

Brüssel, 23. aprill 2021
(OR. en)

Institutsioonidevaheline
dokument:
2021/0106(COD)

8115/21
ADD 4

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

SAATEMÄRKUSED

Saatja:	Euroopa Komisjoni peasekretär, allkirjastanud Martine DEPREZ, direktor
Kättesaamise kuupäev:	22. aprill 2021
Saaja:	Jeppe TRANHOLM-MIKKELSEN, Euroopa Liidu Nõukogu peasekretär
Komisjoni dok nr:	SWD(2021) 85 final
Teema:	KOMISJONI TALITUSTE TÖÖDOKUMENT MÕJU HINDAMISE ARUANDE KOMMENTEERITUD KOKKUVÕTE <i>Lisatud dokumendile:</i> Ettepanek: EUROOPA PARLAMENDI JA NÕUKOGU MÄÄRUS, MILLEGA NÄHAKSE ETTE TEHISINTELLEKTI KÄSITLEVAD ÜHTLUSTATUD ÕIGUSNORMID (TEHISINTELLEKTI KÄSITLEV ÕIGUSAKT) JA MUUDETAKSE TEATAVAID LIIDU ÕIGUSAKTE

Käesolevaga edastatakse delegatsioonidele dokument SWD(2021) 85 final.

Lisatud: SWD(2021) 85 final



EUROOPA
KOMISJON

Brüssel, 21.4.2021
SWD(2021) 85 final

KOMISJONI TALITUSTE TÖÖDOKUMENT
MÕJU HINDAMISE ARUANDE KOMMENTEERITUD KOKKUVÕTE

Lisatud dokumendile:

Ettepanek: EUROOPA PARLAMENDI JA NÕUKOGU MÄÄRUS,
MILLEGA NÄHAKSE ETTE TEHISINTELLEKTI KÄSITLEVAD ÜHTLUSTATUD
ÕIGUSNORMID (TEHISINTELLEKTI KÄSITLEV ÕIGUSAKT) JA MUUDETAKSE
TEATAVAID LIIDU ÕIGUSAKTE

{COM(2021) 206 final} - {SEC(2021) 167 final} - {SWD(2021) 84 final}

Kommenteeritud kokkuvõte
Mõjuhinnang tehisintellekti reguleeriva raamistiku kohta
A. Vajadus meetmete järele
Mis on probleem ja miks on tegemist ELi tasandi probleemiga?
Tehisintellekt on kujunemisjärgus üldotstarbeline tehnoloogia ehk äärmiselt võimas kogum programmeerimismeetodeid. Tehisintellektisüsteemide kasutuselevõtul on tugev potentsiaal luua sotsiaalseid hüvesid ja majanduskasvu ning suurendada ELi innovatsiooni ja konkurentsivõimet maailmas. Teatavatel juhtudel võib tehisintellektisüsteemide kasutamine tekitada siiski probleeme. Teatavate tehisintellektisüsteemide eriomadused võivad põhjustada uusi riske seoses 1) ohutuse ja turvalisusega ning 2) põhiõigustega, ja süvendada olemasolevate riskide realiseerumise tõenäosust või intensiivsust. Lisaks muudavad tehisintellektisüsteemid 3) õiguskaitseasutustele keeruliseks kehtivate eeskirjade täitmise kontrollimise ja tagamise. Need küsimused toovad omakorda kaasa 4) õigusliku ebakindluse ettevõtjate jaoks, 5) tehisintellektitehnoloogia potentsiaalselt aeglasema kasutuselevõtu ettevõtjate ja kodanike usalduse puudumise tõttu ning 6) riikide ametiasutuste regulatsiooni, et leevendada võimalikku välismõju, mis võib killustada siseturgu.
Mida tuleks saavutada?
Reguleeriva raamistiku eesmärk on lahendada need probleemid, luues tingimused usaldusväärse tehisintellekti arenguks ja kasutamiseks liidus, et tagada ühtse turu nõuetekohane toimimine. Erieesmärgid on: 1) tagada, et turule lastavad ja kasutatavad tehisintellektisüsteemid on turvalised ja kooskõlas kehtiva põhiõigusi käsitleva õigusega ning liidu väärtustega; 2) tagada õiguskindlus tehisintellektialaste investeringute ja innovatsiooni soodustamiseks; 3) tugevdada valitsemistava ja tõhustada põhiõigusi käsitleva kehtiva õiguse ja tehisintellektisüsteemidele kohalduvate ohutusnõuete täitmise tagamist ning 4) hõlbustada seaduslike, ohutute ja usaldusväärsete tehisintellektisüsteemide ühtse turu väljatöötamist ja vältida turu killustumist.
Milline on ELi tasandi meetmete lisaväärtus (subsidiiaarsus)?
Kuna suuremahulised andmed ja andmestikud, millele tehisintellektisüsteemid sageli tuginevad, on piiriülesed, ei suuda liikmesriigid üksi algatuse eesmärgi tõhusalt täita. Usaldusväärset tehisintellekti reguleeriva Euroopa raamistikuga soovitakse kehtestada liidus ühtsed õigusnormid tehisintellektitehnoloogiat või eraldiseisvaid tehisintellektirakendusi kasutavate toodete ja teenuste arendamise, turule laskmise ja kasutamise kohta. Selle eesmärk on tagada võrdsed võimalused ja kaitsta kõiki Euroopa Liidu kodanikke, tugevdades ühtlasi Euroopa tehisintellekti valdkonna konkurentsivõimet ja tööstusbaasi. ELi meetmed tehisintellekti valdkonnas hoogustavad siseturgu ja võivad anda Euroopa tööstusele maailmas märkimisväärse konkurentsieelise tulenevalt mastaabisäästust, mida liikmesriigid ei suuda üksi saavutada.
B. Lahendused
Millised on poliitikavariandid eesmärkide saavutamiseks? Kas on olemas eelistatud variant? Kui ei, siis miks?
Kaaluti järgmisi variante: variant 1: ELi õigusakt, millega luuakse vabatahtlik märgistuskord; variant 2: ajutine valdkondlik lähenemisviis; variant 3: horisontaalne ELi õigusakt, millega kehtestatakse kohustuslikud nõuded suure riskiga tehisintellektirakendustele; variant 3+: sama mis 3, kuid koos vabatahtlike tegevusjuhenditega muu kui suure riskiga tehisintellektirakenduste kohta ning variant 4: horisontaalne ELi õigusakt, millega kehtestatakse kohustuslikud nõuded kõigile tehisintellektirakendustele. Eelistatud on variant 3+, sest see tagab proportsionaalsed kaitsemeetmed tehisintellektiga kaasnevate riskide eest, viies samas haldus- ja vastavuskulud miinimumini. Vastutust tehisintellektirakenduste eest käsitletakse konkreetselt tulevastes eraldi õigusnormides ja seega poliitikavariandid seda ei hõlma.
Millised on eri sidusrühmade seisukohad? Kes toetab millist varianti?

Ettevõtjad, ametiasutused, akadeemikud ja valitsusvälised organisatsioonid on ühel meelel, et esineb seaduslünki või et vaja on uusi õigusakte, kuigi ettevõtjate seas on see enamuse väiksem. Tööstus ja ametiasutused leiavad, et kohustuslikud nõuded tuleks kehtestada vaid suure riskiga tehisintellektirakendustele. Kodanikud ja kodanikuühiskond nõustuvad väiksema tõenäosusega kohustuslike nõuete kehtestamisega üksnes suure riskiga tehisintellektirakendustele.
C. Eelistatud poliitikavariandi mõju
Millised on eelistatud poliitikavariandi (kui see on olemas, vastasel korral peamiste poliitikavariantide) eelised?
Kodanike arvates vähendab eelistatud poliitikavariant ohtu nende turvalisusele ja põhiõigustele. Tehisintellekti pakkujatele tekitab see õiguskindluse ja tagab, et tehisintellektiga seotud teenuste ja toodete piiriülesel pakkumisel ei esine takistusi. See suurendab tehisintellekti kasutavate ettevõtjate usaldusväärsust nende klientide silmis. Riikide haldusasutuste arvates suurendab see üldsuse usaldust tehisintellekti kasutamise vastu ja tugevdab jõustamismehhanisme (kehtestades Euroopa koordineerimismehhanismi, tagades asjakohase suutlikkuse ja hõlbustades tehisintellektisüsteemide auditeerimist uute dokumenteerimis-, jälgitavus- ja läbipaistvusnõuete alusel).
Millised on eelistatud poliitikavariandi (kui see on olemas, vastasel korral peamiste poliitikavariantide) kulud?
Ettevõtjad või ametiasutused, kes arendavad või kasutavad tehisintellektirakendusi, mis hõlmavad suurt riski kodanike ohutusele või põhiõigustele, peaksid järgima harmoneeritud tehniliste standarditega kehtestatavaid horisontaalseid erinõudeid ja -kohustusi. Nõuete järgimise koondatud kogukulu on 2025. aastaks hinnanguliselt 100–500 miljonit eurot, mis vastab kuni 4–5 %-le suure riskiga tehisintellekti valdkonda tehtavatest investeeringutest (mis on hinnanguliselt 5–15 % kõigist tehisintellektirakendustest). Suure riskiga tehisintellekti valdkonda tehtavatest investeeringutest veel 2–5 % võivad moodustada kontrollikulud. Kulusid ei peaks kandma ettevõtjad või ametiasutused, kes arendavad või kasutavad tehisintellektirakendusi, mis ei ole liigitatud suure riskiga rakendusteks. Küll aga võivad nad otsustada järgida vabatahtlikke tegevusjuhendeid, et täita sobivad nõuded ja tagada, et nende tehisintellekt on usaldusväärne. Sellistel juhtudel võivad kulud olla kuni sama suured kui suure riskiga rakenduste puhul, kuid tõenäoliselt väiksemad.
Milline on mõju VKEdele ja konkurentsivõimele?
Suurem üldine usaldus tehisintellekti vastu toob rohkem kasu VKEdele kui suurtele ettevõtjatele, kes saavad loota ka oma kaubamärgi kuvandile. Suure riskiga rakendusi arendavad VKEd peaksid kandma suurte ettevõtjatega sarnaseid kulusid. Digitehnoloogia suure skaleeritavuse tõttu võib väikestel ja keskmise suurusega ettevõtjatel olla nende väiksusest hoolimata tohtu haare ja mõju miljonitele isikutele. Seega võib suure riskiga tehisintellektirakendusi pakkuvate VKEde väljajätmine reguleeriva raamistiku kohaldamisalast raskesti kahjustada usalduse suurendamise eesmärki. Raamistikus nähakse aga ette erimeetmed, sealhulgas regulatsiooni testkeskkonnad või digitaalse innovatsiooni keskuste kaudu pakutav abi, et toetada VKEsid uute eeskirjade järgimisel, võttes arvesse nende erivajadusi.
Kas on ette näha märkimisväärset mõju riigieelarvetele ja ametiasutustele?
Liikmesriigid peaksid määrama järelevalveasutused, mis juhivad õigusnõuete rakendamist. Järelevalvefunktsiooni täites võiksid nad tugineda olemasolevale korrale, näiteks vastavushindamisasutuste või turujärelevalve korrale, kuid vajaksid piisavat tehnoloogilist oskusteavet ja vahendeid. Olenevalt igas liikmesriigis eelnevalt olemasolevast struktuurist võiks see olla 1–25 täistööaja ekvivalenti liikmesriigi kohta.
Kas on oodata muud olulist mõju?
Eelistatud poliitikavariant vähendaks märkimisväärselt riske kodanike põhiõigustele ja liidu üldisematele väärtustele ning suurendaks teatavate tehisintellektitehnoloogiat või eraldiseisvaid tehisintellektirakendusi sisaldavate toodete ja teenuste ohutust.
Proportsionaalsus?
Ettepanek on proportsionaalne ja vajalik eesmärkide täitmiseks, sest järgib riskipõhist lähenemisviisi ja

sellega kehtestatakse regulatiivne koormus vaid siis, kui tehisintellektisüsteemid põhjustavad tõenäoliselt suuri riske põhiõigustele või ohutusele. Muul juhul kehtestatakse ainult minimaalsed läbipaistvuskohustused, eelkõige kohustus jagada teavet, et märgistada tehisintellektisüsteemi kasutamine inimestega suhtlemisel või süvavõltsingute kasutamine õigusvastastel eesmärkidel. Harmoneeritud standardid, lisasuunised ja nõuete täitmise abivahendid aitavad pakkujatel ja kasutajatel järgida nõudeid ja vähendada kulusid.

D. Järeldused

Millal poliitika läbi vaadatakse?

Komisjon avaldab aruande, milles hinnatakse raamistikku ja vaadatakse see läbi, viis aastat pärast selle kohaldamise alguskuupäeva.