Euroopa Parlament
2019-2024

Istungidokument

A9-0232/2021

13.7.2021

RAPORT

tehisintellekti kohta kriminaalõiguses ning tehisintellekti politsei- ja õigusasutuste poolt kriminaalasjades kasutamise kohta
(2020/2016(INI))

Kodanikuvabaduste, justiits- ja siseasjade komisjon

Raportöör: Petar Vitanov

PR_INI

SISUKORD

lk

EUROOPA PARLAMENDI RESOLUTSIOONI ETTEPANEK

tehisintellekti kohta kriminaalõiguses ning tehisintellekti politsei- ja õigusasutuste poolt kriminaalasjades kasutamise kohta
(2020/2016(INI))

Euroopa Parlament,

– võttes arvesse Euroopa Liidu lepingut, eriti selle artikleid 2 ja 6, ning Euroopa Liidu toimimise lepingut, eriti selle artiklit 16,

– võttes arvesse Euroopa Liidu põhiõiguste hartat, eriti selle artikleid 6, 7, 8, 11, 12, 13, 20, 21, 24 ja 47,

– võttes arvesse inimõiguste ja põhivabaduste kaitse konventsiooni,

– võttes arvesse Euroopa Nõukogu konventsiooni üksikisikute kaitse kohta isikuandmete automatiseeritud töötlemisel (ETS 108) ja selle muutmise protokolli (konventsioon nr 108+),

– võttes arvesse Euroopa Nõukogu kohtute efektiivsust hindava komisjoni (CEPEJ) Euroopa eetikahartat tehisintellekti kasutamise kohta kohtusüsteemides ja nende keskkonnas,

– võttes arvesse komisjoni 8. aprilli 2019. aasta teatist „Usalduse loomine inimkeskse tehisintellekti vastu“ (COM(2019)0168),

– võttes arvesse usaldusväärse tehisintellekti eetikasuuniseid, mille avaldas komisjoni kõrgetasemeline tehisintellekti eksperdirühm 8. aprillil 2019,

– võttes arvesse komisjoni 19. veebruari 2020. aasta valget raamatut „Tehisintellekt: Euroopa käsitus tipptasemel ja usaldusväärsest tehnoloogiast“ (COM(2020)0065),

– võttes arvesse komisjoni 19. veebruari 2020. aasta teatist „Euroopa andmestrateegia“ (COM(2020)0066),

– võttes arvesse Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta määrust (EL) 2016/679 füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus)[1],

– võttes arvesse Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta direktiivi (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

[1] ELT L 119, 4.5.2016, lk 1.

vaba liikumist ning millega tunnistatakse kehtetuks nõukogu raamotsus 2008/977/JSK[2],

– võttes arvesse Euroopa Parlamendi ja nõukogu 23. oktoobri 2018. aasta määrust (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[3],

– võttes arvesse Euroopa Parlamendi ja nõukogu 12. juuli 2002. aasta direktiivi 2002/58/EÜ, milles käsitletakse isikuandmete töötlemist ja eraelu puutumatuse kaitset elektroonilise side sektoris (eraelu puutumatust ja elektroonilist sidet käsitlev direktiiv)[4],

– võttes arvesse Euroopa Parlamendi ja nõukogu 11. mai 2016. aasta määrust (EL) 2016/794, mis käsitleb Euroopa Liidu Õiguskaitsekoostöö Ametit (Europol) ning millega asendatakse ja tunnistatakse kehtetuks nõukogu otsused 2009/371/JSK, 2009/934/JSK, 2009/935/JSK, 2009/936/JSK ja 2009/968/JSK[5],

– võttes arvesse oma 19. juuni 2020. aasta resolutsiooni George Floydi surmale järgnenud rassismivastaste meeleavalduste kohta[6],

– võttes arvesse oma 14. märtsi 2017. aasta resolutsiooni suurandmete mõju kohta põhiõigustele, sealhulgas eraelu puutumatusele, andmekaitsele, diskrimineerimiskeelule, turvalisusele ja õiguskaitsele[7],

– võttes arvesse 20. veebruaril 2020. aastal kodanikuvabaduste, justiits- ja siseasjade komisjonis toimunud kuulamist teemal „Tehisintellekt kriminaalõiguses ning selle kasutamine politsei- ja õigusasutuste poolt kriminaalasjades“,

– võttes arvesse aruannet, mis käsitleb kodanikuvabaduste, justiits- ja siseasjade komisjoni 2020. aasta veebruari lähetust Ameerika Ühendriikidesse,

– võttes arvesse kodukorra artiklit 54,

– võttes arvesse siseturu- ja tarbijakaitsekomisjoni ning õiguskomisjoni arvamusi,

– võttes arvesse kodanikuvabaduste, justiits- ja siseasjade komisjoni raportit (A9-0232/2021),

A. arvestades, et digitehnoloogiad üldiselt ning andmetöötluse ja -analüüsi levik eriti tehisintellekti abil on erakordselt paljulubavad ja riskantsed; arvestades, et tehisintellekti arengus on viimastel aastatel toimunud suur hüpe, mistõttu see on üks 21. sajandi strateegilisi tehnoloogiaid, millega kaasnevad potentsiaalselt märkimisväärsed eelised tõhususe, täpsuse ja mugavuse osas ning mis toob seega Euroopa majandusse ja ühiskonda positiivseid muutusi, kuid kujutab ühtlasi suurt ohtu

[2] ELT L 119, 4.5.2016, lk 89.
[3] ELT L 295, 21.11.2018, lk 39.
[4] ELT L 201, 31.7.2002, lk 37.
[5] ELT L 135, 24.5.2016, lk 53.
[6] Vastuvõetud tekstid, P9_TA(2020)0173.
[7] ELT C 263, 25.7.2018, lk 82.

põhiõigustele ja õigusriigi põhimõttel põhinevatele demokraatlikele riikidele; arvestades, et tehisintellekti ei peaks käsitlema eesmärgina omaette, vaid inimeste kasuks rakendatava vahendina, mille lõppeesmärk on inimeste heaolu, inimvõimekuse ja ohutuse suurendamine;

B. arvestades, et hoolimata arvutite töötlemiskiiruse ja mälumahu pidevast arengust ei ole veel olemas programme, mis suudaksid võistelda inimeste paindlikkusega laiemate valdkondade üleselt või ülesannetes, mis eeldavad konteksti mõistmist või kriitilist analüüsi; arvestades, et mõned tehisintellekti rakendused on teatud konkreetsete ülesannete (nt õigustehnoloogia) sooritamisel saavutanud inimekspertide ja -spetsialistide sooritustaseme ning suudavad pakkuda tulemusi oluliselt suurema kiirusega ja laiema ulatusega;

C. arvestades, et mõned riigid, sealhulgas mitu liikmesriiki, kasutavad tehisintellekti rakendusi või tehisintellekti manussüsteeme õiguskaitses ja kohtusüsteemis rohkem kui teised, mis on osaliselt tingitud puudulikust reguleerimisest ja regulatiivsetest erinevustest, mis lubavad või keelavad kasutada tehisintellekti teatud eesmärkidel; arvestades, et tehisintellekti järjest suurem kasutus kriminaalõiguses põhineb eelkõige lubadustel, et see vähendaks teatavat liiki kuritegevust ja tooks kaasa objektiivsemad otsused; arvestades, et need lubadused alati ei täitu;

D. arvestades, et hartas sätestatud põhiõigused ja -vabadused peaksid olema tagatud tehisintellekti ja sellega seotud tehnoloogiate kogu elutsükli jooksul, eriti nende projekteerimise, arendamise, kasutuselevõtu ja kasutamise ajal, ning neid tuleks kohaldada õiguskaitse suhtes igas olukorras;

E. arvestades, et tehisintellekti tehnoloogiat tuleks arendada nii, et selle keskmes oleksid inimesed, see vääriks üldsuse usaldust ja töötaks alati inimeste teenistuses; arvestades, et tehisintellekti süsteemidel peaks olema lõplik garantii, et need on loodud nii, et inimoperaator saab need alati välja lülitada;

F. arvestades, et tehisintellekti süsteemid peavad olema loodud kõigi ühiskonnaliikmete kaitse ja kasu eesmärgil (süsteemi väljatöötamisel tuleb arvesse võtta ka haavatavat, tõrjutud elanikkonda), peavad olema mittediskrimineerivad ja ohutud, nende otsused peavad olema selgitatavad ja läbipaistvad, need peavad austama inimeste autonoomiat ja põhiõigusi, et olla usaldusväärsed, nagu on kirjeldatud kõrgetasemelise tehisintellekti eksperdirühma eetikasuunistes;

G. arvestades, et liidul koostöös liikmesriikidega lasub oluline vastutus selle eest, et tehisintellekti kohtu- ja õiguskaitse valdkonna rakenduste elutsükli ja kasutamisega seotud otsused tehakse läbipaistvalt, need kaitsevad täielikult põhiõigusi ning eelkõige ei põlista olemasolevat diskrimineerimist, kallutatust ja eelarvamusi; arvestades, et asjakohased poliitilised valikud peaksid järgima vajalikkuse ja proportsionaalsuse põhimõtteid, et tagada põhiseaduslikkus ning õiglane ja inimlik kohtusüsteem;

H. arvestades, et tehisintellekti rakendused võivad pakkuda õiguskaitse valdkonnas suurepäraseid võimalusi, eelkõige õiguskaitse- ja õigusasutuste töömeetodite parandamisel ning teatavat liiki kuritegudega, eelkõige finantskuritegudega, rahapesuga ja terrorismi rahastamisega, veebis toimuva laste seksuaalse kuritarvitamise ja ärakasutamisega ning teatavat liiki küberkuritegevusega tõhusamal võitlemisel,

panustades seeläbi ELi kodanike ohutusse ja julgeolekusse, kuid samal ajal võivad nendega kaasneda märkimisväärsed ohud inimeste põhiõigustele; arvestades, et tehisintellekti üldine kasutamine massijälgimise eesmärgil oleks ebaproportsionaalne;

I. arvestades, et tehisintellekti süsteemide arendamine politsei- ja õigusasutuste jaoks ning nende kasutamine hõlmab mitmete üksikisikute, organisatsioonide, masinakomponentide, tarkvara algoritmide ja inimkasutajate panust sageli keerukates ja proovilepanevates keskkondades; arvestades, et tehisintellekti rakendused õiguskaitses ja kohtusüsteemis on erinevates arenguetappides, alates kontseptsiooni väljatöötamisest prototüüpimise või hindamiseni ja heakskiidule järgneva kasutuseni; arvestades, et tulevikus võib tekkida uusi kasutusvõimalusi, kui tehnoloogia muutub küpsemaks tänu kogu maailmas käimasolevale intensiivsele teaduslikule uurimistööle;

J. arvestades, et hädavajalik on luua tehisintellekti süsteemide võimalike kahjulike mõjude eest kriminaalõiguse valdkonnas selge juriidilise vastutuse kandmise mudel; arvestades, et selle valdkonna õigusnormid peaksid alati säilitama inimese vastutuse ning nende eesmärk peab olema esiteks ja eelkõige vältida kahjuliku mõju põhjustamist;

K. arvestades, et kui tehisintellekti süsteeme kasutatakse õiguskaitse ja kohtuvaldkonnas, on lõpuks liikmesriikide vastutus tagada põhiõiguste täielik austamine;

L. arvestades, et põhiõiguste kaitsmise ja tõhusa politseitegevuse vaheline suhe peab alati olema oluline element aruteludes selle üle, kas ja kuidas tuleks tehisintellekti kasutada õiguskaitse valdkonnas, kus otsustel võivad olla pikaajalised tagajärjed üksikisikute elule ja vabadusele; arvestades, see on eriti tähtis, kuna tehisintellektil on potentsiaal olla püsiv osa meie kriminaalõiguse ökosüsteemist, pakkudes uurivat analüüsi ja abi;

M. arvestades, et õiguskaitseasutused kasutatavad tehisintellekti sellistes rakendustes nagu näotuvastustehnoloogiad, näiteks kahtlusaluste andmebaaside sirvimiseks ja inimkaubanduse või laste seksuaalse ärakasutamise ja kuritarvitamise ohvrite tuvastamiseks, numbrimärgi automaattuvastus, kõneleja tuvastus, huultelt lugemise tehnoloogiad, pealtkuulamine (st lasutuvastusalgoritmid), autonoomne otsing identifitseeritavates andmebaasides ja selliste andmebaaside analüüs, prognoosimine (ennetav politseitegevus ja sageli kuriteopaigaks olevate kohtade analüüs), käitumise tuvastamise vahendid, kõrgtehnoloogilised virtuaalsed lahkamisvahendid surmapõhjuse kindlaks määramiseks, autonoomsed vahendid finantspettuse ja terrorismi rahastamise kindlaks tegemiseks, sotsiaalmeedia seire (andmekoorimine ja -kogumine seoste kindlaks tegemiseks) ning eri tuvastamisvõimalusi hõlmavad automatiseeritud seiresüsteemid (näiteks südamelöökide tuvastamine ja soojuskaamerad); arvestades, et eespool nimetatud rakenduste ning teiste võimalike või tulevaste õiguskaitses kasutatavate tehisintellekti rakenduste usaldusväärsus, täpsus ning mõju põhiõigustele ja kriminaalõigussüsteemide dünaamikale võib olla väga erinev; arvestades, et paljusid neist vahenditest kasutatakse ELi mittekuuluvates riikides, kuid liidu andmekaitseõigustiku ja kohtupraktika kohaselt oleksid need ebaseaduslikud; arvestades, et algoritmide rutiinne kasutuselevõtmine, isegi madala valepositiivsete tulemuste määra korral, võib tuua kaasa palju rohkem valehäireid kui õigeid häireid;

N. arvestades, et tehisintellekti vahendeid ja rakendusi kasutatakse ka mitme riigi kohtusüsteemis kogu maailmas, sealhulgas eelvangistust puudutavate otsuste

toetamiseks, karistuse määramisel, uue kuriteo toimepanemise tõenäosuse arvutamisel ja katseaja määramisel, vaidluste internetipõhisel lahendamisel, kohtupraktika haldamisel ja seadusele hõlbustatud juurdepääsu tagamisel; arvestades, et see on toonud muu kui valge nahavärviga inimeste ja teiste vähemuste jaoks kaasa moonutatud ja väiksemad võimalused; arvestades, et nende kasutamine piirdub praegu ELis, kui mõned liikmesriigid välja arvata, peamiselt tsiviilasjadega;

O. arvestades, et tehisintellekti kasutamisega õiguskaitse valdkonnas kaasnevad paljud potentsiaalselt suured ja mõnel juhul vastuvõetamatud ohud üksikisikute põhiõiguste kaitsele, nagu läbipaistmatu otsuste tegemine, eri liiki diskrimineerimine ja vead, mis on omased aluseks olevale algoritmile, mida võivad tugevdada tagasisideahelad, ning ohud eraelu puutumatuse ja isikuandmete kaitsele, väljendus- ja teabevabaduse kaitsele, süütuse presumptsioonile, õigusele tõhusale õiguskaitsevahendile ja õiglasele kohtulikule arutamisele ning ka ohud üksikisikute vabadusele ja julgeolekule;

P. arvestades, et õiguskaitseasutuste ja kohtusüsteemi kasutatavad tehisintellekti süsteemid on haavatavad ka infosüsteemide vastu suunatud tehisintellekti toel rünnakute ja andmemürgituse suhtes, mille puhul kaasatakse tahtlikult vale andmekogum, et luua kallutatud tulemusi; arvestades, et sellistes olukordades võib tekkinud kahju olla veelgi suurem ja see võib nii üksikisikuid kui ka rühmi oluliselt rohkem kahjustada;

Q. arvestades, et tehisintellekti kasutuselevõttu õiguskaitse ja kohtuvaldkonnas ei tohiks näha pelgalt tehnilise teostatavusena, vaid poliitilise otsusena õiguskaitse- ja kriminaalõigussüsteemide ülesehituse ja eesmärkide kohta; arvestades, et kaasaegne kriminaalõigus põhineb ideel, et ametiasutused reageerivad rikkumisele pärast selle toimepanemist, eeldamata, et kõik inimesed on ohtlikud ja neid tuleb võimalike väärtegude ennetamiseks pidevalt jälgida; arvestades, et tehisintellektil põhinevad seiretehnikad seavad selle lähenemisviisi tõsiselt kahtluse alla ja tingivad vajaduse, et kogu maailma seadusandjad hindaksid kiiresti ja põhjalikult selliste tehnoloogiate kasutuselevõtu lubamise tagajärgi, mis vähendavad inimeste rolli õiguskaitses ja kohtumõistmisel;

1. kordab, et kuna tehisintellekti keskmes on suure hulga isikuandmete töötlemine, kehtib kõigis tehisintellekti valdkondades õigus eraelu puutumatuse ja isikuandmete kaitsele ning tuleb täielikult järgida liidu andmekaitse ja eraelu puutumatuse kaitse õigusraamistikku; tuletab seetõttu meelde, et EL on juba kehtestanud andmekaitsestandardid õiguskaitses, mis moodustavad kõigi tulevaste tehisintellekti kasutamist õiguskaitses ja kohtusüsteemis käsitlevate õigusaktide aluse; tuletab meelde, et isikuandmete töötlemine peaks olema seaduslik ja õiglane, töötlemise eesmärgid peaksid olema täpsustatud, selgesõnalised ja õiguspärased, töötlemine peaks olema asjakohane ega tohiks ületada töötlemise eesmärki, see peaks olema täpne ja ajakohastatud ning ebatäpsed andmed tuleks (kui ei kohaldata piiranguid) parandada või kustutada, andmeid ei tohiks säilitada kauem, kui on vajalik, tuleks kehtestada selged ja asjakohased tähtajad selliste andmete kustutamiseks või nende säilitamise vajaduse korrapäraseks läbivaatamiseks ning neid tuleks töödelda turvaliselt; rõhutab lisaks, et tuleks vältida isikute võimalikku tuvastamist tehisintellekti rakenduse abil, kasutades varem anonüümseks muudetud andmeid;

2. kinnitab veel kord, et kõik õiguskaitse ja kohtusüsteemi jaoks mõeldud tehisintellekti

lahendused peavad samuti olema täielikus kooskõlas selliste põhimõtetega nagu inimväärikus, diskrimineerimiskeeld, liikumisvabadus, süütuse presumptsioon ja kaitseõigus, sealhulgas vaikimisõigus, väljendus- ja teabevabadus, kogunemis- ja ühinemisvabadus, võrdsus seaduse ees, poolte võrdsuse põhimõte ning õigus tõhusale õiguskaitsevahendile ja õiglasele kohtulikule arutamisele, kooskõlas hartaga ning Euroopa inimõiguste konventsiooniga; rõhutab, et tehisintellekti rakenduste kasutamine tuleb keelata, kui see on põhiõigustega vastuolus;

3. tunnistab, et kogu maailmas tehisintellekti rakenduste väljatöötamise kiirus ei võimalda koostada rakenduste ammendavat loetelu ning seetõttu on vaja selget ja sidusat juhtimismudelit, millega tagatakse nii üksikisikute põhiõigused kui ka arendajatele õigusselgus, arvestades tehnoloogia pidevat arengut; on siiski seisukohal, et arvestades politsei- ja õigusasutuste rolli ja vastutust ning nende poolt kuritegude ennetamiseks, uurimiseks, avastamiseks või nende eest vastutusele võtmiseks või kriminaalkaristuste täitmisele pööramiseks tehtavate otsuste mõju, tuleb tehisintellekti rakenduste kasutamine liigitada kõrge riskiastmega kasutamiseks juhtudel, kui see võib oluliselt mõjutada üksikisikute elu;

4. on sellega seoses seisukohal, et mis tahes tehisintellekti vahendid, mille on välja töötanud või mida kasutavad õiguskaitse- või kohtuasutused, peaksid olema vähemalt ohutud, töökindlad, turvalised ja eesmärgipäraselt kasutatavad, nende puhul tuleb järgida õigluse, võimalikult väheste andmete kogumise, vastutuse, läbipaistvuse, mittediskrimineerimise ja selgitatavuse põhimõtteid ning nende vahendite väljatöötamise, kasutamise ja kasutuselevõtu puhul tuleks hinnata riske ning rangelt kontrollida nende vajalikkust ja proportsionaalsust, kusjuures kaitsemeetmed peavad olema proportsionaalsed avastatud riskidega; rõhutab, et usaldus kodanike seas ELis arendatud, kasutusele võetud ja kasutatava tehisintellekti vastu sõltub nende kriteeriumide täielikust täitmisest;

5. tunnistab teatavat liiki tehisintellekti rakenduste positiivset panust õiguskaitse- ja õigusasutuste töösse kogu liidus; toob näitena esile täiustatud kohtupraktika haldamise, mis saavutatakse täiendavaid otsinguvõimalusi pakkuvate vahenditega; on veendunud, et tehisintellektil on õiguskaitses ja kohtusüsteemis mitmeid muid võimalikke kasutusviise, mida võiks uurida, võttes arvesse CEPEJ poolt vastu võetud eetikaharta (tehisintellekti kasutamise kohta kohtusüsteemides ja nende keskkonnas) viit põhimõtet ja pöörates erilist tähelepanu CEPEJ nimetatud „kasutusviisidele, mida tuleb käsitleda kõige suurema ettevaatlikkusega“;

6. rõhutab, et igale tehnoloogiale saab anda uue kasutusotstarbe, ning nõuab seetõttu ranget demokraatlikku kontrolli ja sõltumatut järelevalvet kõigi õiguskaitse- ja õigusasutuste kasutatavate tehisintellektil põhinevate tehnoloogiate üle, eriti nende üle, millele saab anda uue kasutusotstarbe massijärelevalve või massilise profiilimise eesmärgil; võtab seetõttu väga murelikult teadmiseks õiguskaitsesektoris kasutatavate teatavate tehisintellekti tehnoloogiate potentsiaali massijälgimise alal; rõhutab õiguslikku nõuet takistada massijälgimist tehisintellekti tehnoloogiate abil, mis olemuselt ei vasta vajalikkuse ja proportsionaalsuse põhimõtetele, ning keelata selliste rakenduste kasutamine, mis võivad kaasa tuua massijälgimise;

7. rõhutab, et lähenemisviis, mis on mõnes ELi mittekuuluvas riigis võetud

massijälgimistehnoloogia arendamiseks, kasutuselevõtmiseks ja kasutamiseks, sekkub ebaproportsionaalselt põhiõigustesse ja seega ei tohi EL seda järgida; rõhutab seetõttu, et kaitsemeetmeid õiguskaitse- ja õigusasutuste poolt tehisintellekti tehnoloogiate väärkasutamise vastu tuleb samuti kogu liidus ühetaoliselt reguleerida;

8. rõhutab tehisintellekti rakenduste, nagu masinõppe, sealhulgas rakenduste aluseks olevate algoritmide kasutamisest tulenevat võimalikku kallutatuse ja diskrimineerimise ohtu; märgib, et kallutatus võib tuleneda aluseks olevatest andmekogumitest, eriti kui kasutatakse vanu andmeid, selle võivad põhjustada algoritmide väljatöötajad või see võib tekkida süsteemide rakendamisel tegelikus keskkonnas; juhib tähelepanu sellele, et tehisintellekti rakenduste abil saavutatud tulemusi mõjutab paratamatult kasutatavate andmete kvaliteet ning sellised loomupärased eelarvamused kalduvad järk-järgult suurenema ning seeläbi põlistama ja võimendama olemasolevat diskrimineerimist, eriti teatavatesse etnilistesse rühmadesse või rassismi tõttu ebasoodsas olukorras olevatesse kogukondadesse kuuluvate isikute puhul;

9. rõhutab asjaolu, et paljud praegu kasutatavad algoritmipõhised identifitseerimistehnoloogiad identifitseerivad ja klassifitseerivad ebaproportsionaalselt sageli valesti ning põhjustavad seetõttu kahju rassismi tõttu ebasoodsas olukorra olevatele inimestele, teatavatesse etnilistesse kogukondadesse kuuluvatele isikutele, LGBTI-inimestele, lastele, eakatele ja naistele; tuletab meelde, et isikutel on peale korrektse identifitseerimise õiguse ka õigus mitte olla identifitseeritud, välja arvatud juhul, kui seda nõutakse seadusega kaaluka ja õigustatud avaliku huvi tõttu; rõhutab, et tehisintellekti ennustused, mis põhinevad konkreetse isikute rühma omadustel, toovad kaasa olemasolevate diskrimineerimisvormide võimendamise ja paljundamise; on seisukohal, et automaatse diskrimineerimise ja kallutatuse vältimiseks tuleks teha suuri jõupingutusi; nõuab tugevaid lisakaitsemeetmeid juhul, kui õiguskaitse- või kohtuasutuste tehisintellekti süsteeme kasutatakse alaealiste puhul või alaealistega seoses;

10. rõhutab võimu asümmeetriat tehisintellekti tehnoloogiate kasutajate ja nende vahel, kelle suhtes seda kasutatakse; rõhutab, et on hädavajalik, et tehisintellekti vahendite kasutamine õiguskaitse- ja õigusasutuste poolt ei muutuks ebavõrdsuse, sotsiaalse lõhestatuse või tõrjutuse teguriks; rõhutab tehisintellekti vahendite kasutamise mõju kahtlusaluste kaitseõigustele, raskusi sisulise teabe saamisel nende toimimise kohta ja sellest tulenevaid raskusi nende tulemuste vaidlustamisel kohtus, eriti uurimise all olevate isikute poolt;

11. võtab teadmiseks ohud, mis on seotud eriti andmeleketega, andmete turvalisuse rikkumisega ning loata juurdepääsuga isikuandmetele ja muule tehisintellekti süsteemide kaudu töödeldavale näiteks kriminaaluurimiste või kohtuasjadega seotud teabele; rõhutab, et tuleb hoolikalt kaaluda õiguskaitses ja kohtuasutuste poolt kasutatavate tehisintellekti süsteemide turvalisuse ja ohutuse aspekte ning need süsteemid peavad olema piisavalt kindlad ja vastupidavad, et vältida tehisintellekti süsteemide vastu suunatud kuritahtlike rünnakute võimalikke katastroofilisi tagajärgi; rõhutab, kui oluline on sisseprojekteeritud turve ja spetsiaalne inimjärelevalve enne teatavate kriitilise tähtsusega rakenduste kasutamist, ning nõuab seetõttu, et õiguskaitse- ja õigusasutused kasutaksid üksnes tehisintellekti rakendusi, mis järgivad eraelu puutumatuse ja isikuandmete lõimitud kaitse põhimõtet, et vältida funktsioonide

laienemist;

12. rõhutab, et ühelgi õiguskaitse- või kohtuasutuste kasutataval tehisintellekti süsteemil ei tohiks olla võimalik kahjustada inimeste kehalist puutumatust, anda üksikisikutele õigusi või panna neile juriidilisi kohustusi;

13. tunnistab raskusi võimaliku kahju korral juriidilise vastutuse ja kohustuse korrektsel tuvastamisel, arvestades tehisintellekti süsteemide arendamise ja toimimise keerukust; peab vajalikuks luua selge ja õiglane juriidilise vastutuse ja kohustuse kandmise kord digitaalsetest kõrgtehnoloogiatest tulenevate võimalike negatiivsete tagajärgede korral; toonitab siiski, et eesmärk peab olema ennekõike selliste tagajärgede tekkimist algusest peale vältida; nõuab seetõttu, et kõigi tehisintellekti rakenduste puhul õiguskaitse kontekstis rakendataks ettevaatuspõhimõtet; rõhutab, et juriidiline vastutus ja kohustus peab alati lasuma füüsilisel või juriidilisel isikul, kes tuleb tehisintellekti toel tehtavate otsuste puhul alati tuvastada; rõhutab seetõttu vajadust tagada tehisintellekti süsteeme tootvate ja haldavate ettevõttestruktuuride läbipaistvus;

14. peab nii kaitseõiguste kasutamise tõhususe kui ka riiklike kriminaalõigussüsteemide läbipaistvuse seisukohast oluliseks, et tehisintellekti vahendite kasutamise tingimusi, viise ja tagajärgi õiguskaitse ja kohtuvaldkonnas, samuti sihtmärgiks olevate isikute õigusi, sealhulgas tõhusaid ja kergesti kättesaadavaid kaebuste käsitlemise ning kahju hüvitamise menetlusi reguleerib konkreetne, selge ja täpne õigusraamistik; rõhutab kriminaalmenetluse osaliste õigust pääseda juurde andmete kogumise protsessile ja sellega seotud hindamistele, mis on tehtud või saadud tehisintellekti rakendusi kasutades; rõhutab, et õigusalases koostöös osalevad täitvad asutused peavad teisele liikmesriigile või ELi mittekuuluvale riigile väljaandmise (või üleandmise) taotluse üle otsustamisel hindama, kas tehisintellekti vahendite kasutamine taotlevas riigis võib ilmselt kahjustada põhiõigust õiglasele kohtumenetlusele; palub komisjonil anda välja suunised selle kohta, kuidas sellist hindamist kriminaalasjades tehtava õigusalase koostöö raames teha; rõhutab, et liikmesriigid peaksid kooskõlas kohaldatavate õigusaktidega tagama, et üksikisikuid teavitatakse, kui õiguskaitseasutused või kohtud kasutavad nende suhtes tehisintellekti rakendusi;

15. juhib siiski tähelepanu sellele, et kui inimesed toetuvad ainult masinate loodud andmetele, profiilidele ja soovitustele, ei suuda nad teha sõltumatut hindamist; rõhutab võimalikke raskeid negatiivseid tagajärgi, eriti õiguskaitse ja õigusemõistmise valdkonnas, kui üksikisikud usaldavad liialt tehisintellekti vahendite näiliselt objektiivset ja teaduslikku olemust ega kaalu võimalust, et nende tulemused on ebaõiged, mittetäielikud, mitteasjakohased või diskrimineerivad; rõhutab, et tehisintellekti süsteemide abil saadud tulemuste liigset usaldamist tuleks vältida, ning rõhutab, et ametiasutused peavad kasvatama enesekindlust ja teadmisi, et pidada algoritmilist soovitust küsitavaks või seda mitte järgida; peab oluliseks, et ootused selliste tehnoloogiliste lahenduste suhtes oleksid realistlikud ning et ei lubataks täiuslikke õiguskaitsealaseid lahendusi ja kõigi toimepandud õiguserikkumiste avastamist;

16. rõhutab, et kohtu- ja õiguskaitse valdkonnas peab õiguslike või samalaadsete tagajärgedega otsuse alati tegema inimene, keda saab tehtud otsuste eest vastutusele võtta; on seisukohal, et neil, kelle suhtes kohaldatakse tehisintellektil põhinevaid

süsteeme, peab olema võimalik kasutada õiguskaitsevahendeid; tuletab meelde, et ELi õiguse kohaselt on isikul õigus sellele, et tema suhtes ei tehta üksnes andmete automatiseeritud töötlemisele toetuvat otsust, millel on teda puudutavad õiguslikud tagajärjed või mis avaldab talle märkimisväärset mõju; rõhutab lisaks, et automatiseeritud töötlusel põhinevate üksikotsuste tegemine ei tohi põhineda isikuandmete eriliikidel, välja arvatud juhul, kui on kehtestatud asjakohased meetmed andmesubjekti õiguste, vabaduste ja õigustatud huvide kaitsmiseks; rõhutab, et ELi õigus keelab profiilianalüüsi, mis toob kaasa füüsiliste isikute diskrimineerimise isikuandmete eriliikide põhjal; rõhutab, et otsused õiguskaitse valdkonnas on peaaegu alati otsused, millel on õiguskaitseasutuste täitva olemuse ja tegevuse tõttu õiguslikud tagajärjed isikule, keda need puudutavad; märgib, et tehisintellekti kasutamine võib mõjutada inimeste otsuseid ja kõiki kriminaalmenetluse etappe; on seetõttu seisukohal, et tehisintellekti süsteeme kasutavad ametiasutused peavad järgima väga kõrgeid õiguslikke standardeid ja tagama inimsekkumise, eriti sellistest süsteemidest saadud andmete analüüsimisel; nõuab seetõttu, et austataks kohtunike suveräänset kaalutlusõigust ja igal üksikjuhul eraldi otsuse tegemist; nõuab, et keelataks tehisintellekti ja seotud tehnoloogiate kasutamine kohtuotsuste ettepanekute koostamiseks;

17. nõuab algoritmide selgitatavust, läbipaistvust, jälgitavust ja kontrollimist järelevalve vajaliku osana, et tagada, et tehisintellekti süsteemide kohtuasutustes ja õiguskaitse eesmärgil arendamine, kasutuselevõtt ja kasutamine oleksid kooskõlas põhiõigustega ning et inimesed neid usaldaksid, samuti selleks, et tehisintellekti algoritmide abil saadud tulemused muudetaks arusaadavaks kasutajatele ja neile, kelle suhtes neid süsteeme kohaldatakse, ning et lähteandmed ja see, kuidas süsteem teatava järelduse tegi, oleksid läbipaistvad; juhib tähelepanu sellele, et tehnilise läbipaistvuse, töökindluse ja täpsuse tagamiseks peaks liidu õiguskaitse- või õigusasutustel olema lubatud osta ainult selliseid vahendeid ja süsteeme, mille algoritmid ja loogika on auditeeritavad ja kättesaadavad vähemalt politseile ja kohtutele ning sõltumatutele audiitoritele, et võimaldada nende hindamist, auditeerimist ja kontrollimist, ning müüjad ei tohi neid sulgeda ega märgistada kui ärisaladusi; juhib lisaks tähelepanu sellele, et tuleks tagada selges ja arusaadavas keeles dokumendid, mis käsitlevad teenuse olemust, arendatud vahendeid, jõudlust ja tingimusi, milles need eeldatavasti toimivad, ning võimalikke põhjustatavaid ohte; kutsub seetõttu õigus- ja õiguskaitseasutusi üles tagama ennetavat ja täielikku läbipaistvust eraettevõtjate suhtes, kes varustavad neid õiguskaitse ja kohtuvaldkonna jaoks mõeldud tehisintellekti süsteemidega; soovitab seetõttu võimaluse korral kasutada avatud lähtekoodiga tarkvara;

18. ergutab õiguskaitse- ja õigusasutusi tegema kindlaks ja hindama valdkondi, kus mõned vajadustele kohandatud tehisintellekti lahendused võiksid olla kasulikud, ning vahetama parimaid tavasid tehisintellekti kasutuselevõtu alal; nõuab, et liikmesriigid ja ELi ametid võtaksid vastu asjakohased avaliku hanke menetlused tehisintellekti süsteemide kohta, kui neid kasutatakse õiguskaitse või kohtu kontekstis, et tagada nende vastavus põhiõigustele ja kohaldatavatele õigusaktidele, tagades sealhulgas, et tarkvaradokumendid ja algoritmid on pädevatele ja järelevalveasutustele läbivaatamiseks kättesaadavad ja juurdepääsetavad; nõuab eelkõige siduvaid eeskirju, mis kohustaksid avaldama avaliku ja erasektori partnerlused, lepingud ja soetamised ning nende hankimise eesmärgi; rõhutab vajadust tagada asutustele vajalik rahastus ja

varustada nad vajaliku oskusteabega, et tagada täielik vastavus tehisintellekti kasutuselevõtuga seotud eetilistele, õiguslikele ja tehnilistele nõuetele;

19. nõuab, et tehisintellekti süsteemid ja otsustusprotsess, millega visandatakse nende funktsioonid, määratakse kindlaks süsteemide suutlikkus ja piirangud ning peetakse kohustusliku dokumentatsiooniga järge, milliste tegurite põhjal otsus tehti, oleksid jälgitavad; rõhutab, kui oluline on täielik dokumentatsioon treeningandmete, nende konteksti, eesmärgi, täpsuse ja kõrvalmõjude kohta ning algoritmide koostajate ja arendajate poolt nende töötlemise ja põhiõigustele vastavuse kohta; rõhutab, et alati peab olema võimalik teisendada tehisintellekti süsteemi arvutuskäik inimesele arusaadavale kujule;

20. nõuab, et tehtaks kohustuslik põhiõigustele avalduva mõju hinnang, enne kui tehisintellekti süsteemi õiguskaitse- või kohtusüsteemis rakendatakse või see seal kasutusele võetakse, et hinnata võimalikku ohtu põhiõigustele; tuletab meelde, et eelnev andmekaitsealane mõjuhinnang on kohustuslik igasuguse töötlemise puhul, eriti uute tehnoloogiate kasutamisel, millega võib tõenäoliselt kaasneda suur oht füüsiliste isikute õigustele ja vabadustele, ning on seisukohal, et see kehtib enamiku õiguskaitse ja kohtuvaldkonnas kasutatavate tehisintellekti tehnoloogiate korral; rõhutab andmekaitseasutuste ja põhiõiguste ametite asjatundlikkust nende süsteemide hindamisel; rõhutab, et need põhiõigustele avalduva mõju hinnangud tuleks teha võimalikult avalikult ja kodanikuühiskonna aktiivsel osalusel; nõuab, et mõjuhinnangutes esitataks selgelt ka tuvastatud riskide kõrvaldamiseks vajalikud kaitsemeetmed ja et mõjuhinnangud tehtaks enne tehisintellekti süsteemi kasutuselevõttu võimalikult suures ulatuses avalikkusele kättesaadavaks;

21. rõhutab, et ainult stabiilne Euroopa tehisintellekti juhtimine koos sõltumatu hindamisega võimaldab tagada vajaliku põhiõiguste printsiipide rakendamise; nõuab kõigi õiguskaitse- ja kohtusüsteemis kasutatavate tehisintellekti süsteemide korrapärast kohustuslikku auditit sõltumatu asutuse poolt juhtudel, kui see võib oluliselt mõjutada üksikisikute elu, et testida ja hinnata algoritmipõhiseid süsteeme, nende konteksti, eesmärki, täpsust, tulemuslikust ja ulatust, ning pärast nende kasutuselevõttu, et avastada, uurida, diagnoosida ja parandada soovimatut ja kahjulikku mõju ning tagada tehisintellekti süsteemide toimimine ettenähtud viisil; nõuab seetõttu selleks selget institutsioonilist raamistikku, sealhulgas nõuetekohast regulatiivset ja üldist järelevalvet, et tagada täielik rakendamine ja täielikult informeeritud demokraatlik arutelu tehisintellekti vajalikkuse ja proportsionaalsuse üle kriminaalõiguse valdkonnas; rõhutab, et nende auditite tulemused tuleks teha avalikes registrites kättesaadavaks, nii et kodanikud teaksid, milliseid tehisintellekti süsteeme kasutatakse ja millised meetmeid võetakse põhiõiguste rikkumiste heastamiseks;

22. rõhutab, et andmekogumid ja algoritmipõhised süsteemid, mida kasutatakse tehisintellekti ja sellega seotud tehnoloogiate arendamisel andmetöötluse erinevates staadiumites klassifikatsioonide, hindamiste ja ennustuste tegemisel, võivad samuti kaasa tuua inimrühmade eristava kohtlemise ning nii otsese kui ka kaudse diskrimineerimise, eriti kuna ennetava politseitegevuse algoritmide treenimiseks kasutatavad andmed peegeldavad käimasoleva järelevalve prioriteete ning seetõttu võivad need tuua kaasa olemasolevate eelarvamuste paljundamise ja võimendamise; rõhutab seetõttu, et eriti õiguskaitses ja kohtusüsteemis kasutamiseks mõeldud

tehisintellekti tehnoloogia puhul on nõutavad valdkondadevahelised uuringud ja sisend, sealhulgas teadus- ja tehnoloogiauuringute, kriitiliste rassiuuringute, puuetealaste uuringute ja muude sotsiaalsele kontekstile spetsialiseerunud erialade valdkonnast, sealhulgas küsimus, kuidas erinevus on konstrueeritud, klassifitseerimistöö ja selle tagajärjed; rõhutab, et seetõttu on vaja süstemaatiliselt investeerida nende valdkondade tehisintellekti uurimisse ja kõigi tasandite uurimistöösse integreerimisse; rõhutab ka seda, kui tähtis on, et töörühmad, mis neid tehisintellekti süsteeme õiguskaitse ja kohtute jaoks kavandavad, arendavad, katsetavad, hooldavad, kasutusele võtavad ja hangivad, peegeldaksid võimaluse korral ühiskonna mitmekesisust üldiselt, kuna see on mittetehniline vahend diskrimineerimisohu vähendamiseks;

23. rõhutab lisaks, et piisava aruandekohustuse, vastutuse ja kohustuse tagamiseks on vaja erikoolitust eetiliste sätete, võimalike ohtude, piirangute ja tehisintellekti tehnoloogia korrektse kasutamise alal, eelkõige politsei ja kohtuasutuste töötajate jaoks; rõhutab, et sobiv kutsealane koolitus ja kvalifikatsioon peaksid tagama, et otsustajaid koolitatakse kallutatuse võimalikkuse alal, kuna andmekogumid võivad põhineda diskrimineerivatel ja eelarvamuslikel andmetel; toetab teadlikkuse kasvatamise ja hariduslike algatuste loomist, et tagada õiguskaitses ja kohtuasutustes töötavate isikute teadlikkus ja arusaamine tehisintellekti süsteemide piirangutest, võimekusest ja nende kasutusega kaasnevatest ohtudest, sealhulgas automatiseerimise kallutatuse ohust; tuletab meelde, et kui tehisintellekti treeningandmete kogumitesse lisada politseijõudude poolt nende kohustuste täitmisel esinenud rassismi juhtumid, toob see paratamatult kaasa rassistliku kallutatuse tehisintellekti genereeritud tulemustes, hinnangutes ja soovitustes; kordab üleskutset liikmesriikidele edendada sellepärast diskrimineerimisvastaseid meetmeid ning arendada riiklikke tegevuskavasid rassismi vastu politseitegevuses ja kohtusüsteemis;

24. märgib, et ennetav politseitegevus kuulub õiguskaitse valdkonnas kasutatavate tehisintellekti rakenduste hulka, kuid hoiatab, et ennetava politseitegevusega saab küll analüüsida andmekogumeid mustrite ja seoste tuvastamiseks, kuid see ei suuda vastata põhjuslikkuse küsimusele ega ennustada usaldusväärselt individuaalset käitumist ning seetõttu ei tohi see olla sekkumise ainus alus; juhib tähelepanu sellele, et mitu Ameerika Ühendriikide linna on pärast auditeid lõpetanud ennetava politseitegevuse süsteemide kasutamise; tuletab meelde, et LIBE-komisjoni 2020. aasta veebruaris toimunud lähetuse ajal Ühendriikidesse teatasid New Yorgi linna ja Cambridge'i (Massachusetts) politseiosakonnad parlamendiliikmetele, et nad kaotasid järk-järgult oma ennetava politseitegevuse programmid nende vähese tõhususe, diskrimineeriva mõju ja praktilise läbikukkumise tõttu ning hakkasid selle asemel kasutama kogukondlikku politseitegevust; märgib, et see tõi kaasa kuritegevuse määrade languse; on seetõttu vastu sellele, kui õiguskaitseasutused kasutavad tehisintellekti üksikisikute või rühmade käitumise ennustamiseks, tuginedes varasematele andmetele ja varasemale käitumisele, rühma kuulumisele, asukohale või muudele sellistele omadustele, püüdes nii tuvastada isikuid, kes panevad tõenäoliselt toime kuriteo;

25. võtab teadmiseks näotuvastuse eri kasutusviisid, näiteks (kuid mitte ainult) kontrollimise/autentimise (st näo ja isikut tõendava dokumendi foto sobitamine, nt e-piirid), tuvastamise (st foto sobitamine fotode andmebaasiga) ja tuvastamise (st nägude tuvastamine reaalajas sellistest allikatest nagu videovalve stseenid ja nende sobitamine andmebaasidega, nt reaalajas jälgimine), millest igaühel on erinev mõju põhiõiguste

kaitsele; on kindlal arvamusel, et näotuvastussüsteemide kasutamine õiguskaitses peaks piirduma selgelt põhjendatud eesmärkidega, seejuures tuleb täielikult austada proportsionaalsuse ja vajalikkuse põhimõtteid ning kohaldatavat õigust; kinnitab veel kord, et näotuvastustehnoloogia kasutamine peab vastama vähemalt võimalikult väheste andmete kogumise, andmete täpsuse, säilitamispiirangute, andmete turvalisuse ja andmete eest vastutamise nõuetele, samuti olema seaduslik, õiglane, läbipaistev ja järgima konkreetset, selgesõnalist ja õiguspärast eesmärki, mis on selgelt liikmesriigi või liidu õiguses kindlaks määratud; on arvamusel, et kontrollimis- ja autentimissüsteeme saab jätkuvalt edukalt kasutusele võtta ja kasutada ainult siis, kui nende kahjulikku mõju on võimalik leevendada ja eespool nimetatud kriteeriumid on täidetud;

26. nõuab lisaks, et avalikult juurdepääsetavates kohtades keelataks automatiseeritud analüüsi kasutamine ja/või muude inimtunnuste, nagu kõnnaku, sõrmejälgede, DNA, hääle ning muude biomeetriliste ja käitumuslike signaalide tuvastamine;

27. nõuab siiski, et selliste näotuvastussüsteemide õiguskaitse eesmärgil kasutuselevõtule, mille ülesanne on tuvastada, välja arvatud juhul, kui neid kasutatakse rangelt kuriteoohvrite tuvastamiseks, kehtestataks moratoorium seni, kuni tehnilisi standardeid saab pidada täielikult põhiõigustele vastavaks, saadud tulemused ei ole kallutatud ega diskrimineerivad, õigusraamistik tagab ranged kaitsemeetmed väärkasutuse vastu ning range demokraatliku kontrolli ja järelevalve ning selliste tehnoloogiate kasutamise vajalikkuse ja proportsionaalsuse kohta on empiirilisi tõendeid; märgib, et kui eespool nimetatud kriteeriumid ei ole täidetud, ei tohiks süsteeme kasutada ega kasutusele võtta;

28. väljendab suurt muret eraõiguslike näotuvastuse andmebaaside, nagu Clearview AI (andmebaas enam kui kolme miljardi fotoga, mis on kogutud ebaseaduslikult suhtlusvõrgustikest ja mujalt internetist, sealhulgas ELi kodanike fotod) kasutamise pärast õiguskaitses tegutsejate ja luureteenistuse poolt; kutsub liikmesriike üles kohustama õiguskaitses tegutsejaid avalikustama, kas nad kasutavad Clearview AI tehnoloogiat või teiste pakkujate samalaadseid tehnoloogiaid; tuletab meelde Euroopa Andmekaitsenõukogu arvamust, et sellise teenuse nagu Clearview AI kasutamine õiguskaitseasutuste poolt Euroopa Liidus ei oleks ilmselt ELi andmekaitsekorraga kooskõlas; nõuab, et keelataks eraõiguslike näotuvastuse andmebaaside kasutamine õiguskaitses;

29. võtab teadmiseks komisjoni teostatavusuuringu Prümi otsuse[8] võimalike muudatuste kohta, sealhulgas seoses näokujutistega; võtab teadmiseks varasema uurimistöö tulemused, et ükski uus võimalik tunnus, nt iirise- või näotuvastus, ei ole kohtuekspertiisi kontekstis nii usaldusväärne kui DNA või sõrmejäljed; tuletab komisjonile meelde, et igasugune seadusandlik ettepanek peab tuginema tõenditele ja austama proportsionaalsuse põhimõtet; nõuab tungivalt, et komisjon pikendaks Prümi otsuse raamistikku ainult juhul, kui kohtuekspertiisi kontekstis on näotuvastuse usaldusväärsuse kohta võrreldes DNA või sõrmejälgedega kindlad teaduslikud tõendid, pärast täieliku mõjuhinnangu tegemist ning võttes arvesse Euroopa Andmekaitseinspektori ja Euroopa Andmekaitsenõukogu soovitusi;

[8] Nõukogu 23. juuni 2008. aasta otsus 2008/615/JSK piiriülese koostöö tõhustamise kohta, eelkõige seoses terrorismi- ja piiriülese kuritegevuse vastase võitlusega. ELT L 210, 6.8.2008, lk 1.

30. rõhutab, et biomeetriliste andmete kasutamine on laiemalt seotud inimväärikuse õiguse põhimõttega, mis on kõigi hartaga tagatud põhiõiguste alus; on seisukohal, et igasuguste biomeetriliste andmete kasutamine ja kogumine kaugtuvastuse eesmärgil, näiteks teostades avalikes kohtades näotuvastust, samuti automaatse piirikontrolli väravates, mida kasutatakse piirikontrolliks lennujaamades, võivad kujutada põhiõigustele konkreetseid ohte, mille mõju võib sõltuvalt kasutuse eesmärgist, kontekstist ja ulatusest olla väga erinev; rõhutab lisaks emotsioonituvastustehnoloogia, nagu silmade liikumist ja pupilli suuruse muutusi avastavate kaamerate vaidlustatavat teaduslikku kehtivust õiguskaitse valdkonnas; on seisukohal, et biomeetrilise tuvastamise kasutamist õiguskaitse ja kohtusüsteemi kontekstis tuleks alati pidada kõrge riskiga tegevuseks ning seetõttu tuleks selle suhtes kohaldada lisanõudeid, nagu on soovitanud komisjoni kõrgetasemeline tehisintellekti eksperdirühm;

31. väljendab suurt muret programmi „Horisont 2020“ vahenditest rahastatud teadustöö projektide pärast, mille raames kasutatakse tehisintellekti välispiiridel, nagu projekt iBorderCtrl – nutikas valedetektori süsteem, mis profileerib reisijaid arvutiga automatiseeritud intervjuu (mis on filmitud reisija veebikaameraga enne reisi algust) ja tehisintellektil põhineva 38 mikrožesti analüüsi põhjal ning mida testitakse Ungaris, Lätis ja Kreekas; kutsub seepärast komisjoni üles seadusandlike ja muude kui seadusandlike vahendite ning vajaduse korral rikkumismenetluste kaudu rakendama keeldu biomeetriliste andmete, sealhulgas näokujutiste igasugusele töötlemisele õiguskaitse eesmärkidel, mis toob kaasa massijälgimise avalikes kohtades; kutsub lisaks komisjoni üles peatama selliste biomeetriaga seotud teadusuuringute, kasutuse või programmide rahastamise, mis toovad tõenäoliselt kaasa valimatu massilise jälgimise avalikes kohtades; rõhutab sellega seoses, et erilist tähelepanu tuleks pöörata mehitamata õhusõidukite kasutamisele politseioperatsioonides ja kohaldada selle suhtes ranget raamistikku;

32. toetab soovitusi, mille on esitanud komisjoni kõrgetasemeline tehisintellekti eksperdirühm, kes pooldab tehisintellektipõhise isikute massilise hindamise keelamist; on seisukohal, et igasugune normatiivne kodanike suuremahuline hindamine avalike asutuste poolt, eriti õiguskaitse ja kohtuvaldkonnas, toob kaasa autonoomsuse kaotuse, ohustab mittediskrimineerimise põhimõtet ja seda ei saa pidada ELi õiguses kodifitseeritud põhiõigustega, eriti inimväärikusega, kooskõlas olevaks;

33. nõuab suuremat üldist läbipaistvust, et saada täielik ülevaade tehisintellekti rakenduste kasutamisest liidus; nõuab, et liikmesriigid esitaksid põhjalikku teavet vahendite kohta, mida nende õiguskaitse- ja õigusasutused kasutavad, kasutatavate vahendite liikide kohta, nende kasutamise eesmärkide kohta ja kuriteoliikide kohta, mille puhul neid kohaldatakse, ning teataksid ka need vahendid väljatöötanud ettevõtete või organisatsioonide nimed; palub, et õiguskaitse- ja õigusasutused teavitaksid ka üldsust ja annaksid piisavalt läbipaistvalt teada, kuidas nad oma pädevuse teostamisel tehisintellekti ja sellega seotud tehnoloogiat kasutavad, sealhulgas kõnealuse tehnoloogia valepositiivsete ja valenegatiivsete tulemuste määra avalikustamine; nõuab, et komisjon koguks ja ajakohastaks teavet ühes kohas; kutsub komisjoni üles avaldama ja ajakohastama ka teavet tehisintellekti kasutamise kohta õiguskaitse- ja õigusülesandeid täitvate liidu ametite poolt; palub Euroopa Andmekaitsenõukogul hinnata nende õiguskaitseasutustes ja kohtusüsteemis kasutatavate tehisintellekti tehnoloogiate ja rakenduste seaduslikkust;

34. tuletab meelde, et tehisintellekti rakendusi, sealhulgas õiguskaitse ja kohtusüsteemi kontekstis kasutatavaid rakendusi, arendatakse kogu maailmas kiire tempoga; nõuab tungivalt, et kõik Euroopa sidusrühmad, sealhulgas liikmesriigid ja komisjon, tagaksid rahvusvahelise koostöö kaudu väljaspool ELi asuvate partnerite kaasamise, et tõsta rahvusvahelisel tasandil standardeid ning leida tehisintellekti kasutamiseks, eriti õiguskaitse ja kohtusüsteemi huvides, ühine ja täiendav õigus- ja eetikaraamistik, mis järgib täielikult hartat, Euroopa andmekaitseõigustikku ja inimõigusi laiemalt;

35. nõuab, et Euroopa Liidu Põhiõiguste Amet koostaks koostöös Euroopa Andmekaitsenõukogu ja Euroopa Andmekaitseinspektoriga põhjalikud suunised, soovitused ja parimad tavad, et veelgi täpsustada õiguskaitse- ja õigusasutustes kasutatavate tehisintellekti rakenduste ja lahenduste väljatöötamise, kasutamise ja kasutuselevõtu kriteeriume ja tingimusi; kohustub viima läbi uuringu õiguskaitsedirektiivi[9] rakendamise kohta, et teha kindlaks, kuidas on tagatud isikuandmete kaitse õiguskaitse- ja õigusasutuste töötlemistoimingutes, eelkõige uute tehnoloogiate väljatöötamisel või kasutuselevõtmisel; kutsub lisaks komisjoni üles kaaluma, kas õiguskaitse- ja õigusasutuste poolt tehisintellekti rakenduste ja lahenduste väljatöötamise, kasutamise ja kasutuselevõtu kriteeriumide ja tingimuste edasiseks täpsustamiseks on vaja konkreetseid seadusandlikke meetmeid;

36. teeb presidendile ülesandeks edastada käesolev resolutsioon nõukogule ja komisjonile.

[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.

SELETUSKIRI

Tehisintellekt on üks 21. sajandi strateegilisi tehnoloogiaid, millega kaasnevad märkimisväärsed eelised tõhususe, täpsuse ja mugavuse osas ning mis seega edendab Euroopa majandust. Tehisintellekti rakendused on muu hulgas parandanud tervishoiuteenuste kvaliteeti, suurendanud põllumajanduse tõhusust, aidanud kaasa kliimamuutuste leevendamisele ja nendega kohanemisele ning tõhustanud tootmist.

Tehisintellekt on komisjoni praeguse koosseisu üks peamisi prioriteete. Komisjoni president Ursula von der Leyen teatas oma poliitilistes suunistes, et kavas on välja töötada tehisintellekti inim- ja eetilise mõju üleeuroopaline kooskõlastatud käsitusviis ja algatada mõttetalgud, mille teema on suurandmete parem kasutamine innovatsiooni edendamiseks. Tehisintellekti ELi tasandi küsimusena tõstatamisega paralleelselt on kaasnenud arutelu selle üle, kuidas tagada usaldus tehisintellekti tehnoloogiate vastu, ja kuidas tagada, et need tehnoloogiad ei ohusta ELi põhiõigusi.

Euroopa Parlament on tehisintellekti küsimusega tegelenud mitu aastat enne seda, kui komisjon otsustas selle prioriteediks muuta. Mitmed resolutsioonid, mis Euroopa Parlament on alates 2016. aastast suurandmete, robootika ja tehisintellekti teemal vastu võtnud, näitavad, kui tähtsaks parlament seda teemat peab. Resolutsioonides on vaadeldud tehisintellekti erinevaid mõjusid ning seda, kuidas see mõjutab heaolu, haridust, tehnoloogiat, seaduslikke ja põhiõigusi ning tööstust üldiselt. Nendes resolutsioonides on rõhutatud vajadust võtta vastu nn inimkeskne lähenemisviis, mis põhineb põhiõiguste austamisel, konkreetsemalt ELi põhiõiguste hartal ja andmekaitseraamistikul.

Tehisintellekt ühendab „tehnoloogialiike, milles põimuvad andmed, algoritmid ja andmetöötlusvõimsus“ ning seega on „praeguse kasvuspurdi taga ennekõike andmete töötlemise alal tehtud edusammud ja nende üha suurem kättesaadavus“[1]. Tehisintellekti keskmes on asjaolu, et see põhineb eri allikatest pärit suurte andmekogumite, k.a isikuandmete kogumisel, analüüsil ja pideval koondamisel , mille puhul andmeid töödeldakse automaatselt arvutialgoritmide ja täiustatud andmetöötlusvahenditega. Need meetodid kasutavad nii salvestatud kui ka voona edastatavaid andmeid, et teha kindlaks teatavaid korrelatsioone, suundumusi ja mudeleid (suurandmete analüüs). Tehisintellekti jaoks kasutatavad andmed ei ole pärit mitte ainult üksikisikutelt endilt; tehisintellekti rakendused kasutavad enamasti tööstusest, äritegevusest ja avalikust sektorist pärit andmeid, mida töödeldakse erinevatel eesmärkidel. Isegi kui tehisintellekti rakenduste kasutatavad andmed võivad mõnikord olla isikustamata, hõlmavad tehisintellektiga seotud toimingud sageli isikuandmete töötlemist, millega kaasnevad automatiseeritud otsused, mis üksikisikuid otseselt mõjutavad. Seetõttu nõuavad tehisintellekti sellised omadused, et selles valdkonnas pööratakse erilist tähelepanu andmekaitset ja eraelu puutumatust käsitlevate aluspõhimõtete austamisele.

Tehisintellekt pakub suurepäraseid võimalusi ka õiguskaitse ja kriminaalõiguse valdkonnas, eelkõige õiguskaitse- ja kohtuasutuste töömeetodite parandamisel ning teatud liiki kuritegude, eriti finantskuritegude, rahapesu ja terrorismi rahastamise ning teatavat liiki küberkuritegude vastase võitluse tõhustamisel. Selles sektoris hõlmavad tehisintellekti rakendused selliseid tehnoloogiaid, nagu näotuvastus, numbrimärgi automaattuvastus, kõneleja tuvastus, huultelt

[1] COM(2020) 65 final.

lugemise tehnoloogia, pealtkuulamine (st lasutuvastusalgoritmid), autonoomne otsing identifitseeritavates andmebaasides ja selliste andmebaaside analüüs, prognoosimine (ennetav politseitegevus ja kuriteopaiga analüüs), käitumise tuvastamise vahendid, autonoomsed vahendid finantspettuse ja terrorismi rahastamise kindlakstegemiseks, sotsiaalmeedia seire (andmekoorimine ja -kogumine seoste kindlakstegemiseks), helistaja rahvusvahelise mobiilside tunnuse püüdurid (IMSI-püüdurid), ning eri tuvastamisvõimalusi hõlmavad automatiseeritud seiresüsteemid (näiteks südamelöökide tuvastamine ja soojuskaamerad. Kohtuasutustes võidakse tehisintellekti vahendeid kasutada uue õigusrikkumise tõenäosuse arvutamisel ja katseaja määramisel või karistuse määramise üle otsustamisel.

Vaatamata tehisintellektist saadavale kasule on tõsiasi, et tehisintellekti kasutamisega kaasnevad mitmed võimalikud ohud, nagu läbipaistmatu otsuste tegemine, eri liiki diskrimineerimine, eraellu sekkumine, isikuandmete kaitsega seotud probleemid, inimväärikuse ning sõna- ja teabevabaduse rikkumine. Need võimalikud ohud süvenevad õiguskaitse- ja kriminaalõiguse sektoris, sest nad võivad mõjutada süütuse presumptsiooni, üksikisiku vabaduse ja turvalisuse põhiõigust ning tõkestada tõhusa õiguskaitsevahendi kasutamist ja õiglast kohtumõistmist.

Käesolevas raportis püütakse käsitleda küsimusi, mis on seotud tehisintellekti kasutamisega kriminaalõiguses ning selle politsei ja kohtuasutuste poolt kriminaalasjades kasutamisega. Tunnistades tehisintellektist tulenevaid võimalusi ja eeliseid, rõhutatakse selles ka kaasnevaid võimalikke olulisi ohte ja kahjusid.

Raportis rõhutatakse vajadust täielikult austada põhiõigusi, mis on sätestatud ELi põhiõiguste hartas, liidu eraelu ja andmekaitse seaduses, nimelt direktiivis (EL) 2016/680 (politseidirektiiv), ning vajadust rakendada tehisintellekti elutsükli jooksul mitmeid aluspõhimõtteid nagu algoritmide selgitused ja läbipaistvus, jälgitavus, kohustuslik põhiõigustele avaldatava mõju hindamine enne mis tahes tehisintellekti süsteemi rakendamist või kasutuselevõttu ning kohustuslikud auditid. Kõik need nõuded ei ole vajalikud mitte ainult selleks, et tagada tehisintellekti süsteemide õiguspärasus, vaid ka selleks, et saavutada üksikisikute usaldus nende kasutamise suhtes õiguskaitse- ja kohtuasutustes.

Viimasena kutsub raportöör üles kehtestama moratooriumi näotuvastussüsteemide kasutuselevõtmisele õiguskaitse eesmärgil. Nende tehnoloogiate praegune olukord, märkimisväärne mõju põhiõigustele nõuab põhjalikku ja avatud ühiskondlikku arutelu, et kaaluda mitmesuguseid tõstatatud küsimusi ja tehnoloogiate rakendamise põhjendusi.

3.9.2020

SISETURU- JA TARBIJAKAITSEKOMISJONI ARVAMUS

kodanikuvabaduste, justiits- ja siseasjade komisjonile

tehisintellekti kohta kriminaalõiguses ning tehisintellekti politsei- ja õigusasutuste poolt kriminaalasjades kasutamise kohta
(2020/2016(INI))

Arvamuse koostaja: Marcel Kolaja

ETTEPANEKUD

Siseturu- ja tarbijakaitsekomisjon palub vastutaval kodanikuvabaduste, justiits- ja siseasjade komisjonil lisada oma resolutsiooni ettepanekusse järgmised ettepanekud:

A. arvestades, et kui pidada silmas nii tehisintellekti positiivset ühiskondlikku potentsiaali kui ka olemuslikke riske, tuleks digitaalse ühtse turu toimimist parandada, suurendades selleks tehisintellekti pakkujate õiguskindlust ning ka tarbijate usaldust ja turvalisust, ning selleks tuleb tugevdada kaitsemeetmeid, et tagada õigusriik ja põhiõiguste austamine, eelkõige õigus eraelu puutumatusele ja isikuandmete kaitsele, õigus võrdsusele ja mittediskrimineerimisele, õigus heale haldusele, õigus õiglasele kohtumenetlusele ja õigus kõrgetasemelisele tarbijakaitsele; arvestades, et ühtse turu killustatuse vältimiseks on Euroopal vaja tehisintellekti ühist käsitust ja reguleerimist selle kasutamiseks kriminaalasjades politsei- ja õiguskaitseasutuste poolt;

B. arvestades, et tehisintellekti katsetamine ja kasutamine politsei- ja õigusasutuste poolt mitmesugustel kasutusaladel koos kõigi tagajärgede ja ohtudega, mida see endaga kaasa toob, on laialt levinud, olgu selleks näotuvastussüsteemid, DNA profileerimine, kuritegevuse ennetav kaardistamine ja mobiiltelefonide andmete väljavõtmine, kõrgetasemelised kohtupraktika otsingumootorid, vaidluste veebipõhine lahendamine või masinõpe õigusemõistmiseks;

C. arvestades, et tehisintellekti kasutamine võib tekitada kriminaalasjades õigusemõistmises paradigma muutuse;

D. arvestades, et Euroopa Liidu Põhiõiguste Ameti aruande kohaselt on näotuvastustehnoloogiate võimaliku kasutamise või katsetamise kohta liikmesriikides

praegu saadaval ainult piiratud hulgal teavet[1];

E. arvestades, et andmekaitseasutused leidsid, et nendes liikmesriikides, kus oli näotuvastustehnoloogiate kasutamise kohta mõnevõrra teavet, ei vastanud nende tehnoloogiate kasutamine andmekaitsealastele õigusaktidele ja nende kasutuselevõtuks puudus õiguslik alus;

F. arvestades, et siseturu valdkonnas võib liit olukorda oluliselt muuta riigihankemenetluste reformimise teel, viies valitsuste tegevuse ja käitumise kooskõlla teiseste poliitikaeesmärkidega, nagu andmekaitse ja mittediskrimineerimine;

G. arvestades, et projekteerimis-, katse- ja rakendusetapis võib andmetel põhinevate algoritmipõhiste otsuste tegemisel esineda diskrimineerimist andmekogumites või algoritmides sisalduva kallutatuse tõttu;

H. arvestades, et tehisintellekti tehniline arendamine ja rakendamine peab olema põhimõtetest lähtuv, et tagada inim- ja põhiõiguste järgimine;

I. arvestades, et Euroopa Nõukogu kohtute efektiivsust hindav komisjon avaldas 4. detsembril 2018 eetilise harta tehisintellekti kasutamise kohta kohtusüsteemides ning selles on esitatud eetilised põhimõtted tehisintellekti kasutamiseks kohtusüsteemides;

J. arvestades, et tehisintellekti tehnoloogiate teatavad kasutusviisid on eriti tundlikud ja neid võidakse kuritarvitada ning et mõned tehnoloogiaettevõtted on seetõttu hiljuti otsustanud lõpetada sellega seotud tarkvara pakkumise;

1. on seisukohal, et kuna politsei- ja õigusasutuste ülesanne on kaitsta avalikke huve ja pidades silmas nende ülesannete iseloomu, tuleb nende asutuste kasutatav tehisintellekt liigitada üldiselt suure riskiga tehisintellektiks ning seda tuleb kohelda äärmiselt hoolikalt ja vastavalt kõrgeimatele andmekaitsestandarditele; on seisukohal, et siseturul on tehisintellekti jaoks kiiresti vaja ühtset Euroopa õigusraamistikku; on seisukohal, et EL peaks tehisintellekti arendamise ja kasutamise valdkonnas võtma juhtrolli liidu tasandi õigusnormide kehtestamiseks, sealhulgas avalike hangete kohta, ning need peaksid põhinema selgetel eeskirjadel ning põhiõigustel ja eetikal, mis võimaldaks tagada kogu ELis ühesuguse tarbijakaitse kõrge taseme ja ühtsed tööstusstandardid, et võimaldada siseturu paremat toimimist ning soodustada ühtlasi innovatsiooni ja edendada ettevõtjate, eelkõige VKEde õiguskindlust; kutsub komisjoni üles enne võimalike uute seadusandlike ettepanekute algatamist kontrollima kehtivate õigusaktide kohaldamist ja nende täitmise tagamist;

2. tunnistab, et tehisintellekti kasutamine õigusvaldkonnas võib aidata parandada menetluste tõhusust ja kvaliteeti; rõhutab sellega seoses, et eelkõige on vaja järgida õigusnorme, mis on sätestatud Euroopa inimõiguste ja põhivabaduste kaitse konventsioonis ning Euroopa Nõukogu konventsioonis üksikisikute kaitse kohta isikuandmete automatiseeritud töötlemisel;

[1] Euroopa Liidu Põhiõiguste Amet: „Facial recognition technology: fundamental rights considerations in the context of law enforcement“, (FRA Focus), 27. november 2019 – https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf

3. kutsub komisjoni üles turul saadaolevat tehisintellekti tehnoloogiat ning selle kasutamise taset politsei- ja õigusasutuste poolt riikide kaupa hindama;

4. rõhutab, et tehisintellekt peaks aitama vähendada avaliku sektori asutuste halduskoormust ja suurendama nende otsustusprotsessi tõhusust ning et tehisintellekti süsteemid peaksid alati tuginema inimjärelevalvele, -koostööle ja -koordineerimisele; toonitab sellega seoses, et lõplikku vastutust mis tahes otsuste tegemise eest kriminaalasjades peaksid alati kandma inimesed; rõhutab täpsete andmekogumite tähtsust, kui neid kasutatakse seonduvate e-valitsuse protsesside ja haldusotsuste tegemise hõlbustamiseks kogu liidus;

5. rõhutab innovatsiooni, läbipaistvuse, jälgitavuse ja kontrollimise võimaldamise tähtsust; rõhutab, et avatud lähtekoodiga tehisintellekt võib sellele kaasa aidata ning tugevdada ühtlasi ka koostööd ja edendada algoritmide kasutamise ja loomisega seotud ideede ja kogemuste vahetamise kultuuri;

6. on seisukohal, et politsei ja õiguskaitseasutuste poolt kriminaalasjades kasutatav tehisintellekt tuleks riigihankemenetluse raames võimaluse korral avaldada avatud lähtekoodiga tarkvarana kooskõlas kohaldatavate õigusaktidega, sealhulgas Euroopa Parlamendi ja nõukogu 17. aprilli 2019. aasta direktiiviga (EL) 2019/790, mis käsitleb autoriõigust ja autoriõigusega kaasnevaid õigusi digitaalsel ühtsel turul, kusjuures tarkvara dokumentatsioon ja algoritmid peaksid olema kättesaadavad, võimaldades seega pädevatel asutustel kontrollida, kuidas tehisintellekti süsteem teatavale järeldusele jõudis; rõhutab, et põhiõiguste audit peaks olema osa nõuetelevastavuse eelhindamisest; on arvamusel, et selgitatavad ja erapooletud algoritmid, mis vastavad piisava läbipaistvuse kohustusele, ning avaandmete kasutamine koolituseks kooskõlas kohaldatavate õigusaktidega, sealhulgas direktiiviga (EL) 2019/1024 avaandmete ja avaliku sektori valduses oleva teabe taaskasutamise kohta, ilma et see piiraks määrust (EL) 2016/679, on ELi õiguse ja väärtuste ning kohaldatavate andmekaitsenormide austamist tagades ning ilma uurimist või kriminaalvastutusele võtmist ohtu seadmata olulised tagamaks, et ettevõtjad ja kodanikud, sealhulgas tarbijad, saavad usaldada ja kasutada paremaid, juurdepääsetavaid, mittediskrimineerivaid ja usaldusväärseid avalikke teenuseid õiglaste kuludega;

7. rõhutab, et tehisintellektil põhinev andmete kogumine ja üksikisikute jälgimine peaks piirduma kuriteos kahtlustatavatega ja kohtu poolt heaks kiidetud jälgimisega kooskõlas kohaldatavate siseriiklike õigusaktidega, võttes arvesse eraelu austamist ja süütuse presumptsiooni, sealhulgas ka teiste kasutajate ja tarbijate puhul, keda sellised süsteemid ja tavad võivad tahtmatult mõjutada; rõhutab, et kui otsuste tegemisele aitavad kaasa statistilised arvutused, peaksid asjakohane kutsealane koolitus ja kvalifikatsioon tagama, et otsustajatele õpetatakse kallutatuse võimalikkust, sest andmekogumid võivad põhineda diskrimineerivatel ja eelarvamuslikel andmetel; rõhutab sellega seoses algoritmide ja algandmete kvaliteedi tähtsust ning tuletab meelde, et tehisintellekti kasutamine andmete sisestamisel ja analüüsimisel peab põhinema mittediskrimineerimise põhimõttel; nõuab, et selliste rakenduste hankemenetlused sisaldaksid kaitsemeetmeid võimaliku kallutatuse vastu; nõuab, et liikmesriikide õigus- ja politseiasutused vahetaksid tehisintellekti tehnoloogiate ja vahendite rakendamise kohta teavet ja parimaid tavasid, et vältida ühtsel turul killustunud käsitust ning tagada tarbijate ja kodanike kaitse kogu liidus;

8. rõhutab, et liikmesriigid peaksid kooskõlas kohaldatava kriminaalõigusega tagama, et kodanikke ja tarbijaid teavitatakse sellest, kui nendega seotud juhul kasutatakse tehisintellekti, ning et kodanikele tuleks teha kättesaadavaks lihtsad, tõhusad ja kergesti juurdepääsetavad kaebuste ja kahjuhüvitusnõuete menetlused, sealhulgas õiguskaitsevahendid, et nad saaksid oma õigusi tõhusalt kaitsta;

9. tuletab meelde, et teatavat liiki tehisintellekt, sealhulgas näotuvastustehnoloogiate kasutamine avalikus ruumis, automatiseeritud käitumise avastamine ja profiilianalüüs, mille põhjal inimesed jagatakse piiridel riskikategooriatesse, biomeetriline tuvastamine ja äratundmine massilise jälgimise eesmärgil, kodanike massiline hindamine ja ennetav politseitegevus, on kõrge riskiga ning kutsub komisjoni kuritarvitamise ohu kõrvaldamiseks üles nende hankeid ja kasutamist reguleerima; peab sellega seoses tervitatavaks komisjoni käimasolevat tööd biomeetriliste tehnoloogiate kasutamise hindamisel ja regulatiivsete võimaluste kaalumisel, sealhulgas riskipõhist käsitlust ja nende keelustamist konkreetsetel asjaoludel ning vajalike kaitsemeetmete kehtestamist, kui nende kasutamine on õigustatud;

10. toonitab, et üksnes statistilistel arvutustel põhinevate otsuste standardimise ärahoidmiseks tuleb säilitada kohtunike suveräänne kaalutlusõigus ja juhtumipõhine otsustamine.

TEAVE VASTUVÕTMISE KOHTA
NÕUANDVAS KOMISJONIS

Vastuvõtmise kuupäev	3.9.2020
Lõpphääletuse tulemus	+: 40 –: 4 0: 0
Lõpphääletuse ajal kohal olnud liikmed	Alex Agius Saliba, Andrus Ansip, Alessandra Basso, Brando Benifei, Adam Bielan, Hynek Blaško, Biljana Borzan, Vlad-Marius Botoş, Markus Buchheit, Dita Charanzová, Deirdre Clune, David Cormand, Petra De Sutter, Carlo Fidanza, Evelyne Gebhardt, Sandro Gozi, Maria Grapini, Svenja Hahn, Virginie Joron, Eugen Jurzyca, Arba Kokalari, Marcel Kolaja, Kateřina Konečná, Andrey Kovatchev, Jean-Lin Lacapelle, Maria-Manuel Leitão-Marques, Morten Løkkegaard, Adriana Maldonado López, Antonius Manders, Beata Mazurek, Leszek Miller, Dan-Ştefan Motreanu, Kris Peeters, Anne-Sophie Pelletier, Christel Schaldemose, Andreas Schwab, Tomislav Sokol, Ivan Štefanec, Kim Van Sparrentak, Marion Walsmann, Marco Zullo
Lõpphääletuse ajal kohal olnud asendusliikmed	Maria da Graça Carvalho, Anna Cavazzini, Krzysztof Hetman

NIMELINE LÕPPHÄÄLETUS
NÕUANDVAS KOMISJONIS

40	+
PPE	Maria da Graça Carvalho, Deirdre Clune, Krzysztof Hetman, Arba Kokalari, Andrey Kovatchev, Antonius Manders, Dan-Ştefan Motreanu, Kris Peeters, Andreas Schwab, Tomislav Sokol, Ivan Štefanec, Marion Walsmann
S&D	Alex Agius Saliba, Brando Benifei, Biljana Borzan, Evelyne Gebhardt, Maria Grapini, Maria-Manuel Leitão-Marques, Adriana Maldonado López, Leszek Miller, Christel Schaldemose
RENEW	Andrus Ansip, Vlad-Marius Botoş, Dita Charanzová, Sandro Gozi, Svenja Hahn, Morten Løkkegaard
ID	Hynek Blaško
VERTS/ALE	Anna Cavazzini, David Cormand, Petra De Sutter, Marcel Kolaja, Kim Van Sparrentak
ECR	Adam Bielan, Carlo Fidanza, Eugen Jurzyca, Beata Mazurek
EUL/NGL	Kateřina Konečná, Anne-Sophie Pelletier
NI	Marco Zullo

4	-
ID	Alessandra Basso, Markus Buchheit, Virginie Joron, Jean-Lin Lacapelle

0	0

Kasutatud tähised:
+ : poolt
- : vastu
0 : erapooletu

15.9.2020

ÕIGUSKOMISJONI ARVAMUS

kodanikuvabaduste, justiits- ja siseasjade komisjonile

tehisintellekti kohta kriminaalõiguses ning tehisintellekti politsei- ja õigusasutuste poolt kriminaalasjades kasutamise kohta
(2020/2016(INI))

Arvamuse koostaja: Angel Dzhambazki

ETTEPANEKUD

Õiguskomisjon palub vastutaval kodanikuvabaduste, justiits- ja siseasjade komisjonil lisada oma resolutsiooni ettepanekusse järgmised ettepanekud:

A. arvestades, et õigus õiglasele kohtumenetlusele on õiguslikult siduv põhiõigus, mis on jõustamise eesmärgil sätestatud Euroopa Liidu põhiõiguste hartas ning inimõiguste ja põhivabaduste kaitse konventsioonis; arvestades, et seda kohaldatakse kogu kriminaalmenetluse kestel, sealhulgas õiguskaitses, ning selle kaitse välistab menetluse kõigis etappides selliste meetmete, sealhulgas tehniliste meetmete võtmise, mille otsene või kaudne tagajärg on kaitseõiguste sisuline tühistamine; arvestades, et selle põhimõttega seotud tagatised, eelkõige kohtu sõltumatus, võrdsus seaduse ees ja süütuse presumptsioon, on kriminaalõiguse valdkonnas rangemad; arvestades, et neid õigusi tuleb järgida igas olukorras, eelkõige tehisintellekti kasutamisel, eriti seetõttu, et tehisintellektil põhinevad tehnoloogiad võivad mõjutada eri inimõigusi;

B. arvestades, et isikuandmete kaitset kohaldatakse alati kooskõlas isikuandmete kaitse üldmäärusega[1] ja vajaduse korral muude asjakohaste õigusaktidega;

C. arvestades, et tehisintellekt ja seonduvad tehnoloogiad, sealhulgas nende iseõppimisvõime, hõlmavad alati mingil määral inimsekkumist;

D. arvestades, et tehisintellektist võib saada kriminaalõigussüsteemide püsiv osa;

E. arvestades, et tehisintellekt ja seonduvad tehnoloogiad on liidu jaoks esmatähtsad, arvestades tehnoloogiasektori kiiret arengut ja seda, kui tähtis on hoolikalt jälgida nende praegust ja tulevast mõju Euroopa ainulaadsele intellektuaalomandi õiguste süsteemile;

[1] 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 (ELT L 119, 4.5.2016, lk 1).

arvestades, et paljudes sektorites, näiteks robootika-, transpordi- ja tervishoiusektoris, rakendatakse juba praegu tehisintellekti ja seonduvaid tehnoloogiaid;

F. arvestades, et tehisintellekti ja seonduvaid tehnoloogiaid saaks kasutada kriminaalõiguses selleks, et alandada kuritegevuse taset ning kasutada neid teatavate menetluste lihtsustamiseks kuritegevuse analüüsimise ja tõkestamise eesmärgil statistilise analüüsi kasutamisel, samuti kuritegude avastamisel ja uurimisel; arvestades, et andmekaitse ja eraelu puutumatusega seotud puudujääkide leevendamiseks peaks liit edasi arendama oma tarkvara, andmesalvestuse ja tehisintellektitehnoloogiate alast suutlikkust;

G. arvestades, et nende tehnoloogiate abil saab luua anonüümseid statistilisi andmebaase, mis aitavad ametiasutustel, teadlastel ja seadusandjatel arvandmeid analüüsida ja tõhusalt kujundada meetmeid, mille toel kuritegevust tõkestada ja õigusrikkujaid edukalt ühiskonda tagasi tuua;

H. arvestades, et tehisintellekti õigusraamistik ja selle kohaldamine kriminaalõiguses peaks vajaduse korral hõlmama seadusandlikke meetmeid, alates kohustuslikest meetmetest selliste tavade ärahoidmiseks, mis kindlasti kahjustaksid põhiõigusi ja -vabadusi;

I. arvestades, et tehisintellektisüsteemidele olemuslikult omase läbipaistmatuse tõttu võivad kriminaalõiguses kasutatavad uued vahendid minna vastuollu mõnede põhivabadustega;

J. arvestades, et kriminaalmenetlustes kahtlustatavate ja süüdistatavate isikute põhiõiguste kaitseks tuleb kriminaalõiguse küsimustes tehisintellektisüsteemide rakendamisega kaasneda võivaid riske ennetada ja leevendada;

1. rõhutab, kui tähtis on nõuetekohaselt hinnata selliseid tehisintellektisüsteemide kasutamisega seotud riske nagu diskrimineerimine ja eraelu puutumatuse rikkumine, ning võtta arvesse tehisintellekti ja seonduvate tehnoloogiate meie ühiskonnas kasutamise kõiki eetilisi ja operatiivseid tagajärgi, eelkõige nende kasutamisel riigiasutuste, politsei- ja kohtuasutuste poolt kriminaalõiguse süsteemides; see puudutab ka vastutus- ja tõendamisküsimusi tehisintellekti süsteemide toimimisega seotud võimalike vigade korral; on seisukohal, et piirangute kehtestamiseks ja vajalike kaitsemeetmete tagamiseks on vaja selget õigusraamistikku; on seisukohal, et avaliku ja erasektori üksused, kes vastutavad tehisintellekti vahendite ja teenuste esialgse kavandamise ja arendamise eest, peaksid võtma arvesse ja järgima eetikapõhimõtteid, näiteks neid, mis on sätestatud Euroopa Nõukogu Euroopa eetikahartas tehisintellekti kasutamise kohta kohtusüsteemides ja nende keskkonnas, nii et ühiskonna kõik sidusrühmad omaksid põhjalikku teavet tehisintellekti programme tootvate ettevõtete struktuuri kohta; rõhutab, kui oluline on inimtegur, mis peab alati olema lõplik otsustaja tehisintellektitehnoloogial põhineva tarkvara kasutamisel ja kriminaalsüsteemis, nii politseitöös kui ka kriminaalõiguses; kinnitab, et biomeetrilise tuvastamise tarkvara tuleks kasutada ainult seal, kus see on selgelt õigustatud;

2. rõhutab vajadust luua ja säilitada tasakaal tehisintellektisüsteemide kriminaalmenetluses kasutamise ning kõigi Euroopa ja rahvusvahelises õiguses sätestatud põhiõiguste ja menetluslike tagatiste järgimise vahel;

3. rõhutab, kui tähtis on tehisintellekti kasutamisel nõuetekohaselt järgida õigusriigi ning kohtuotsuste sõltumatuse põhimõtteid;

4. kutsub komisjoni üles veelgi täpsustama tehisintellekti ja seonduvate tehnoloogiate abil kogutud andmete, sealhulgas üksikisikute otsest või kaudset tuvastamist võimaldavate isikustamata ja anonüümseks muudetud andmete kaitset ja jagamist käsitlevaid eeskirju, järgides täielikult isikuandmete kaitse üldmäärust ja e-privaatsuse direktiivi[2]; toonitab lisaks, et õigus õiglasele kohtumenetlusele peaks hõlmama kodanike ja menetlusosaliste õigust pääseda juurde nendele andmetele, eriti kui neid kogutakse (kooskõlas isikuandmete kaitse üldmäärusega) nende isiklikest seadmetest või varustusest, samuti nende kaitseõiguse eesmärgil niipea, kui nad on juriidiliselt vastutavad;

5. rõhutab, kui tähtis on suurendada kriminaalõiguses kasutatavate tehisintellektisüsteemide läbipaistvust, et võimaldada kohtulikku järelevalvet ning tagada, et tehisintellekti ja seonduvate tehnoloogiate arendajad tagaksid pädevate asutuste ja kodanike huvides algoritmide ja algoritmipõhiste otsuste piisava läbipaistvuse; rõhutab osapoolte üldist õigust pääseda juurde protsessidele, mis on seotud andmete kogumisega, kuritegevuse ennetamiseks kasutatavate prognoosidega, kriminaaltõendite kataloogimise ja hindamisega ning selle kindlakstegemisega, kas kahtlustatav võib olla ühiskonnale ohtlik, kui seda ei piirata kehtiva ELi õigusega, näiteks direktiiviga (EL) 2016/680[3]; lisaks rõhutab, et tähtis on tehisintellektipõhiste või tehisintellekti toel saadud tulemuste kättesaadavus, võimalus määratleda, kes vastutab teavitamismenetluste eest, ning võimalus määratleda tehisintellekti ja seonduvate tehnoloogiate roll kriminaalasjades, eelkõige seoses suurte tõendimahtude analüüsimisega kriminaaluurimisel ning kahtlusaluste või kuriteoohvrite kindlakstegemisega; tuletab meelde, kui olulised on küsimused, mis on seotud tehisintellekti ja seonduvate tehnoloogiate juhtimise, põhiõiguste ja menetluslike tagatiste, mittediskrimineerimise, vastutuse, läbipaistvuse, erapooletuse, õigluse ja intellektuaalse terviklikkusega, ning rõhutab vajadust tagada seejuures pidev inimkontroll; nõuab, et kohtuasutusi tuleb kohustada põhjendama oma otsuseid, ka juhul, kui nad kasutavad tehisintellektil põhineva tehnoloogia abil saadud tõendeid, mis nõuavad kõrgetasemelist kohtulikku kontrolli ja rangeid vastuvõetavuskriteeriume vastavalt Euroopa Parlamendi 16. veebruari 2017. aasta resolutsioonile robootika kohta[4], milles rõhutatakse, et alati peaks olema võimalik esitada kõigi selliste tehisintellekti abil tehtud otsuse põhjendused, mis võivad mõjutada ühe või mitme inimese elu; tuletab meelde, et tehisintellekti ja seonduvate tehnoloogiate kasutamine kuritegude tõkestamisel erineb nende kasutamisest kriminaalõiguses; rõhutab, et tehisintellektitehnoloogiatel peab alati olema alluv roll;

6. tuletab meelde, et tehisintellekti ja seonduvate tehnoloogiate kõige tõsisemaid väärkasutamisi, nagu massiline jälgimine, profiilide koostamine ja prognoosivad

---

[2] Euroopa Parlamendi ja nõukogu 12. juuli 2002. aasta direktiiv 2002/58/EÜ, milles käsitletakse isikuandmete töötlemist ja eraelu puutumatuse kaitset elektroonilise side sektoris (EÜT L 201, 31.7.2002, lk 37).

[3] 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 (ELT L 119, 4.5.2016, lk 89).

[4] Euroopa Parlamendi 16. veebruari 2017. aasta resolutsioon soovitustega komisjonile robootikat käsitlevate tsiviilõiguse normide kohta (ELT C 252, 18.7.2018, lk 239).

politseiprogrammid, mille abil saaks hinnata kuriteo tõenäolist toimumiskohta, kahtlustatavate tõenäolist asukohta, isiku ohvristamise, ohustatuse, teadmata kadunuks jäämise või koduvägivalla või seksuaalkuriteo ohvriks või toimepanijaks olemise tõenäosust, ning nõuetekohaste menetlusõiguste rikkumisi, võivad toime panna õiguskaitseasutused;

7. rõhutab, kui oluline on kasutada tõendite kogumisel ja analüüsimisel ise genereeritud andmeid; tuletab meelde, et nii kriminaalpreventsioonis kui ka kriminaalõiguses võivad andmesisestuse ja -väljundi analüüsi vead või võimalik väärkasutamine ning selle tõlgendamine tuleneda inimtegurist, ning nõuab seetõttu kõigis otsustusprotsessides tehisintellektitehnoloogiate kasutamise tulemuslikkuse ja sobivuse analüüsimisel ettevaatlikku lähenemist;

8. kutsub kõiki pädevaid avaliku sektori asutusi, eriti selliseid õiguskaitseasutusi nagu politsei ja kohtuasutused, ja eelkõige kriminaalõiguslikes küsimustes, üles teavitama üldsust sellest, kuidas nad oma pädevuse teostamisel tehisintellekti ja seonduvaid tehnoloogiaid kasutavad, ning kasutama neid piisavalt läbipaistvalt;

9. peab väga tähtsaks, et kriminaalmenetlustes tehisintellektisüsteemide kasutamisel oleks tagatud selliste kriminaalmenetluse aluspõhimõtete järgimine nagu näiteks õigus õiglasele kohtumenetlusele, süütuse presumptsioon ja õigus tõhusale õiguskaitsevahendile, ning tagataks automatiseeritud otsustusprotsesside järelevalve ja sõltumatu kontroll;

10. rõhutab, kui tähtis on inimjuhtimise põhimõte ning tehisintellekti poolt või selle abil loodud väljundite kontrollimine; tuletab meelde, kui tähtsad on põhiõiguste austamise tagamiseks ja tehisintellekti võimalike vigade ärahoidmiseks juhtimise, läbipaistvuse, selgitatavuse ja aruandlusega seotud küsimused;

11. rõhutab oma ettevaatlikku lähenemist biomeetrilise tuvastamise tarkvara kasutamisele; juhib tähelepanu andmekaitsele olemuslikult omasest ebapiisavusest tingitud vääritimõistmistele ja isikuandmete kaitse nõuete rikkumistele; märgib murega, et välisriigid koondavad erasektori arendajate ja teenusepakkujate kaudu Euroopa Liidu kodanike isikuandmeid;

12. tuletab meelde, et vastavalt praegustele ELi andmekaitsenormidele ja Euroopa Liidu põhiõiguste hartale võib tehisintellekti kasutada biomeetriliseks tuvastamiseks ainult juhul, kui selline kasutamine on nõuetekohaselt põhjendatud ja proportsionaalne ning kohaldatakse piisavaid kaitsemeetmeid; kiidab heaks komisjoni kõrgetasemelise tehisintellekti eksperdirühma soovitused biomeetrilise tuvastuse tehnoloogia proportsionaalseks, kaalutletud ja riskipõhiseks kasutamiseks kooskõlas isikuandmete kaitse alaste õigusaktidega; teeb ettepaneku, et sellise tehnoloogia kasutamine peab olema kehtivate seaduste alusel selgelt põhjendatud ning et komisjon hindaks, kuidas neid soovitusi tõhusalt integreerida, pidades eriti silmas õigust eraelu puutumatusele ja isikuandmete kaitset;

13. on kindlalt veendunud, et tehisintellekti või seonduvate tehnoloogiate kaudu tehtud otsused, eriti kohtu- ja õiguskaitsevaldkonnas, millel on otsene ja märkimisväärne mõju füüsiliste või juriidiliste isikute õigustele ja kohustustele, peaksid alluma rangele inimkontrollile ja nõuetekohasele menetlusele;

14. peab vajalikuks analüüsida, kas on otstarbekas õiguskaitsealaste otsuste tegemist osaliselt tehisintellektile delegeerida, ning kui jah, siis millistel tingimustel ja mis osas võiks tehisintellekti sellist kasutamist lubada; on seisukohal, et avalike asutuste otsuseid asendada suutvat tehisintellekti ja seonduvaid tehnoloogiaid tuleks käsitleda äärmise ettevaatusega; rõhutab vajadust töötada välja tehisintellekti kavandamise ja kasutamise ranged eetikapõhimõtted ja spetsiaalsed tegevusjuhendid õiguskaitse- ja kohtuasutuste abistamiseks juhtudel, kui õiguskaitsealaste otsuste tegemine delegeeritakse tehisintellektile; viitab õiguskomisjonis käimasolevale tööle.

TEAVE VASTUVÕTMISE KOHTA NÕUANDVAS KOMISJONIS

Vastuvõtmise kuupäev	10.9.2020
Lõpphääletuse tulemus	+: 22 –: 3 0: 0
Lõpphääletuse ajal kohal olnud liikmed	Manon Aubry, Gunnar Beck, Geoffroy Didier, Angel Dzhambazki, Ibán García Del Blanco, Jean-Paul Garraud, Esteban González Pons, Mislav Kolakušić, Gilles Lebreton, Karen Melchior, Jiří Pospíšil, Franco Roberti, Marcos Ros Sempere, Liesje Schreinemacher, Stéphane Séjourné, Raffaele Stancanelli, Marie Toussaint, Adrián Vázquez Lázara, Axel Voss, Marion Walsmann, Tiemo Wölken, Lara Wolters, Javier Zarzalejos
Lõpphääletuse ajal kohal olnud asendusliikmed	Heidi Hautala, Emil Radev

NIMELINE LÕPPHÄÄLETUS NÕUANDVAS KOMISJONIS

22	+
PPE	Geoffroy Didier, Esteban González Pons, Jiří Pospíšil, Emil Radev, Axel Voss, Marion Walsmann, Javier Zarzalejos
S&D	Ibán García Del Blanco, Franco Roberti, Marcos Ros Sempere, Tiemo Wölken, Lara Wolters
RENEW	Karen Melchior, Liesje Schreinemacher, Stéphane Séjourné, Adrián Vázquez Lázara
ID	Gunnar Beck, Jean-Paul Garraud, Gilles Lebreton
ECR	Angel Dzhambazki, Raffaele Stancanelli
NI	Mislav Kolakušić

3	–
VERTS/ALE	Heidi Hautala, Marie Toussaint
GUE/NGL	Manon Aubry

0	0

Kasutatud tähised:
+ : poolt
– : vastu
0 : erapooletu

TEAVE VASTUVÕTMISE KOHTA
VASTUTAVAS KOMISJONIS

Vastuvõtmise kuupäev	29.6.2021
Lõpphääletuse tulemus	+: 36 –: 24 0: 6
Lõpphääletuse ajal kohal olnud liikmed	Magdalena Adamowicz, Konstantinos Arvanitis, Malik Azmani, Katarina Barley, Pernando Barrena Arza, Pietro Bartolo, Nicolas Bay, Vladimír Bilčík, Vasile Blaga, Ioan-Rareş Bogdan, Patrick Breyer, Saskia Bricmont, Joachim Stanisław Brudziński, Jorge Buxadé Villalba, Damien Carême, Caterina Chinnici, Marcel de Graaff, Anna Júlia Donáth, Lena Düpont, Cornelia Ernst, Laura Ferrara, Nicolaus Fest, Jean-Paul Garraud, Maria Grapini, Sylvie Guillaume, Andrzej Halicki, Evin Incir, Sophia in ‘t Veld, Patryk Jaki, Marina Kaljurand, Fabienne Keller, Peter Kofod, Łukasz Kohut, Moritz Körner, Alice Kuhnke, Jeroen Lenaers, Juan Fernando López Aguilar, Lukas Mandl, Roberta Metsola, Nadine Morano, Javier Moreno Sánchez, Maite Pagazaurtundúa, Nicola Procaccini, Emil Radev, Paulo Rangel, Terry Reintke, Diana Riba i Giner, Ralf Seekatz, Michal Šimečka, Birgit Sippel, Sara Skyttedal, Martin Sonneborn, Tineke Strik, Ramona Strugariu, Annalisa Tardino, Tomas Tobé, Dragoş Tudorache, Milan Uhrík, Tom Vandendriessche, Bettina Vollath, Elissavet Vozemberg-Vrionidi, Jadwiga Wiśniewska, Elena Yoncheva, Javier Zarzalejos
Lõpphääletuse ajal kohal olnud asendusliikmed	Tanja Fajon, Miguel Urbán Crespo

NIMELINE LÕPPHÄÄLETUS
VASTUTAVAS KOMISJONIS

36	**+**
NI	Laura Ferrara, Martin Sonneborn
Renew	Malik Azmani, Anna Júlia Donáth, Sophia in ‘t Veld, Fabienne Keller, Moritz Körner, Maite Pagazaurtundúa, Michal Šimečka, Ramona Strugariu, Dragoş Tudorache
S&D	Katarina Barley, Pietro Bartolo, Caterina Chinnici, Tanja Fajon, Maria Grapini, Sylvie Guillaume, Evin Incir, Marina Kaljurand, Łukasz Kohut, Juan Fernando López Aguilar, Javier Moreno Sánchez, Birgit Sippel, Bettina Vollath, Elena Yoncheva
The Left	Konstantinos Arvanitis, Pernando Barrena Arza, Cornelia Ernst, Miguel Urbán Crespo
Verts/ALE	Patrick Breyer, Saskia Bricmont, Damien Carême, Alice Kuhnke, Terry Reintke, Diana Riba i Giner, Tineke Strik
24	**-**
ID	Nicolas Bay, Nicolaus Fest, Jean-Paul Garraud, Marcel de Graaff, Peter Kofod, Annalisa Tardino, Tom Vandendriessche
NI	Milan Uhrík
PPE	Magdalena Adamowicz, Vladimír Bilčík, Vasile Blaga, Ioan-Rareş Bogdan, Lena Düpont, Andrzej Halicki, Jeroen Lenaers, Lukas Mandl, Roberta Metsola, Nadine Morano, Paulo Rangel, Ralf Seekatz, Sara Skyttedal, Tomas Tobé, Elissavet Vozemberg-Vrionidi, Javier Zarzalejos
6	**0**
ECR	Joachim Stanisław Brudziński, Jorge Buxadé Villalba, Patryk Jaki, Nicola Procaccini, Jadwiga Wiśniewska
PPE	Emil Radev

Kasutatud tähised:
+ : poolt
- : vastu
0 : erapooletu