursimahukas ja seetõttu on realistlik eeldada, et ainult väike osa ettevõtetest saavad võimaluse selles osaleda. Testkeskkonnas osalemine võib olla konkurentsieelis. Andmete taaskasutamise lubamiseks oleks vaja hoolikalt kaaluda, kuidas osalejaid valida, et tagada nende reguleerimisalasse kuulumine ja vältida ebaõiglast kohtlemist. Euroopa Andmekaitsekoostöögrupi ja Euroopa Andmekaitseinspektor on mures, et andmete taaskasutamise võimaldamine testkeskkonnas erineb isikuandmete kaitse üldmääruse vastutusmeetodist, kus vastutus lasub vastutaval töötlejal, mitte pädeval asutusel.
66. Lisaks leiavad Euroopa Andmekaitsekoostöögrupi ja Euroopa Andmekaitseinspektor, et arvestades testkeskkonna eesmärke, milleks on tehisintellektisüsteemide väljatöötamine, katsetamine ja valideerimine, ei saa testkeskkonnad kuuluda õiguskaitse direktiivi reguleerimisalasse. Kuigi õiguskaitse direktiivis nähakse ette andmete taaskasutamist teadusuuringute jaoks, kohaldatakse teiseseks otstarbeks töödeldud andmetele isikuandmete kaitse üldmäärust või ELi institutsioonide, ametite, organite ja asutuste andmekaitsemäärust, mitte enam õiguskaitse direktiivi.
67. Pole selge, mida reguleeritud testkeskkond hõlmab. Tekib küsimus, kas kavandatav reguleeritud testkeskkond hõlmab igas liikmesriigis IT-taristut koos edasise töötlemise täiendavate õiguslike alustega või pakub lihtsalt juurdepääsu regulatiivsetele teadmistele ja juhistele. Euroopa Andmekaitsekoostöögrupi ja Euroopa Andmekaitseinspektor kutsuvad seadusandjat üles ettepanekus seda kontseptsiooni täpsustama ja selgelt märkima, et reguleeritud testkeskkond ei tähenda pädevate asutuste kohustust pakkuda oma tehnilist taristut. Igal juhul tuleb vastavalt sellisele selgitusele tagada pädevatele asutustele rahalised vahendid ja inimressursid.

68. Viimasena soovivad Euroopa Andmekaitseinspektor ja Euroopa Andmekaitseinspektor rõhutada piiriüleste tehisintellektisüsteemide arendamist ja et need tehakse tervikuna kättesaadavaks Euroopa digitaalsel ühtsel turul. Selliste tehisintellektisüsteemide puhul ei tohiks reguleeritud testkeskkond kui innovatsioonivahend saada piiriülese arengu takistuseks. Seetõttu soovitavad Euroopa Andmekaitseinspektor ja Euroopa Andmekaitseinspektor kooskõlastatud piiriülest käsitlust, mis on riiklikul tasandil kõigile VKEdele veel piisaval määral kättesaadav, pakkudes ühtset raamistikku kogu Euroopas, ilma et see oleks liiga piirav. Tuleb leida tasakaal Euroopa koordineerimise ja riiklike menetluste vahel, et vältida tulevase tehisintellekti määruse vastuolulist rakendamist, mis takistaks ELi-ülest innovatsiooni.

3.3 Läbipaistvus

69. Euroopa Andmekaitseinspektor ja Euroopa Andmekaitseinspektor tervitavad asjaolu, et suure riskiga tehisintellektisüsteemid registreeritakse avalikus andmebaasis (viidatud ettepaneku artiklites 51 ja 60). Seda andmebaasi tuleks kasutada kui võimalust anda üldsusele teavet tehisintellektisüsteemi rakendusala, selle toimimist kahjustada võivatest teadaolevatest puudustest ja juhtumitest ning teenusepakkujate poolt nende lahendamiseks ja parandamiseks võetud abinõudest.
70. Demokraatia aluspõhimõte on kontrolli- ja tasakaalusüsteemi kasutamine. Seetõttu on asjaolu, et kuritegude avastamiseks, ennetamiseks, uurimiseks või nende eest vastutusele võtmiseks kasutatavate tehisintellektisüsteemide suhtes ei kehti läbipaistvuskohustus, liiga lai erand. Tuleb eristada tuvastamise või ennetamise tehisintellektisüsteemi ja kuritegude eest vastutusele võtmiseks kasutatavaid tehisintellektisüsteemi. Ennetamise ja tuvastamise kaitsemeetmed peavad olema süütuse presumptsiooni tõttu tugevamad. Lisaks avaldavad Euroopa Andmekaitseinspektor ja Euroopa Andmekaitseinspektor kahetsust, et ettepanekus ei ole esitatud hoiatusi, mida võib tõlgendada kui luba kasutada kontrollimata ja suure riskiga tehisintellektisüsteemi või rakendusi.
71. Isegi hästi toimivas demokraatias peaks juhtudel, mil avalikkusele saab salajasuse tõttu pakkuda läbipaistvust vähe või üldse mitte, olema kehtestatud kaitsemeetmed. Vastavad tehisintellektisüsteemid tuleks registreerida pädevas järelevalveasutuses ja tagada läbipaistvus.
72. Tehisintellektisüsteemide läbipaistvuse tagamine on väga keeruline eesmärk. Paljude tehisintellektisüsteemide täielikult kvantitatiivne otsustusmeetod, mis erineb olemuslikult enamasti põhjuslikul ja teoreetilisel mõttekäigul rajanevast inimlikust käsitlusest, võib olla vastuolus vajadusega saada arusaadav selgitus masina töö eeldatavate tulemuste kohta. Määrus peaks edendama uusi, aktiivsemaid ja õigeaegsemaid viise, kuidas teavitada tehisintellektisüsteemide kasutajaid süsteemi (otsuste tegemise) olekust mis tahes ajahetkel ning anda varajane hoiatus võimalike kahjulike tagajärgede kohta, et üksikisikud, kelle õigusi ja vabadusi võivad masina autonoomsed otsused kahjustada, saaksid reageerida või otsuse vaidlustada.

3.4 Andmete eriliikide ja kuritegudega seotud andmete töötlemine

73. Andmete eriliikide töötlemist õiguskaitse valdkonnas reguleeritakse ELi andmekaitse õigusraamistiku sätetega, sealhulgas õiguskaitse direktiivi ja selle riiklike rakendusaktidega. Ettepanekus väidetakse, et see ei paku isikuandmete, sealhulgas isikuandmete eriliikide töötlemise üldist õiguslikku alust (vt põhjendus 41). Samas on ettepaneku artikli 10 lõikes 5 sätestatud, et „selliste süsteemide pakkujad võivad töödelda isikuandmete eriliike”. Lisaks nõutakse samas sättes täiendavaid kaitsemeetmeid, esitades ka vastavaid näiteid. Seega näib, et ettepanek sekkub isikuandmete kaitse üldmääruse, õiguskaitse direktiivi ning ELi institutsioonide, ametite, organite ja asutuste andmekaitsemääruse kohaldamisse. Kuigi Euroopa Andmekaitse nõukogu ja Euroopa Andmekaitseinspektor tervitavad püüet kehtestada piisavad kaitsemeetmed, on vaja ühtsemat regulatiivset käsitlust, sest praegused sätted ei tundu olevat piisavalt selged, et luua andmete eriliikide töötlemise õiguslik alus, ning neid tuleb täiendada kaitsemeetmetega, mida tuleb veel hinnata. Kui isikuandmeid on kogutud õiguskaitse direktiivi ulatusse kuuluva töötlemise teel, tuleb arvesse võtta ka võimalikke täiendavaid kaitsemeetmeid ja piiranguid, mis tulenevad õiguskaitse direktiivi ülevõtvatest riiklikest õigusaktidest.

3.5 Vastavusmehhanismid

3.5.1 Sertifitseerimine

74. Ettepaneku üks põhisambaid on sertifitseerimine. Ettepanekus kirjeldatud sertifitseerimissüsteem põhineb üksuste struktuuril (teavitavad asutused/teavitatud asutused/komisjon) ja vastavushindamis-/sertifitseerimismehhanismil, mis hõlmab suure riskiga tehisintellektisüsteemidele kehtivaid kohustuslikke nõudeid, ning tugineb määrusel (EL) nr 1025/2012 põhinevatel ühtlustatud Euroopa standarditel ja komisjoni kehtestatud ühistel tehnilistel kirjeldustel. See mehhanism erineb sertifitseerimissüsteemist, mille eesmärk on tagada andmekaitse eeskirjade ja põhimõtete järgimine, nagu on sätestatud isikuandmete kaitse üldmääruse artiklites 42 ja 43. Siiski ei ole selge, kuidas teavitatud asutuste (ettepaneku kohaselt väljastatud) sertifikaadid suhestuvad isikuandmete kaitse üldmääruses sätestatud andmekaitse sertifikaatide, -pitsrite ja -märgistega, erinevalt teiste sertifikaatide kohta sätestatust (vt artikli 42 lõige 2 määruse (EL) 2019/881 alusel väljastatud sertifikaatide kohta).

75. Kui suure riskiga tehisintellektisüsteemid põhinevad isikuandmete töötlemisel või töötlevad isikuandmeid oma ülesannete täitmiseks, võivad nimetatud kõrvalekalded tekitada kõikidele asjaomastele asutustele õiguslikku ebakindlust, sest võivad põhjustada olukordi, mil ettepaneku alusel sertifitseeritud ja CE-vastavusmärgisega märgistatud (turule lastud või kasutusele võetud) tehisintellektisüsteeme võidakse kasutada viisil, mis ei ole kooskõlas andmekaitse eeskirjade ja põhimõtetega.

76. Ettepanekul puudub selge seos andmekaitse õigusaktide ning ELi ja liikmesriikide muude õigusaktidega, mida kohaldatakse III lisas loetletud suure riskiga tehisintellektisüsteemide eri valdkondade suhtes. Eelkõige peaks ettepanek sisaldama võimalikult väheste andmete kogumise ja lõimitud andmekaitse põhimõtteid kui üht aspekti, mida tuleb enne CE-vastavusmärgise saamist arvesse võtta, arvestades suure riskiga tehisintellektisüsteemide võimalikku suurt

sekkumist eraelu puutumatus ja isikuandmete kaitse põhiõigustesse ning vajadust tagada tehisintellektisüsteemide vastu suur usaldustase. Seetõttu soovivad Euroopa Andmekaitseinspektor ja Euroopa Andmekaitseinspektor ettepanekut muuta, et selgitada seost nimetatud määruse alusel väljastatud sertifikaatide ning andmekaitseinspektorite, -pitserite ja -märgiste vahel. Andmekaitseasutused peaksid osalema ühtlustatud standardite ja ühtsete tehniliste kirjelduste koostamisel ja kehtestamisel.

77. Vastavushindamist käsitleva ettepaneku artikli 43 kontekstis näib artiklis 47 sätestatud vastavushindamise erand olevat väga lai, hõlmates liiga palju erandeid (nt avaliku julgeoleku erakorralised põhjused või inimeste elu ja tervise kaitse, keskkonnakaitse ning peamiste tööstus- ja taristuvarade kaitse). Teeme seadusandjatele ettepaneku seda kitsendada.

3.5.2 Toimimisjuhendid

78. Ettepaneku artikli 69 kohaselt edendavad komisjon ja liikmesriigid selliste toimimisjuhendite koostamist, mille eesmärk on soodustada ja hõlbustada suure riskiga tehisintellektisüsteemidele kohaldatavate nõuete vabatahtlikku kohaldamist tehisintellektisüsteemide suhtes, mis ei ole suure riskiga tehisintellektisüsteemid, ja lisanõuete kohaldamist. Kooskõlas isikuandmete kaitse üldmääruse põhjendusega 78 soovivad Euroopa Andmekaitseinspektor ja Euroopa Andmekaitseinspektor teha kindlaks ja määratleda sünergia nende instrumentide ja isikuandmete kaitse üldmääruses sätestatud toimimisjuhendite vahel, mis toetavad andmekaitse järgimist. Selles kontekstis on asjakohane selgitada, kas isikuandmete kaitset tuleb pidada „lisanõueteks“, mida artikli 69 lõikes 2 osutatud toimimisjuhendites võib käsitleda. Samuti on oluline tagada, et artikli 69 lõikes 1 osutatud toimimisjuhendites käsitletavat „tehnilised kirjeldused ja lahendused“, mille eesmärk on soodustada tehisintellekti määruse eelnõu nõuete kohaldamist, ei oleks vastuolus isikuandmete kaitse üldmääruse ning ELi institutsioonide, ametite, organite ja asutuste andmekaitsemääruse eeskirjade ja põhimõtetega. See annaks nende vahendite järgimisele mitte suure riskiga tehisintellektisüsteemide pakkujate poolt (kuivõrd sellised süsteemid põhinevad isikuandmete töötlemisel või isikuandmete töötlemisel oma ülesande täitmiseks) lisaväärtust, sest tagab, et vastutavad ja volitatud töötajad suudavad nende süsteemide kasutamisel oma andmekaitsekohustusi täita.
79. Samal ajal täiendaks toimimisjuhendite lõimimine ka usaldusväärse tehisintellekti õigusraamistikku, suurendades usaldust sellise tehnoloogia kasutamise vastu ohutul ja seaduskuulekal (sealhulgas põhiõigusi austaval) viisil. Nende vahendite ülesehitust tuleks aga tugevdada, kavandades mehhanismid, mis aitavad kontrollida, kas sellised juhendid pakuvad tõhusaid „tehnilisi spetsifikatsioone ja lahendusi“, ning sätestades „selged eesmärgid ja peamised tulemusnäitajad nende eesmärkide saavutamise mõõtmiseks“ juhendite lahutamatu osana. Lisaks puudub viide toimimisjuhendite (kohustuslikule) jälgimismehhanismile, mis aitaks kontrollida, kas mitte suure riskiga tehisintellektisüsteemide pakkujad järgivad nende sätteid. Samuti võib üksikute pakkujate võimalus selliseid juhendeid koostada (ja rakendada) (vt seletuskirja punkt 5.2.7) nende instrumentide tõhusust ja jõustatavust veelgi nõrgendada.

80. Lõpetuseks paluvad Euroopa Andmekaitse nõukogu ja Euroopa Andmekaitseinspektor selgitusi algatuste liikide kohta, mida komisjon võib vastavalt ettepaneku põhjendusele 81 välja töötada, „et aidata vähendada tehnilisi tõkkeid, mis takistavad tehisintellekti arendamise jaoks toimuvat piiriülest andmevahetust”.

4 JÄRELDUSED

81. Kuigi Euroopa Andmekaitseenõukogu ja Euroopa Andmekaitseinspektor tervitavad komisjoni ettepanekut ja leiavad, et selline määrus on ELi kodanike ja elanike põhiõiguste tagamiseks vajalik, leiavad nad, et ettepanekut tuleks selle kohaldatavuse ja tõhususe tagamiseks mitmes küsimuses kohandada.
82. Arvestades ettepaneku keerukust ja käsitletavaid probleeme, tuleb teha veel palju tööd, kuni ettepanekuga on loodud hästi toimiv õigusraamistik, mis täiendaks tõhusalt isikuandmete kaitse üldmäärust põhiliste inimõiguste kaitsmisel ja edendaks samas innovatsiooni. Euroopa Andmekaitseenõukogu ja Euroopa Andmekaitseinspektor on jätkuvalt kättesaadavad, et sel teel oma tuge pakkuda.

Brüssel, 18. juuni 2021

Euroopa Andmekaitseenõukogu nimel

Eesistuja

Andrea JELINEK

Euroopa Andmekaitseinspektori nimel

inspektor

Wojciech Rafał WIEWIÓROWSKI