ELi uus tehisintellekti määrus keelab inimeste põhiõigusi selgelt ohustavad süsteemid

2 aastat tagasi - 11.12.2023 Autor: AM

Euroopa Parlament ja nõukogu saavutasid reedel poliitilise kokkuleppe tehisintellekti määruse suhtes, mille kohta komisjon tegi ettepaneku 2021. aasta aprillis.

Euroopa Komisjoni president Ursula von der Leyen ütles: „Tehisintellekt juba muudab meie igapäevaelu. See on alles algus. Tehisintellekti arukas ja laialdane kasutamine võib tuua meie majandusele ja ühiskonnale tohutut kasu. Seepärast on mul väga hea meel Euroopa Parlamendi ja nõukogu poliitilise kokkuleppe üle. ELi tehisintellekti reguleeriv õigusakt on esimene terviklik tehisintellekti käsitlev õigusraamistik kogu maailmas. Seega on see ajalooline hetk. Tehisintellekti määrus viib Euroopa väärtused üle uude ajastusse ning aitab edendada vastutustundlikku innovatsiooni Euroopas. See tagab inimeste ja ettevõtjate ohutuse ja põhiõigused ning toetab seega usaldusväärse tehisintellekti arendamist ja kasutuselevõttu ELis. Määrus on oluline samm inimkeskse tehisintellekti ülemaailmsete reeglite ja põhimõtete väljatöötamisel.“

Uued reeglid lähtuvad riskidest

Reeglid on riskipõhised ja neid kohaldatakse kõigis liikmesriikides otse ja ühetaoliselt.

Valdav osa tehisintellektisüsteeme kuulub minimaalse riski kategooriasse. Minimaalse riskiga rakendusi, nagu tehisintellektil põhinevad soovitussüsteemid või rämpspostifiltrid, uued reeglid ei puuduta, kuna need süsteemid ei kujuta endast inimeste õigustele või ohutusele mingit ohtu või on see oht minimaalne. Küll aga võivad ettevõtjad vabatahtlikult kehtestada selliste rakenduste jaoks täiendavaid käitumisjuhiseid.

Suure riskiga tehisintellektisüsteemid peavad vastama rangetele nõuetele. Neil peavad olema süsteemid riskide maandamiseks, andmekogumid peavad olema kvaliteetsed, tegevust tuleb logida, dokumentatsioon peab olema üksikasjalik ja kasutajateave selge, tagatud peab olema inimjärelevalve ning kõrgel tasemel töökindlus, täpsus ja küberturvalisus. Suure riskiga tehisintellektisüsteemide hulka kuuluvad näiteks vee-, gaasi- ja elektritaristu; meditsiiniseadmed;

süsteemid, millega määratakse kindlaks juurdepääs haridusasutustele või mida kasutatakse inimeste värbamiseks; samuti süsteemid, mida kasutatakse õiguskaitse, piirikontrolli, kohtu ja demokraatlike protsesside valdkonnas. Suure riskiga süsteemideks peetakse ka biomeetrilise tuvastamise, kategoriseerimise ja emotsioonide tuvastamise süsteeme.

Tehisintellektisüsteemid, millega seotud riskid on vastuvõetamatud ning mida peetakse selgeks ohuks inimeste põhiõigustele, keelatakse.

Need on süsteemid või rakendused, mis manipuleerivad inimeste käitumisega, et mõjutada kasutaja vaba tahet. Siia kuuluvad näiteks kõnelevad mänguasjad, mis võivad soodustada alaealiste ohtlikku käitumist või süsteemid, mis võimaldavad valitsustel või ettevõtetel anda inimestele nn sotsiaalseid punkte ning teatavad ennetavaks politseitegevuseks kasutatavad rakendused. Lisaks keelatakse teatavad biomeetrilised süsteemid, näiteks töökohal kasutatavad emotsioonituvastussüsteemid, teatavad inimeste kategoriseerimise süsteemid ja õiguskaitse eesmärgil avalikus kohas kasutatavad reaalajas biomeetrilise kaugtuvastamise süsteemid (väikeste eranditega).

Läbipaistvusega seotud risk

Juturobotite ja muude sarnaste tehisintellektisüsteemide puhul peab kasutajal olema selge, et ta suhtleb masinaga. Süvavõltsingud ja muu tehisintellekti loodud sisu tuleb vastavalt märgistada ning biomeetriliste kategoriseerimis- või emotsioonituvastussüsteemide kasutamisest tuleb kasutajaid teavitada. Lisaks tuleb süsteeme kavandada nii, et sünteetiline audio-, video-, teksti- ja kujutiste sisu on märgistatud masinloetavas vormingus ning on võimalik tuvastada, et see on kunstlikult loodud või manipuleeritud sisu.

Reeglite rikkumise korral on ette nähtud trahv. Keelatud rakendustega seotud rikkumiste puhul on trahv 35 miljonit eurot või 7% ettevõtte ülemaailmsest aastakäibest (olenevalt sellest, kumb on suurem), muude nõuete rikkumise eest 15 miljonit eurot või 3% ning ebaõige teabe esitamise eest 7,5 miljonit eurot või 1,5 %. VKEdele ja idufirmadele on ette nähtud proportsionaalsemad trahvimäärad.

Üldkasutavad tehisintellektisüsteemid

Tehisintellekti määrusega kehtestatakse üldkasutatava tehisintellekti jaoks erinormid, mis tagavad läbipaistvuse kogu väärtusahelas. Väga võimsate mudelite puhul, mis võivad põhjustada süsteemseid riske, kehtestatakse siduvad

lisakohustused seoses riskide juhtimise ja ohtlike intsidentide jälgimise, mudeli hindamise ja stressitestimisega. Neid kohustusi hakatakse rakendama tegevusjuhiste kaudu, mille töötavad välja ettevõtjad, teadlased, kodanikuühiskond ja muud sidusrühmad koos komisjoniga.

Määruse rakendamise üle hakkavad riiklikku järelevalvet tegema pädevad turujärelevalveasutused. Euroopa tasandil koordineerimiseks loob Euroopa Komisjon Euroopa tehisintellekti ameti, mis hakkab jälgima ka üldkasutatavaid tehisintellektimudeleid käsitlevate normide rakendamist ja jõustamist.

Järgmised sammud

Euroopa Parlament ja nõukogu peavad poliitilise kokkuleppe nüüd ametlikult heaks kiitma. Seejärel avaldatakse see Euroopa Liidu Teatajas ning määrus jõustub 20 päeva pärast avaldamist. Määrust hakataks kohaldama kaks aastat pärast selle jõustumist, v.a keelud, mida hakatakse kohaldama juba kuue kuu möödumisel ja üldkasutatava tehisintellekti eeskirjad, mida hakatakse kohaldama 12 kuu pärast. Määruse kohaldamisele eelneval üleminekuperioodil on tehisintellekti arendajatel Euroopast ja kogu maailmast võimalus ühineda komisjoni algatatud tehisintellekti paktiga, et hakata määruse nõudeid vabatahtlikult täitma juba enne nende kohaldamise algust.

Pilt