



A9-0232/2021

13.7.2021

MIETINTÖ

tekoälystä rikosoikeudessa ja sen käytöstä poliisi- ja oikeusviranomaisten suorittamassa rikosasioiden käsittelyssä
(2020/2016(INI))

Kansalaisvapauksien sekä oikeus- ja sisäasioiden valiokunta

Esittelijä: Petar Vitanov

SISÄLTÖ

	Sivu
EUROOPAN PARLAMENTIN PÄÄTÖSLAUSELMAESITYS	3
PERUSTELUT	18
SISÄMARKKINA- JA KULUTTAJANSUOJAVALIOKUNNAN LAUSUNTO	20
OIKEUDELLISTEN ASIOIDEN VALIOKUNNAN LAUSUNTO	26
TIEDOT HYVÄKSYMISESTÄ ASIASTA VASTAAVASSA VALIOKUNNASSA	33
LOPULLINEN ÄÄNESTYS NIMENHUUTOÄÄNESTYKSENÄ ASIASTA VASTAAVASSA VALIOKUNNASSA	34

EUROOPAN PARLAMENTIN PÄÄTÖSLAUSELMAESITYS

tekoälystä rikosoikeudessa ja sen käytöstä poliisi- ja oikeusviranomaisten suorittamassa rikosasioiden käsittelyssä (2020/2016(INI))

Euroopan parlamentti, joka

- ottaa huomioon Euroopan unionista tehdyn sopimuksen (SEU) ja erityisesti sen 2 ja 6 artiklan sekä Euroopan unionin toiminnasta tehdyn sopimuksen (SEUT) ja erityisesti sen 16 artiklan,
- ottaa huomioon Euroopan unionin perusoikeuskirjan ja erityisesti sen 6, 7, 8, 11, 12, 13, 20, 21, 24 ja 47 artiklan,
- ottaa huomioon ihmisoikeuksien ja perusvapauksien suojaamiseksi tehdyn yleissopimuksen,
- ottaa huomioon Euroopan neuvoston yleissopimuksen yksilöiden suojelusta henkilötietojen automaattisessa tietojenkäsittelyssä (ETS 108) ja sen muutospöytäkirjan (yleissopimus 108+),
- ottaa huomioon oikeuslaitoksen toimivuutta tarkastelevan Euroopan neuvoston pysyvän komitean (CEPEJ) eurooppalaisen eettisen peruskirjan tekoälyn käytöstä oikeusjärjestelmissä ja niiden ympäristössä,
- ottaa huomioon 8. huhtikuuta 2019 annetun komission tiedonannon luottamuksen rakentamisesta ihmiskeskiseen tekoälyyn (COM(2019)0168),
- ottaa huomioon komission tekoälyä käsittelevän korkean tason asiantuntijaryhmän 8. huhtikuuta 2019 julkaisemat luotettavaa tekoälyä koskevat eettiset ohjeet,
- ottaa huomioon 19. helmikuuta 2020 annetun komission valkoisen kirjan ”Tekoälystä – Eurooppalainen lähestymistapa huippuosaamiseen ja luottamukseen” (COM(2020)0065),
- ottaa huomioon 19. helmikuuta 2020 annetun komission tiedonannon ”Euroopan datastrategia” (COM(2020)0066),
- ottaa huomioon luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta 27. huhtikuuta 2016 annetun Euroopan parlamentin ja neuvoston asetuksen (EU) 2016/679 (yleinen tietosuojasetus)¹,
- ottaa huomioon luonnollisten henkilöiden suojelusta toimivaltaisten viranomaisten suorittamassa henkilötietojen käsittelyssä rikosten ennalta estämistä, tutkimista, paljastamista tai rikoksiin liittyviä syytetoimia tai rikosoikeudellisten seuraamusten

¹ EUVL L 119, 4.5.2016, s. 1.

täytäntöönpanoa varten sekä näiden tietojen vapaasta liikkuvuudesta ja neuvoston puitepäätöksen 2008/977/YOS kumoamisesta 27. huhtikuuta 2016 annetun Euroopan parlamentin ja neuvoston direktiivin (EU) 2016/680²,

- ottaa huomioon luonnollisten henkilöiden suojelusta unionin toimielinten, elinten ja laitosten suorittamassa henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta sekä asetuksen (EY) N:o 45/2001 ja päätöksen N:o 1247/2002/EY kumoamisesta 23. lokakuuta 2018 annetun Euroopan parlamentin ja neuvoston asetuksen (EU) 2018/1725³,
 - ottaa huomioon henkilötietojen käsittelystä ja yksityisyyden suojasta sähköisen viestinnän alalla 12. heinäkuuta 2002 annetun Euroopan parlamentin ja neuvoston direktiivin 2002/58/EY (sähköisen viestinnän tietosuojadirektiivi)⁴,
 - ottaa huomioon Euroopan unionin lainvalvontayhteistyövirastosta (Europol) sekä neuvoston päätösten 2009/371/YOS, 2009/934/YOS, 2009/935/YOS, 2009/936/YOS ja 2009/968/YOS korvaamisesta ja kumoamisesta 11. toukokuuta 2016 annetun Euroopan parlamentin ja neuvoston asetuksen (EU) 2016/794⁵,
 - ottaa huomioon 19. kesäkuuta 2020 antamansa päätöslauselman rasisminvastaisista mielenosoituksista George Floydin kuoleman johdosta⁶,
 - ottaa huomioon 14. maaliskuuta 2017 antamansa päätöslauselman massadatan vaikutuksista perusoikeuksiin: yksityisyys, tietosuoja, syrjimättömyys, turvallisuus ja lainvalvonta⁷,
 - ottaa huomioon kansalaisvapauksien sekä oikeus- ja sisäasioiden valiokunnassa (LIBE) 20. helmikuuta 2020 pidetyn kuulemisen tekoälystä rikosoikeudessa ja sen käytöstä poliisi- ja oikeusviranomaisten suorittamassa rikosasioiden käsittelyssä,
 - ottaa huomioon raportin LIBE-valiokunnan tiedonhankintamatkasta Yhdysvaltoihin helmikuussa 2020,
 - ottaa huomioon työjärjestyksen 54 artiklan,
 - ottaa huomioon sisämarkkina- ja kuluttajansuojavaliokunnan sekä oikeudellisten asioiden valiokunnan lausunnot,
 - ottaa huomioon kansalaisvapauksien sekä oikeus- ja sisäasioiden valiokunnan mietinnön (A9-0232/2021),
- A. ottaa huomioon, että digitaalitekniikka yleensä ja erityisesti tekoälyn mahdollistama tietojenkäsittelyn ja data-analyysien lisääntyminen tuovat mukanaan erittäin suuria lupauksia ja riskejä; ottaa huomioon, että viime vuosina tekoäly on ottanut suuren

² EUVL L 119, 4.5.2016, s. 89.

³ EUVL L 295, 21.11.2018, s. 39.

⁴ EYVL L 201, 31.7.2002, s. 37.

⁵ EUVL L 135, 24.5.2016, s. 53.

⁶ Hyväksytyt tekstit, P9_TA(2020)0173.

⁷ EUVL C 263, 25.7.2018, s. 82.

harppauksen eteenpäin, ja se on yksi 2000-luvun strategisista teknologioista, jolla on mahdollisuus tuottaa huomattavia tehokkuuteen, tarkkuuteen ja käyttömukavuuteen liittyviä hyötyjä ja vaikuttaa siten myönteisesti Euroopan talouteen ja yhteiskuntaan, mutta josta voi myös aiheutua suuria riskejä perusoikeuksille ja oikeusvaltioperiaatteen perustaville demokratioille; toteaa, että tekoäly ei ole itsetarkoitus vaan väline, joka palvelee ihmisiä ja jonka perimmäisenä tavoitteena on lisätä ihmisten hyvinvointia, valmiuksia ja turvallisuutta;

- B. toteaa, että tietokoneiden prosessointinopeuden ja muistikapasiteetin jatkuvasta kehittämisestä huolimatta ei ole vielä olemassa ohjelmia, joiden joustavuus olisi ihmisen tasolla laajempien aihealueiden käsittelyssä tai tehtävissä, jotka edellyttävät asiayhteyden tai kriittisen analyysin ymmärtämistä; panee merkille, että jotkin tekoälysovellukset ovat saavuttaneet asiantuntijoita ja ammattilaisia vastaavan tason tiettyjen tarkasti rajattujen tehtävien (esimerkiksi oikeudellinen teknologia) suorittamisessa ja että ne kykenevät tuottamaan tuloksia valtavasti nopeammin ja suuremmassa laajuudessa;
- C. ottaa huomioon, että joissakin maissa, useat jäsenvaltiot mukaan lukien, tekoälysovelluksia tai sulautettuja tekoälyjärjestelmiä käytetään lainvalvonnassa ja oikeuslaitoksessa enemmän kuin toisissa, mikä johtuu osittain sääntelyn puutteesta ja sellaisista sääntelyeroista, jotka mahdollistavat tai kieltävät tekoälyn käyttämisen tiettyihin tarkoituksiin; toteaa, että tekoälyn lisääntyvä käyttö rikosoikeuden alalla perustuu erityisesti lupauksiin siitä, että se vähentäisi tiettytyyppistä rikollisuutta ja johtaisi objektiivisempiin päätöksiin; toteaa, että nämä lupaukset eivät kuitenkaan aina pidä paikkaansa;
- D. katsoo, että perusoikeuskirjassa vahvistetut perusoikeudet ja -vapaudet olisi taattava tekoälyn ja siihen liittyvän teknologian koko elinkaaren ajan, erityisesti niiden suunnittelun, kehittämisen, käyttöönoton ja käytön aikana, ja että niitä olisi sovellettava lain täytäntöönpanoon kaikissa olosuhteissa;
- E. katsoo, että tekoälyteknologiaa olisi kehitettävä siten, että ihmiset asetetaan sen keskiöön, että se ansaitsee kansalaisten luottamuksen ja toimii aina ihmisten palveluksessa; toteaa, että tekoälyjärjestelmät on aina suunniteltava niin, että käyttäjällä on tarvittaessa mahdollisuus sulkea järjestelmä;
- F. katsoo, että tekoälyjärjestelmät on suunniteltava kaikkien yhteiskunnan jäsenten suojaksi ja eduksi (suunnittelussa on otettava huomioon heikoimmassa asemassa olevat ja syrjityt väestöryhmät), niiden on oltava syrjimättömiä, turvallisia, päätöksissään helppotajuisia ja avoimia ja niissä on kunnioitettava ihmisen itsemääräämisoikeutta ja perusoikeuksia, jotta ne täyttäisivät tekoälyä käsittelevän korkean tason asiantuntijaryhmän eettisissä ohjeissa määritellyt luotettavuuden vaatimukset;
- G. ottaa huomioon, että unionilla on yhdessä jäsenvaltioiden kanssa ratkaiseva vastuu sen varmistamisesta, että tekoälysovellusten elinkaareen ja käyttöön liittyvät päätökset oikeuslaitoksen ja lainvalvonnan alalla tehdään avoimesti, niillä turvataan täysimääräisesti perusoikeuksien toteutuminen eivätkä ne varsinkaan edistä olemassaolollaan syrjintää, vinoumia tai ennakkoluuloja; katsoo, että asiaa koskevissa poliittisissa valinnoissa olisi noudatettava tarpeellisuus- ja suhteellisuusperiaatteita, jotta

voidaan taata perustuslainmukaisuus sekä oikeudenmukainen ja inhimillinen oikeusjärjestelmä;

- H. toteaa, että tekoäly saattaa tarjota suuria mahdollisuuksia myös lainvalvonnan alalla, erityisesti lainvalvontaviranomaisten ja oikeusviranomaisten työskentelymenetelmien parantamisessa ja tietäntyyppisten rikosten, erityisesti talousrikosten, rahanpesun ja terrorismin rahoituksen sekä verkossa tapahtuvan lasten seksuaalisen riiston ja hyväksikäytön sekä tietäntyyppisten kyberrikosten torjunnan tehostamisessa, mikä lisää EU:n kansalaisten turvallisuutta samalla, kun ne saattavat sisältää merkittäviä riskejä ihmisten perusoikeuksien kannalta; katsoo, että tekoälyn yleinen soveltaminen laajamittaiseen valvontaan olisi suhteetonta;
- I. ottaa huomioon, että poliisi- ja oikeusviranomaisten käyttämien tekoälyjärjestelmien kehittämisessä ja toiminnassa on mukana useita henkilöitä, organisaatioita, konekomponentteja, ohjelmistoalgoritmeja ja käyttäjiä usein monimutkaisissa ja haastavissa ympäristöissä; ottaa huomioon, että lainvalvonnassa ja oikeuslaitoksissa käytettävät tekoälysovellukset ovat eri kehitysvaiheissa, aina käsitteellistämävaiheesta prototyyppien luomiseen ja arviointivaiheesta hyväksynnän jälkeiseen käyttöön; ottaa huomioon, että tulevaisuudessa tekoällylle voi löytyä uusia käyttömahdollisuuksia, kun teknologiat kehittyvät maailmanlaajuisesti käynnissä olevan tieteellisen tutkimuksen seurauksena;
- J. katsoo, että tekoälyjärjestelmien mahdollisia haitallisia vaikutuksia koskevan oikeudellisen vastuun osoittamiseen tarvitaan rikosoikeuden alalla selkeä malli; katsoo, että tämän alan sääntelyssä olisi aina säilytettävä ihmisen vastuuvollisuus ja pyrittävä ennen kaikkea välttämään haitallisia vaikutuksia alun alkaenkin;
- K. katsoo, että viime kädessä on jäsenvaltioiden vastuulla taata perusoikeuksien täysimääräinen kunnioittaminen silloin, kun tekoälyjärjestelmiä käytetään lainvalvonnan ja oikeuslaitoksen alalla;
- L. ottaa huomioon, että perusoikeuksien suojelun ja tehokkaan poliisitoiminnan välisen suhteen on aina oltava olennainen osa keskusteluja siitä, pitäisikö tekoälyä käyttää lainvalvonnan alalla, jossa päätöksillä voi olla pitkäaikaisia vaikutuksia yksilöiden elämään ja vapauteen, ja miten sitä olisi tällä alalla käytettävä; pitää tätä erityisen tärkeänä, sillä tekoälystä voi tulla pysyvä osa rikosoikeudellista ekosysteemiä, koska sitä voidaan käyttää analyysi- ja tukivälineenä rikostutkinnoissa;
- M. toteaa, että lainvalvonnassa käytetään tekoälyä esimerkiksi kasvontunnistustekniikoissa, joiden avulla voidaan mm. etsiä epäiltyjä tietokannoista ja tunnistaa ihmiskaupan tai lasten seksuaalisen riiston ja hyväksikäytön uhreja, automaattisessa rekisterikilpien tunnistamisessa, puhujien tunnistamisessa, puheen tunnistamisessa, huulilukutekniikoissa, kuunteluvalvonnassa (esimerkiksi algoritmi laukausten havaitsemiseen), tunnistettujen tietokantojen itsenäisessä tutkimuksessa ja analysoinnissa, ennakoinnissa (ennakoiva poliisitoiminnan ja rikosten hotspot-analysointi), käyttäytymisen havaitsemisvälineissä, kehittyneissä virtuaalisissa ruumiinavausvälineissä kuolinsyyn määrittämistä varten, itsenäisissä välineissä rahoituspetosten ja terrorismin rahoituksen tunnistamiseksi, sosiaalisen median seurannassa (salaaminen ja tietojen kerääminen niiden louhintaan yhteyksiä varten) ja

automaattisissa seurantajärjestelmissä, joissa on mukana erilaisia havaitsemisvalmiuksia (esimerkiksi sydämenlyöntien havaitseminen ja lämpökamerat); ottaa huomioon, että edellä mainittujen sovellusten sekä muiden lainvalvonnan alan mahdollisten tai tulevien tekoälysovellusten luotettavuus ja tarkkuus voivat vaihdella suuresti ja vaikuttaa perusoikeuksien suojeluun ja rikosoikeudellisten järjestelmien dynamiikkaan; ottaa huomioon, että monia näistä välineistä käytetään EU:n ulkopuolisissa maissa, mutta että ne olisivat unionin tietosuojasäännösten ja oikeuskäytännön nojalla laittomia; ottaa huomioon, että algoritmien rutiininomainen käyttöönotto voi johtaa siihen, että aiheettomien varoitusten määrä ylittää selvästi aiheellisten varoitusten määrän, silloinkin kun väriiden positiivisten osuus on pieni;

- N. ottaa huomioon, että myös monien maiden oikeuslaitokset kaikkialla maailmassa käyttävät tekoälyn välineitä ja sovelluksia muun muassa päätösten tukemiseen tutkintavankeustapauksissa, tuomioissa, uusimista koskevien todennäköisyyksien laskemisessa ja koeajan määrittämisessä sekä verkkovälitteisessä riitojenratkaisussa, oikeuskäytännön hallinnassa ja oikeuden piiriin pääsyn helpottamisessa; ottaa huomioon, että tämä on johtanut muiden kuin valkoisten ihmisten ja muiden vähemmistöjen mahdollisuuksien vääristymiseen ja vähenemiseen; ottaa huomioon, että EU:ssa, joitakin jäsenvaltioita lukuun ottamatta, niiden käyttö rajoittuu tällä hetkellä pääasiassa siviiliasioihin;
- O. ottaa huomioon, että tekoälyn käyttöön lainvalvonnassa liittyy useita mahdollisesti suuria ja yksityishenkilöiden perusoikeuksien suojelua koskevia riskejä, joita eräissä tapauksissa on mahdoton hyväksyä, kuten läpinäkymätön päätöksenteko, erityyppinen syrjintä ja taustalla olevan algoritmin virheet, jotka voivat takaisinkytkennän seurauksena kertautua, sekä yksityisyyden ja henkilötietojen suojaan, sananvapauteen ja tiedonvälityksen vapauteen ja syyttömyysolettamaan kohdistuvat riskit sekä tehokkaisuuden oikeussuojakeinoihin ja oikeudenmukaiseen oikeudenkäyntiin ja ihmisten vapauteen ja turvallisuuteen liittyvät riskit;
- P. ottaa huomioon, että lainvalvonta- ja oikeusviranomaisten käyttämät tekoälyjärjestelmät ovat myös alttiita tekoälyn käyttöön perustuville hyökkäyksille tietojärjestelmiä vastaan tai harhautuksille, joissa järjestelmään syötetään tarkoituksellisesti väärää tietoa vääristyneiden tulosten aikaansaamiseksi; ottaa huomioon, että näissä tilanteissa tästä aiheutuva vahinko on mahdollisesti vielä merkittävämpi ja voi johtaa eksponentiaalisesti suurempaan vahinkoon sekä yksilöille että ryhmille;
- Q. katsoo, että tekoälyn käyttöönottoa lainvalvonnan ja oikeuslaitoksen alalla ei pitäisi nähdä pelkkänä teknisenä toteuttamismahdollisuutena vaan pikemminkin poliittisena päätöksenä, joka koskee lainvalvonta- ja rikosoikeusjärjestelmien suunnittelua ja tavoitteita; toteaa, että nykyaikainen rikosoikeus perustuu ajatukselle, jonka mukaan valtion viranomaiset reagoivat rikokseen sen tapahtumisen jälkeen eivätkä oleta, että kaikki ihmiset ovat vaarallisia ja että heitä on jatkuvasti valvottava mahdollisten rikkomusten estämiseksi; ottaa huomioon, että tekoälyyn perustuvilla valvontatekniikoilla tämä lähestymistapa asetetaan vahvasti kyseenalaiseksi ja edellytetään, että lainsäätäjät kaikkialla maailmassa arvioivat perusteellisesti seurauksia, joita aiheutuu sellaisten teknologioiden käyttöönoton sallimisesta, jotka vähentävät ihmisten roolia lainvalvonnassa ja oikeuskäsittelyssä;

1. toistaa, että koska suurten tietomäärien käsittely on tekoälyn ytimessä, oikeutta yksityiselämän suojaan ja oikeutta henkilötietojen suojaan sovelletaan kaikilla tekoälyn aloilla ja että tietosuojaa ja yksityisyyttä koskevaa unionin oikeudellista kehystä on noudatettava täysimääräisesti; muistuttaa, että EU on jo vahvistanut lainvalvontaa koskevat tietosuojastandardit, jotka muodostavat perustan tekoälyn tulevalle sääntelylle lainsäädännön ja oikeuslaitoksen alalla; muistuttaa, että henkilötietojen käsittelyn olisi oltava laillista ja tasapuolista, käsittelyn tarkoitukset olisi määriteltävä selkeästi ja legitimiä, että käsittelyn olisi oltava riittävää ja asianmukaista eikä se saisi olla liiallista tarkoitukseensa nähden, että käsittelyn olisi oltava täsmällistä ja ajantasaista, ja epätarkat tiedot olisi oikaistava tai poistettava, paitsi jos rajoituksia sovelletaan, että tietoja ei saisi säilyttää pidempään kuin on tarpeen, että selkeitä ja asianmukaisia määräaikoja olisi asetettava tietojen poistamiselle tai säilyttämistarpeen säännölliselle tarkistamiselle ja että tietojen käsittelyn olisi oltava turvallista; korostaa myös, että olisi estettävä mahdollinen yksittäisten henkilöiden tunnistaminen tekoälysovelluksella, jossa käytetään aiemmin anonymisoitua dataa;
2. vahvistaa, että kaikissa lainvalvontaa ja oikeuslaitosta koskevissa tekoälyratkaisuisissa on myös noudatettava täysimääräisesti ihmisarvon, syrjimättömyyden, vapaan liikkuvuuden, syyttömyysolettaman, puolustus-oikeuden ja vaitiolo-oikeuden, sananvapauden ja tiedonvälityksen vapauden, kokoontumis- ja yhdistymisvapauden, lain edessä yhdenvertaisuuden, oikeuskeinojen tasapuolisuuden sekä tehokkaita oikeussuojakeinoja koskevan oikeuden ja oikeudenmukaisen oikeudenkäynnin periaatteita Euroopan unionin perusoikeuskirjan ja Euroopan ihmisoikeussopimuksen mukaisesti; painottaa, että tekoälysovellusten käyttö on kiellettävä, jos se on ristiriidassa perusoikeuksien kanssa;
3. toteaa, että tekoälysovellusten nopea kehitys eri puolilla maailmaa ei mahdollista sovellusten tyhjentävää luetteloa ja edellyttää näin ollen selkeää ja johdonmukaista hallintomallia, jolla taataan sekä yksilöiden perusoikeudet että oikeudellinen selkeys kehittäjille, kun otetaan huomioon teknologian jatkuva kehitys; katsoo kuitenkin, että kun otetaan huomioon poliisi- ja oikeusviranomaisten rooli ja vastuu sekä niiden rikosten torjumista, tutkimista, selvittämistä tai syytteesenpanoa tai rikosoikeudellisten seuraamusten täytäntöönpanoa varten tekemien päätösten vaikutus, tekoälysovellusten käyttö on luokiteltava suurirriskiseksi tapauksissa, joissa on mahdollista vaikuttaa merkittävästi yksilöiden elämään;
4. katsoo tässä yhteydessä, että kaikkien lainvalvonta- tai oikeusviranomaisten kehittämien tai käyttämien tekoälyvälineiden olisi oltava vähintään turvallisia, vakaita, varmoja ja tarkoituksenmukaisia, niissä olisi noudatettava oikeudenmukaisuuden, tietojen minimoinnin, vastuuvollisuuden, avoimuuden, syrjimättömyyden ja helppokäyttöisyyden periaatteita ja niiden kehittämiseen, käyttöönottoon ja käyttöön olisi sovellettava riskinarviointia ja tiukkaa tarpeellisuus- ja suhteellisuustestausta, jossa suojatoimien olisi oltava suhteessa havaittuihin riskeihin; korostaa, että kansalaisten luottamus EU:ssa kehitetyn, käyttöön otetun ja käytetyn tekoälyn käyttöön edellyttää näiden kriteerien täysimääräistä täyttämistä;
5. panee merkille tietuustyypisten tekoälysovellusten myönteisen vaikutuksen lainvalvonta- ja oikeusviranomaisten työhön kaikkialla unionissa; korostaa esimerkiksi parantunutta oikeuskäytännön hallintaa, joka on saavutettu lisähakuvaihtoehdot

mahdollistavilla välineillä; katsoo, että tekoälyn muita mahdollisia käyttötarkoituksia lainvalvonnassa ja oikeuslaitoksessa voitaisiin tutkia ottaen huomioon CEPEJ:n hyväksymän tekoälyn käyttöä oikeusjärjestelmissä ja niiden ympäristössä koskevan eettisen peruskirjan viisi periaatetta ja kiinnittäen erityistä huomiota CEPEJ:n yksilöimiin ”käyttötarkoituksiin, joihin on suhtauduttava äärimmäisellä varauksella”;

6. korostaa, että kaikkia teknologian käyttötarkoituksia voidaan muuttaa, ja vaatii tiukkaa demokraattista valvontaa ja riippumatonta seuranta kaikkelle poliisi- ja oikeusviranomaisten käyttämälle tekoälyä hyödyntävälle teknologialle, erityisesti jos sitä on mahdollista käyttää laajamittaiseen valvontaan ja profilointiin; panee näin ollen erittäin huolestuneena merkille lainvalvonta-alalla olevat mahdollisuudet tietyillä tekoälyteknologioilla toteutettavaan laajamittaiseen valvontaan; korostaa oikeudellista vaatimusta, jonka mukaan on estettävä laajamittainen valvonta tekoälyteknologialla, joka määritelmän mukaan ei ole tarpeellisuus- ja suhteellisuusperiaatteiden mukaista, ja kiellettävä sellaisten sovellusten käyttö, jotka voivat johtaa siihen;
7. korostaa, että joissakin EU:n ulkopuolisissa maissa massavalvontateknologioiden kehittämisessä, käyttöönottossa ja käytössä omaksuttu lähestymistapa haittaa suhteettomasti perusoikeuksia, minkä vuoksi EU:n ei tule noudattaa sitä; korostaa siksi, että suoja-toimia, joilla estetään lainvalvonta- ja oikeusviranomaisten harjoittama tekoälyteknologian väärinkäyttö, on myös säänneltävä yhdenmukaisesti kaikkialla unionissa;
8. korostaa tekoälysovellusten, kuten koneoppimisen, käytön mahdollisesti aiheuttamia vinoumia ja syrjintää myös algoritmeissa, joihin kyseiset sovellukset perustuvat; toteaa, että taustatietoaineistoihin voi sisältyä vääristymiä erityisesti silloin, kun käytetään historiallisia tietoja, algoritmien kehittäjät ottavat ne käyttöön tai kun järjestelmät otetaan käyttöön todellisissa olosuhteissa; huomauttaa, että käytetyn datan laatu vaikuttaa väistämättä tekoälysovellusten tuottamiin tuloksiin ja että tällaiset luontaiset vääristymät ovat taipuvaisia vähitellen lisääntymään ja siten ylläpitämään ja lisäämään olemassa olevaa syrjintää, joka kohdistuu erityisesti tiettyihin etnisiin ryhmiin tai rodullistettuihin yhteisöihin kuuluviin henkilöihin;
9. korostaa, että monet tällä hetkellä käytössä olevat algoritmivetoiset tunnistustekniikat tunnistavat ja luokittelevat suhteettomasti väärin ja aiheuttavat näin ollen vahinkoa rodullistetuille henkilöille, tiettyihin etnisiin yhteisöihin kuuluville henkilöille, hlbtihenkilöille, lapsille ja vanhuksille sekä naisille; muistuttaa, että oikean tunnistamisen oikeuden lisäksi yksilöillä on oikeus jäädä tunnistamattomaksi, ellei laissa edellytetä tunnistamista pakottavista ja oikeutetuista yleiseen etuun liittyvistä syistä; korostaa, että tietyn henkilöryhmän ominaisuuksiin perustuvat tekoälyennusteet lisäävät ja toistavat syrjinnän nykyisiä muotoja; katsoo, että olisi ponnisteltava voimakkaasti automatisoidun syrjinnän ja vääristymien välttämiseksi; vaatii vahvoja lisäsuoja-toimia niihin tapauksiin, joissa lainvalvonta- ja oikeusviranomaisten tekoälyjärjestelmien käyttö kohdistuu tai liittyy alaikäisiin;
10. painottaa valtasuhteiden epäsymmetriaa tekoälyteknologian käyttäjien sekä tekoälyteknologian kohteena olevien välillä; pitää erittäin tärkeänä, että poliisi- ja oikeusviranomaisten harjoittama tekoälyn käyttö rikosasioissa ei lisää eriarvoisuutta, sosiaalista eriytymistä tai syrjäytymistä; korostaa tekoälyvälineiden käytön vaikutuksia

rikoksesta epäiltyjen puolustusoikeuksiin, hankaluuksia niiden toimintaa koskevien merkityksellisten tietojen saamisessa ja siitä erityisesti tutkinnan kohteena oleville henkilöille aiheutuvaa ongelmaa haastaa tekoälyvälineiden tulokset tuomioistuimessa;

11. panee merkille riskit, joita liittyy erityisesti tekoälyjärjestelmien käsittelemiin henkilötietoihin tai muihin rikostutkintoihin tai oikeusjuttuihin liittyvien tietojen tietovuotoihin, tietoturvaloukkauksiin ja luvattomaan käyttöön; korostaa, että lainvalvonnassa ja oikeuslaitoksessa käytettävien tekoälyjärjestelmien turvallisuusnäkökohtia on tarkasteltava huolellisesti ja niiden on oltava riittävän vakaita ja palautumiskykyisiä, jotta voidaan estää tekoälyjärjestelmiin kohdistuvien vihamielisten hyökkäysten mahdolliset katastrofaaliset seuraukset; korostaa sisäänrakennetun turvallisuuden ja ihmisen suorittaman erityisen valvonnan merkitystä ennen tiettyjen kriittisten sovellusten käyttöä ja kehottaa siksi lainvalvonta- ja oikeusviranomaisia käyttämään ainoastaan tekoälysovelluksia, joissa noudatetaan sisäänrakennetun yksityisyyden ja tietosuojan periaatetta, jotta vältetään toimintojen häiriintyminen;
12. korostaa, että lainvalvonta- ja oikeusviranomaisten käyttämien tekoälyjärjestelmien ei olisi sallittava aiheuttaa haittaa ihmisten fyysiselle koskemattomuudelle eikä jakaa oikeuksia tai asettaa oikeudellisia velvoitteita yksilöille;
13. tunnustaa haasteet, jotka liittyvät mahdollisten haittojen oikeudellisen vastuun ja vastuuvollisuuden määrittelyyn, kun otetaan huomioon tekoälyjärjestelmien kehittämisen ja toiminnan monimutkaisuus; katsoo, että on luotava selkeä ja oikeudenmukainen järjestelmä, jonka avulla voidaan osoittaa oikeudellinen vastuu ja korvausvastuu näiden kehittyneiden digitaaliteknologioiden mahdollisista kielteisistä seurauksista; korostaa kuitenkin, että ensisijaisesti on pyrittävä ennaltaehkäisemään tällaisten seurauksien syntyminen; kehottaa siksi soveltamaan ennalta varautumisen periaatetta kaikkiin lainvalvonnan alalla käytettäviin tekoälysovelluksiin; korostaa, että oikeudellisen vastuun ja vastuuvollisuuden on aina oltava luonnollisella henkilöllä tai oikeushenkilöllä, joka on aina yksilöitävä tekoälyn tuella tehtävissä päätöksissä; korostaa siksi tarvetta varmistaa tekoälyjärjestelmiä tuottavien ja hallinnoivien yritysraenteiden avoimuus;
14. katsoo, että sekä puolustusoikeuksien tehokkaan toteuttamisen että kansallisten rikosoikeusjärjestelmien avoimuuden kannalta on olennaisen tärkeää, että tekoälyvälineiden käytön ehtoja, menettelytapoja ja seurauksia lainvalvonnan ja oikeuslaitoksen alalla sekä kohteena olevien henkilöiden oikeuksia ja tuloksellisia ja helposti saatavilla olevia valitus- ja muutoksenhakumenettelyjä sekä oikeudellisia muutoksenhakukeinoja säännellään erityisellä, selkeällä ja täsmällisellä oikeudellisella kehyksellä; korostaa rikosoikeudellisen menettelyn osapuolten oikeutta tutustua tietojenkeruuprosessiin ja siihen liittyviin tekoälysovellusten avulla tehtyihin tai niiden avulla saatuihin arviointeihin; pitää erityisen tarpeellisena, että oikeudellisessa yhteistyössä mukana olevat täytäntöönpanoviranomaiset arvioivat toisen jäsenvaltion tai EU:n ulkopuolisen maan esittämistä luovutus- tai kiinniottopyynnöistä päättäessään, voisiko tekoälyvälineiden käyttö pyynnön esittäneessä maassa vaarantaa perusoikeuden oikeudenmukaiseen oikeudenkäyntiin; kehottaa komissiota antamaan suuntaviivat siitä, miten tällainen arviointi tehdään rikosasioissa tehtävän oikeudellisen yhteistyön yhteydessä; vaatii, että jäsenvaltioiden olisi sovellettavan lainsäädännön mukaisesti

varmistettava, että henkilöille tiedotetaan, kun lainvalvontaviranomaiset tai oikeuslaitos käyttävät tekoälysovelluksia heitä koskevissa asioissa;

15. huomauttaa, että jos ihmiset tukeutuvat pelkästään koneiden tuottamiin tietoihin, profiileihin ja suosituksiin, he eivät kykene tekemään riippumatonta arviointia; korostaa mahdollisesti vakavia kielteisiä seurauksia erityisesti lainvalvonnan ja oikeudenkäytön aloilla, kun yksilöt luottavat liikaa tekoälyvälineiden ilmeisen puolueettomaan ja tieteelliseen luonteeseen eivätkä näin ollen ota huomioon mahdollisuutta, että niiden tulokset voivat olla virheellisiä, puutteellisia, merkityksettömiä tai syrjiviä; korostaa, että liiallista riippuvuutta tekoälyjärjestelmien tarjoamista tuloksista olisi vältettävä, ja korostaa, että viranomaisten olisi tärkeää lisätä luottamusta ja tietämystä algoritmin tekemien suositusten kyseenalaistamiseksi; pitää tärkeänä realistisia odotuksia tällaisista teknologisista ratkaisuksista ja sitä, että ei luvata täydellisiä lainvalvontaratkaisuja ja kaikkien tehtyjen rikosten havaitsemista;
16. korostaa, että oikeus- ja lainvalvontayhteyksissä jokaisen oikeudellisen tai vastaavan päätöksen tekijänä on aina oltava ihminen, joka voidaan saattaa vastuuseen tehdyistä päätöksistä; katsoo, että tekoälyyn perustuvien järjestelmien käyttäjien on voitava turvautua oikeussuojakeinoihin; muistuttaa, että EU:n oikeuden mukaan henkilöllä on oikeus olla joutumatta sellaisen päätöksen kohteeksi, jolla on häntä koskevia oikeusvaikutuksia tai joka vaikuttaa häneen merkittävästi ja joka perustuu yksinomaan automaattiseen tietojenkäsittelyyn; painottaa lisäksi, että automatisoitu yksittäispäätöstenteko ei saa perustua erityisiin henkilötietoryhmiin, paitsi jos on toteutettu asianmukaiset toimenpiteet rekisteröidyn oikeuksien ja vapauksien sekä oikeutettujen etujen suojaamiseksi; korostaa, että EU:n lainsäädännössä kielletään erityisiin henkilötietoryhmiin perustuva profilointi, joka johtaa luonnollisiin henkilöihin kohdistuvaan syrjintään; painottaa, että lainvalvontaviranomaisten ja niiden toimien täytäntöönpanevan luonteen vuoksi lainvalvonnan alalla tehdyillä päätöksillä on lähes aina asianomaista henkilöä koskevia oikeusvaikutuksia; panee merkille, että tekoälyn käyttö voi vaikuttaa ihmisten tekemiin päätöksiin ja että sillä voi olla vaikutuksia rikosprosessien kaikkiin vaiheisiin; katsoo siksi, että tekoälyjärjestelmiä käyttävien viranomaisten on ylläpidettävä erittäin tiukkoja oikeudellisia normeja ja varmistettava ihmisen osallistuminen, erityisesti analysoitaessa tällaisista järjestelmistä peräisin olevia tietoja; edellyttää siksi, että tuomareiden suvereeni harkinta ja tapauskohtainen päätöksenteko on säilytettävä; kehottaa kieltämään tekoälyn ja siihen liittyvän teknologian käyttämisen oikeudellisten päätösten ehdottamiseen;
17. kehottaa huolehtimaan algoritmien ymmärrettävyydestä, läpinäkyvyydestä, jäljitettävyydestä ja todennettavuudesta välttämättömänä valvonnan osana sen varmistamiseksi, että oikeuslaitoksen ja lainvalvonnan tekoälyjärjestelmien kehittämisessä, käyttöönotossa ja käytössä noudatetaan perusoikeuksia, ja kansalaiset luottavat niihin, ja että tekoälyalgoritmien tuottamat tulokset voidaan tehdä käyttäjien ja näiden järjestelmien piiriin kuuluvien ymmärrettäviksi ja että lähdetiedot ja järjestelmän lopputulokseen päätyminen tavat ovat avoimia; huomauttaa, että teknisen läpinäkyvyyden, luotettavuuden ja tarkkuuden varmistamiseksi unionin lainvalvonta- tai oikeusviranomaisten olisi voitava ostaa ainoastaan sellaisia välineitä ja järjestelmiä, joiden algoritmit ja logiikka ovat tarkastettavissa ja ainakin poliisin ja oikeuslaitoksen sekä riippumattomien tarkastajien saatavilla, jotta mahdollistetaan niiden arviointi, tarkastus ja tutkinta, eivätkä myyjät saa sulkea niitä tai merkitä niitä

omistusoikeudellisiksi; toteaa, että dokumentaatiota olisi toimitettava selkeällä ja ymmärrettävällä kielellä palvelun luonteesta, siihen kehitetyistä välineistä, suorituskyvystä ja toimintaedellytyksistä sekä mahdollisista riskeistä; kehottaa siksi oikeus- ja lainvalvontaviranomaisia varmistamaan ennakoivan ja täyden avoimuuden yksityisille yrityksille, jotka tarjoavat niille tekoälyjärjestelmiä lainvalvontaa ja oikeuslaitosta varten; suosittelee siksi avoimen lähdekoodin ohjelmistojen käyttöä mahdollisuuksien mukaan;

18. kannustaa lainvalvonta- ja oikeusviranomaisia määrittämään ja arvioimaan aloja, joilla jotkin räätälöidyt tekoälyratkaisut voisivat olla hyödyllisiä, ja vaihtamaan parhaita käytäntöjä tekoälyn käyttöönnotosta; kehottaa jäsenvaltioita ja EU:n virastoja ottamaan käyttöön asianmukaiset julkiset hankintamenettelyt tekoälyjärjestelmille, kun niitä käytetään lainvalvonta- tai oikeudellisessa yhteydessä, jotta varmistetaan, että järjestelmät ovat perusoikeuksien ja sovellettavan lainsäädännön mukaisia, mukaan lukien sen varmistaminen, että ohjelmistoasiakirjat ja algoritmit ovat toimivaltaiten viranomaisten ja valvontaviranomaisten saatavilla ja valmiina tarkastusta varten; kehottaa erityisesti laatimaan sitovia sääntöjä, jotka velvoittavat julkistamaan julkisen ja yksityisen sektorin kumppanuudet, sopimukset ja hankinnat sekä niiden hankinnan tarkoituksen; korostaa, että viranomaisille on tarjottava tarvittava rahoitus ja asiantuntemus tekoälyn käyttöönottoon liittyvien eettisten, oikeudellisten ja teknisten vaatimusten täysimääräisen noudattamisen varmistamiseksi;
19. kehottaa jäljittämään tekoälyjärjestelmät ja niiden toimintaa kuvaavat päätöksentekoprosessit, joissa määritellään järjestelmien valmiudet ja rajoitukset, ja seuraamaan pakollisella asiakirja-aineistolla, mistä päätöksen määrittelevät ominaisuudet ovat peräisin; korostaa, että on tärkeää säilyttää täydellinen dokumentointi koulutusdatasta, sen asiayhteydestä, tarkoituksesta, tarkkuudesta ja sivuvaikutuksista sekä algoritmien rakentajien ja kehittäjien suorittamasta tietojen käsittelystä ja perusoikeuksien noudattamisesta; tähdentää, että aina on oltava mahdollisuus esittää tekoälyjärjestelmien tekemät laskelmat ihmiselle ymmärrettävässä muodossa;
20. kehottaa tekemään pakollisen perusoikeuksia koskevan vaikutustenarvioinnin ennen tekoälyjärjestelmien täytäntöönpanoa tai käyttöönottoa lainvalvonnassa tai oikeuslaitoksessa, jotta voidaan arvioida mahdolliset perusoikeuksiin kohdistuvat riskit; muistuttaa, että aiempi tietosuojaa koskeva vaikutustenarviointi on pakollinen kaiken tyyppiselle ja etenkin uutta teknologiaa hyödyntävälle käsittelylle, johon todennäköisesti liittyy luonnollisten henkilöiden vapauksien ja oikeuksien kannalta korkea riski, ja katsoo, että tämä pätee myös useimpiin lainvalvonnan ja oikeuslaitoksen alalla käytettäviin tekoälyteknologioihin; korostaa tietosuojaviranomaisten ja perusoikeusvirastojen asiantuntemusta järjestelmien arvioinnissa; korostaa, että nämä perusoikeuksia koskevat vaikutustenarvioinnit olisi toteutettava mahdollisimman avoimesti ja kansalaisyhteiskunnan aktiivisella osallistumisella; vaatii, että vaikutustenarvioinneissa määritellään myös selkeästi suojatoimet, jotka ovat tarpeen tunnistettujen riskien käsittelemiseksi, ja että ne asetetaan mahdollisimman laajasti julkisesti saataville ennen tekoälyjärjestelmien käyttöönottoa;
21. korostaa, että ainoastaan riippumattomasti arvioidulla vankalla eurooppalaisella tekoälyn hallinnoinnilla on mahdollista varmistaa perusoikeusperiaatteiden toteutuminen; kehottaa riippumatonta viranomaista tekemään kaikille lainvalvonta- ja

oikeusviranomaisten käyttämille tekoälyjärjestelmille säännöllisesti pakollisia tarkastuksia, jos järjestelmillä on mahdollisuus aiheuttaa merkittäviä vaikutuksia yksittäisten ihmisten elämään, ja testaamaan ja arvioimaan algoritmijärjestelmien kontekstia, tarkoitusta, tarkkuutta, suorituskykyä ja soveltamisalaa niiden käyttöönoton jälkeen, jotta voidaan havaita, tutkia, diagnosoida ja korjata mahdolliset ei-toivotut ja haitalliset vaikutukset ja varmistaa, että tekoälyjärjestelmät toimivat suunnitellusti; kehottaa siksi luomaan tätä varten selkeän institutionaalisen kehyksen, johon sisältyy asianmukainen sääntely- ja valvontavalvonta, jotta varmistetaan täysimääräinen täytäntöönpano ja taataan täysin tietoon perustuva demokraattinen keskustelu tekoälyn tarpeellisuudesta ja oikeasuhteisuudesta rikosoikeuden alalla; korostaa, että näiden tarkastusten tulokset olisi asetettava saataville julkisiin rekistereihin, jotta kansalaiset tietävät, onko tekoälyjärjestelmiä otettu käyttöön ja mihin toimenpiteisiin on ryhdytty perusoikeuksien loukkausten estämiseksi;

22. painottaa, että taustatietoaineistot ja algoritmiset järjestelmät, joita käytetään tekoälyn ja siihen liittyvän teknologian kehittämisen yhteydessä ja tietojenkäsittelyn eri vaiheissa luokitusten, arviointien ja ennusteiden laatimiseen, voivat johtaa myös sellaisten ihmisryhmien erilaiseen kohteluun ja suoraan ja välilliseen syrjintään, joihin kuuluvilla on yhteisiä ominaisuuksia, etenkin jos ennakoivien poliisialgoritmien opetuksessa käytetty data vastaa käytössä olevia tarkkailun painopisteitä ja saattaa siksi tuottaa ja vahvistaa nykyisiä vinoumia; painottaa siksi, että etenkin lainvalvonta- ja oikeusalalla käyttöön otettavat tekoälyteknologiat edellyttävät monialaista tutkimusta ja panostusta, joita ovat muun muassa luonnontieteelliset ja teknologiset tutkimukset, kriittiset rotututkimukset, vammaisuutta käsittelevät tutkimukset ja muut sosiaalisen tilanteen huomioon ottavat tieteenalat, joilla käsitellään muun muassa erojen kehittymistä sekä luokitustyötä ja sen seurauksia; tähdentää, että sen vuoksi on järjestelmällisesti investoitava siihen, että tällaiset alat yhdistetään tekoälyä koskevaan tutkimukseen kaikilla tasoilla; pitää myös tärkeänä, että näiden tekoälyjärjestelmien suunnittelusta, kehittämisestä, testaamisesta, ylläpidosta, käyttöönotosta ja hankinnasta vastaavissa työryhmissä otetaan huomioon järjestelmien käytön ja yleensä yhteiskunnan monimuotoisuus syrjinnän riskin vähentämiseksi muuten kuin teknisin keinoin;
23. korostaa edelleen, että erityisesti poliisi- ja oikeusalan henkilöstölle on annettava merkittävää erikoiskoulutusta tekoälyteknologian eettisistä säännöksistä, mahdollisista vaaroista, rajoituksista ja asianmukaisesta käytöstä, jotta heihin voi kohdistaa riittävän vastuuvastuun, vastuun ja korvausvastuun vaatimukset; korostaa, että olisi varmistettava soveltuvan koulutuksen ja pätevyyksien avulla, että päätöksentekijät ovat perillä vinoutumien mahdollisuudesta, sillä data-aineistot voivat perustua syrjivään ja ennakoasenteisiin perustuvaan dataan; kannattaa tietoisuuden lisäämistä ja koulutusta koskevien aloitteiden laatimista, jotta voidaan varmistaa, että lainvalvonnassa ja oikeuslaitoksessa työskentelevät henkilöt ovat tietoisia tekoälyjärjestelmien käyttöön liittyvistä rajoituksista, valmiuksista ja riskeistä, mukaan lukien automaation vinoumien riski, ja että he ymmärtävät ne; muistuttaa, että poliisiviranomaiset sisällyttävät tekoälykoulutuksen tietokokonaisuuksiin rasismitapauksia tehtäviensä hoitamisessa, mikä johtaa väistämättä rasistiseen vinoumaan tekoälyn tuottamissa havainnoissa, pisteytyksissä ja suosituksissa; palauttaa mieliin kehotuksensa, että jäsenvaltioiden olisi edistettävä syrjinnän vastaista politiikkaa ja kehitettävä rasismiin vastaisia toimintasuunnitelmia, jotka koskevat myös poliisitoimintaa ja oikeusjärjestelmää;

24. toteaa, että ennakoiva poliisitoiminta on yksi lainvalvonnan alalla käytettävistä tekoälysovelluksista, mutta varoittaa, että vaikka sen avulla voidaan analysoida tarvittavia tietoaineistoja tiettyjen kaavojen ja korrelaatioiden tunnistamiseksi, ennakoiva poliisitoiminta ei kykene määrittämään syy-yhteyksiä eikä ennakoimaan luotettavasti yksittäisen ihmisen käyttäytymistä, eikä se näin ollen voi olla ainoa perusta toimintapäätöksille; huomauttaa, että useat yhdysvaltalaiset kaupungit ovat tarkastusten jälkeen lopettaneet ennakoivan poliisitoiminnan käytön; muistuttaa, että LIBE-valiokunnan Yhdysvaltoihin helmikuussa 2020 tekemän tiedonhankintamatkan aikana valiokunnan jäsenet saivat kuulla New Yorkin ja Cambridgen (Massachusetts) kaupunkien poliisilaitoksen edustajilta, että näissä kaupungeissa oli luovuttu ennakoivan poliisitoiminnan ohjelmista niiden tehottomuuden, syrjivyyden ja käytännön epäonnistumisten takia ja sen sijaan siirrytty lähipoliisitoimintaan; toteaa, että tämä oli johtanut rikosten määrän vähenemiseen; vastustaa siksi lainvalvontaviranomaisten päätöstä käyttää tekoälyä tehdäkseen yksilöitä tai ryhmiä koskevia käyttäytymisennusteita aiempien tietojen ja aiemman käyttäytymisen, ryhmän jäsenyyden, sijainnin tai minkä tahansa muun tällaisen ominaisuuden perusteella ja yrittää näin tunnistaa henkilöt, jotka todennäköisesti syyllistyvät rikokseen;
25. panee merkille kasvojentunnistuksen eri tyypit, kuten muun muassa todentamisen / varmentamisen (reaaliaikaisen kasvon sovittaminen henkilöllisyysasiakirjan valokuvaan, esim. älykkäät rajat), tunnistamisen (esim. valokuvan täsmäyttäminen tiettyyn valokuvia sisältävään tietokantaan) ja havaitsemisen (eli kasvojen reaaliaikainen havaitseminen kameravalvontamateriaalin kaltaisista lähteistä ja niiden yhteensovittaminen tietokantoihin, esim. reaaliaikaiseen valvontaan liittyvät vaikutukset), joilla kaikilla on erilaisia vaikutuksia perusoikeuksien suojelussa; katsoo, että kasvojentunnistusjärjestelmien käyttöönotto lainvalvonnassa olisi rajoitettava selkeästi perusteltuihin tarkoituksiin ja siinä olisi täysimääräisesti noudatettava suhteellisuuden ja tarpeellisuuden periaatteita ja sovellettavaa lainsäädäntöä; vahvistaa, että kasvojentunnistusteknologian käytön on vähintään täytettävä tietojen minimointia, tietojen paikkansapitävyyttä, säilytyksen rajoittamista, tietoturvaa ja vastuuvellisuutta koskevat vaatimukset sekä oltava laillista, oikeudenmukaista, läpinäkyvää ja jäsenvaltioiden tai unionin lainsäädännössä selkeästi määritellyn erityisen, nimenomaisen ja oikeutetun tarkoituksen mukaista; katsoo, että todentamis- ja tunnistamisjärjestelmiä voidaan edelleen käyttää ja käyttää menestyksekkäästi vain, jos niiden haitallisia vaikutuksia voidaan lieventää ja edellä mainitut kriteerit täyttyvät;
26. kehottaa lisäksi kieltämään pysyvästi julkisilla paikoilla muiden inhimillisten ominaisuuksien, kuten kasvot, sormenjäljet, DNA, ääni ja muut biometriset ja käyttäytymiseen liittyvät signaalit, automaattisen analysoinnin ja/tai tunnistamisen;
27. kehottaa kuitenkin keskeyttämään kasvojentunnistusjärjestelmien käyttöönoton lainvalvonnassa, paitsi jos tunnistaminen liittyy ainoastaan rikoksen uhrien tunnistamiseen, kunnes teknisten standardien voidaan katsoa olevan täysin perusoikeuksien mukaisia, saadut tulokset ovat puolueettomia ja syrjimättömiä, oikeudellinen kehys tarjoaa tiukkoja suojatoimia väärinkäyttöä vastaan ja tiukkaa demokraattista valvontaa ja on saatavilla empiiristä näyttöä tällaisten teknologioiden käyttöönoton tarpeellisuudesta ja oikeasuhteisuudesta; toteaa, että jos edellä mainitut kriteerit eivät täyty, järjestelmiä ei pitäisi käyttää eikä ottaa käyttöön;

28. pitää erittäin huolestuttavana, että lainvalvontatoimijat ja tiedustelupalvelut käyttävät yksityisiä kasvojentunnistustietokantoja, kuten Clearview-tekoälyä, jonka tietokannan yli kolme miljardia kuvaa on kerätty laittomasti sosiaalisista verkoista ja muista internetin osista, myös EU:n kansalaisilta; kehottaa jäsenvaltioita velvoittamaan lainvalvontatoimijat ilmoittamaan, käyttävätkö ne Clearview-tekoälyteknologiaa tai vastaavaa muiden palveluntarjoajien teknologiaa; muistuttaa Euroopan tietosuojaneuvoston lausunnosta, jonka mukaan Clearview-tekoälyn kaltaisen palvelun käyttäminen unionin lainvalvontaviranomaisten toiminnassa ”ei todennäköisesti ole EU:n tietosuojajärjestelmän mukaista”; kehottaa kieltämään yksityisten kasvojentunnistustietokantojen käytön lainvalvonnassa;
29. panee merkille komission toteutettavuustutkimuksen mahdollisista Prüm-päätökseen⁸ tehtävistä muutoksista, myös kasvojentunnistukseen liittyen; panee merkille aiemman tutkimuksen, jonka mukaan mahdolliset uudet tunnisteet, kuten iiris- tai kasvojentunnistus, eivät olisi yhtä luotettavia rikosteknisissä yhteyksissä kuin DNA tai sormenjäljet; muistuttaa komissiota siitä, että kaikkien lainsäädäntöehdotusten on perustuttava näyttöön ja että niissä on noudatettava suhteellisuusperiaatetta; kehottaa komissiota laajentamaan Prüm-päätöksen puitteita vain, jos on olemassa vankkaa tieteellistä näyttöä kasvojentunnistuksen luotettavuudesta rikosteknisissä olosuhteissa DNA:han tai sormenjälkiin verrattuna, ja ainoastaan sen jälkeen, kun se on tehnyt kattavan vaikutustenarvioinnin ja Euroopan tietosuojavaltuutetun ja tietosuojaneuvoston suositukset on otettu huomioon;
30. korostaa, että biometrinen tietojen käyttö liittyy laajemmin ihmisarvoa koskevan oikeuden periaatteeseen, joka on kaikkien perusoikeuskirjassa taattujen perusoikeuksien pohjana; katsoo, että biometrinen tietojen käyttö ja kerääminen etätunnistusta varten, esimerkiksi tekemällä kasvojentunnistusta julkisissa tiloissa ja lentoasemien rajatarkastuksissa käytettävillä automaattisilla rajatarkastusporteilla, voi aiheuttaa perusoikeuksille erityisiä riskejä, jotka saattavat vaihdella huomattavasti käyttötarkoituksesta, asiayhteydestä ja soveltamisalasta riippuen; korostaa lisäksi, että tunnistamistekniikan, kuten silmän liikkeitä ja pupillien koon muutoksia havaitsevien kameroiden, tieteellinen validiteetti lainvalvonnan yhteydessä on kiistanalainen; katsoo, että biometrisen tunnistamisen käyttöä lainvalvonta- ja oikeuslaitoksissa olisi aina pidettävä ”suurena riskinä” ja siksi siihen olisi sovellettava lisävaatimuksia tekoälyä käsittelevän komission korkean tason asiantuntijaryhmän suositusten mukaisesti;
31. on erittäin huolestunut Horisontti 2020 -puiteohjelmasta rahoitettuja tutkimushankkeista, jotka koskevat tekoälyn käyttöönottoa EU:n ulkorajoilla; toteaa, että yksi näistä on iBorderCtrl-hanke, matkustajia profiloiva ”älykäs valheenpaljastusjärjestelmä”, joka perustuu matkustajan ennen matkaa verkkokamerallaan kuvaamaan tietokoneavusteiseen haastatteluun sekä 38 mikroeleen tekoälypohjaiseen analyysiin ja jota testataan Unkarissa, Latviassa ja Kreikassa; kehottaa siksi komissiota toteuttamaan säädösten ja muiden välineiden sekä tarvittaessa rikkomusmenettelyjen avulla kiellon, joka koskee kaikkea sellaista lainvalvontaa varten toteutettua henkilötietojen ja kasvokuvien biometristä käsittelyä, joka johtaa laajamittaiseen valvontaan yleisessä käytössä olevilla paikoilla; kehottaa edelleen

⁸ Neuvoston päätös 2008/615/YOS, tehty 23. kesäkuuta 2008, rajatylittävän yhteistyön tehostamisesta erityisesti terrorismin ja rajatylittävän rikollisuuden torjumiseksi. EUVL L 210, 6.8.2008, s. 1.

komissiota lopettamaan sellaisen biometrisen tutkimuksen tai biometrinen sovellusten käyttöönoton tai ohjelmien rahoittamisen, joka voisi tukea summittaista ja laajamittaista valvontaa yleisillä paikoilla; korostaa tässä yhteydessä, että olisi kiinnitettävä erityistä huomiota droonien käyttöön poliisioperaatioissa ja sovellettava tiukkaa kehystä;

32. tukee tekoälyä käsittelevän komission korkean tason asiantuntijaryhmän suosituksia tekoälyä hyödyntävän yksilöiden laajamittaisen pisteyttämisen kieltämisestä; katsoo, että kaikenlainen viranomaisten toteuttama laajamittainen ja normatiivinen kansalaisten pisteyttäminen – erityisesti lainvalvonnan alalla ja oikeuslaitoksissa – johtaa itsemääräämisoikeuden menettämiseen ja vaarantaa syrjimättömyyden periaatteen eikä sitä yleisestikään voida pitää EU:n oikeuteen kirjattujen perusoikeuksien ja varsinkaan ihmisarvon mukaisena;
33. kehottaa lisäämään yleistä avoimuutta tekoälysovellusten käytöstä unionissa, jotta niitä ymmärrettäisiin kattavammin; pyytää jäsenvaltioita toimittamaan kattavat tiedot lainvalvonta- ja oikeusviranomaistensa käyttämistä välineistä, käytössä olevien välineiden tyypeistä, niiden käyttötarkoituksista, niiden soveltamisella käsiteltävien rikosten tyypeistä sekä näitä välineitä kehittäneiden yritysten tai organisaatioiden nimistä; kehottaa lainvalvonta- ja oikeusviranomaisia antamaan yleisölle riittävän avoimesti tietoa tekoälyn ja siihen liittyvien teknologioiden käyttämisestä toimivaltuksiensa täytäntöönpanossa esimerkiksi julkaisemalla väärin positiivisten ja väärin negatiivisten osuuden kyseisen teknologian tuloksista; pyytää komissiota kokoamaan ja päivittämään tiedot yhteen paikkaan; kehottaa komissiota myös julkaisemaan ja päivittämään tietoja siitä, miten lainvalvonta- ja lainkäyttötehtävistä vastaavat unionin virastot käyttävät tekoälyä; kehottaa Euroopan tietosuojaneuvostoa arvioimaan lainvalvontaviranomaisten ja oikeuslaitoksen käyttämien tekoälyteknologioiden ja -sovellusten laillisuutta;
34. muistuttaa, että tekoälysovelluksia, mukaan lukien oikeus- ja lainvalvontayhteyksissä käytettävät sovellukset, kehitetään koko maailmassa kiivaalla tahdilla; kehottaa kaikkia eurooppalaisia sidosryhmiä, myös jäsenvaltioita ja komissiota, varmistamaan kansainvälisen yhteistyön avulla EU:n ulkopuolisten kumppaneiden osallistumisen, jotta voidaan tiukentaa normeja kansainvälisellä tasolla ja löytää tekoälyn käytölle yhteinen ja täydentävä oikeudellinen ja eettinen kehys erityisesti lainvalvontaa ja oikeuslaitosta varten ja jossa noudatetaan täysimääräisesti perusoikeuskirjaa, EU:n tietosuojasäännöstöä ja laajemminkin ihmisoikeuksia;
35. kehottaa EU:n perusoikeusvirastoa laatimaan yhteistyössä Euroopan tietosuojaneuvoston ja tietosuojavaltuutetun kanssa kattavia suuntaviivoja, suosituksia ja parhaita käytäntöjä, jotta lainvalvonta- ja oikeusviranomaisten käyttöön voidaan täsmentää kriteerit ja edellytykset tekoälysovellusten ja -ratkaisujen kehittämiseksi, käytölle ja käyttöönotolle; sitoutuu tekemään tutkimuksen lainvalvontadirektiivin⁹ täytäntöönpanosta selvittääkseen, miten henkilötietojen suoja on varmistettu lainvalvonta- ja oikeusviranomaisten käsittelytoimissa, erityisesti kehitettäessä tai

⁹ Euroopan parlamentin ja neuvoston direktiivi (EU) 2016/680, annettu 27. huhtikuuta 2016, luonnollisten henkilöiden suojelusta toimivaltaisten viranomaisten suorittamassa henkilötietojen käsittelyssä rikosten ennalta estämistä, tutkimista, paljastamista tai rikoksiin liittyviä syytetoimia tai rikosoikeudellisten seuraamusten täytäntöönpanoa varten sekä näiden tietojen vapaasta liikkuvuudesta ja neuvoston puitepäättökseen 2008/977/YOS kumoamisesta. EUVL L 119, 4.5.2016, s. 89.

otettaessa käyttöön uutta teknologiaa; kehottaa komissiota lisäksi harkitsemaan, tarvitaanko erityisiä lainsäädäntötoimia, jotka koskevat perusteita ja edellytyksiä, joiden mukaisesti lainvalvonta- ja oikeusviranomaiset voivat kehittää, käyttää ja ottaa käyttöön tekoälysovelluksia ja -ratkaisuja;

36. kehottaa puhemiestä välittämään tämän päätöslauselman neuvostolle ja komissiolle.

PERUSTELUT

Tekoäly on yksi 2000-luvun strategisista teknologioista, joka tuottaa huomattavia tehokkuuteen, tarkkuuteen ja käyttömukavuuteen liittyviä hyötyjä ja vaikuttaa siten myönteisesti Euroopan talouteen. Tekoälysovellukset ovat muun muassa parantaneet terveydenhuoltoa, tehostaneet maataloutta, edistäneet ilmastomuutoksen hillitsemistä ja siihen sopeutumista sekä tehostaneet tuotantoa.

Tekoäly on yksi nykyisen komission tärkeimmistä painopisteistä. Komission puheenjohtaja Ursula von der Leyen ilmoitti poliittisissa suuntaviivoissaan esittävänsä tekoällyn inhimillisiä ja eettisiä seurauksia koskevaa koordinoitua eurooppalaista lähestymistapaa sekä pohdintaa siitä, kuinka massadataa voidaan käyttää paremmin innovoinnin tueksi. Tekoällyn hyväksyminen unionin tason kysymykseksi on johtanut pohdintaan siitä, miten voidaan taata luottamus tekoälyteknologiaan ja varmistaa, että tekoäly ei vaaranna EU:n perusoikeuksia.

Euroopan parlamentti on kuitenkin käsitellyt tekoälyä useita vuosia ennen kuin komissio päätti asettaa sen ensisijaiseksi tavoitteeksi. Lukuisat massadataa, robotiikkaa ja tekoälyä koskevat parlamentin päätöslauselmat vuodesta 2016 lähtien osoittavat, että parlamentti on pitänyt tätä aihetta tärkeänä. Päätöslauselmissa on tarkasteltu tekoällyn erilaisia seurauksia ja vaikutuksia hyvinvointiin, koulutukseen, teknologiaan, lainsäädäntöön ja perusoikeuksiin sekä teollisuuteen yleensä. Päätöslauselmissa on korostettu tarvetta omaksua ”ihmiskeskeinen” lähestymistapa, joka perustuu perusoikeuksien eli EU:n perusoikeuskirjan ja EU:n tietosuojakehyksen noudattamiseen.

Koska kyseessä on ”joukko teknologioita, joissa yhdistetään dataa, algoritmeja ja laskentatehoa”, ”laskentatehon kasvu ja datan saatavuuden lisääntyminen ovat näin ollen keskeisiä tekoällyn nykyisen noususuhdanteen liikkeellepanevia voimia”¹. Tekoällyn ytimenä on kerätä, analysoida ja koota jatkuvasti eri lähteistä suuria tietomääriä, myös henkilötietoja, joita käsitellään automaattisesti tietokonealgoritmeilla ja kehittyneillä tietojenkäsittelytekniikoilla. Näissä tekniikoissa käytetään sekä tallennettua että suoratoistodataa tiettyjen korrelaatioiden, suuntausten ja mallien luomiseksi (massadata-analyysi). Tekoälyä varten käytetyt tiedot eivät ole peräisin ainoastaan yksityishenkilöiltä: tekoälysovelluksissa käytetään enimmäkseen teollisuudelta, yrityksiltä ja julkiselta sektorilta peräisin olevaa dataa, jota käsitellään eri tarkoituksiin. Vaikka tekoälysovellusten käyttämät tiedot saattavat joskus olla muita kuin henkilötietoja, tekoälytoiminta edellyttää hyvin usein henkilötietojen käsittelyä, sillä tekoälytoiminta johtaa usein automatisoituihin päätöksiin, joilla on välittömiä seurauksia yksilöihin. Näiden tekoällyn ominaispiirteiden vuoksi meidän on kiinnitettävä tällä alalla erityistä huomiota tietosuojaa ja yksityisyyttä koskevien perusperiaatteiden noudattamiseen.

Tekoäly tarjoaa suuria mahdollisuuksia myös lainvalvonnan ja rikosoikeuden alalla, erityisesti lainvalvontaviranomaisten ja oikeusviranomaisten työskentelymenetelmien parantamisessa ja tietäntyyppisten rikosten, erityisesti talousrikosten, rahanpesun ja terrorismin rahoituksen sekä tietäntyyppisten kyberrikosten, torjunnan tehostamisessa. Tällä alalla tekoälysovelluksiin kuuluvat muun muassa kasvontunnistustekniikat, automaattinen rekisterikilpien tunnistaminen, puhujien tunnistaminen, puheen tunnistaminen, huulitalukutekniikat, kuunteluvalvonta (esimerkiksi algoritmi laukausten havaitsemiseen) , tunnistettujen tietokantojen itsenäinen

¹ COM(2020)0065.

tutkimus ja analysointi, ennakointi (ennakoiva poliisitoiminnan ja rikosten hotspot-analysointi), käyttäytymisen havaitsemisvälineet, itsenäiset välineet rahoituspetosten ja terrorismin rahoituksen tunnistamiseksi, sosiaalisen median seuranta (salaaminen ja tietojen kerääminen niiden louhintaan yhteyksiä varten), IMSI-järjestelmän seurantakamerat ja automaattiset seurantajärjestelmät, joissa on mukana erilaisia havaitsemisvalmiuksia (esimerkiksi sydämenlyöntien havaitseminen ja lämpökamerat). Oikeuslaitoksessa tekoälyä voidaan käyttää rikoksenuusimista koskevien todennäköisyyksien laskemiseen ja koeajan tai tuomion määrittämiseen.

Tekoälyn tuomista hyödyistä huolimatta tekoälyyn liittyy samanaikaisesti useita potentiaalisia riskejä, kuten läpinäkymätön päätöksenteko, erityyppinen syrjintä, tunkeutuminen yksityiselämäämme sekä henkilötietojen suojaan, ihmisarvoon sekä sananvapauteen ja tiedonvälityksen vapauteen kohdistuvat haasteet. Nämä mahdolliset riskit pahenevat lainvalvonnan ja rikosoikeuden alalla, koska ne voivat vaikuttaa syyttömyysolettamaan, yksilön vapautta ja turvallisuutta sekä tehokkaita oikeussuojakeinoja ja oikeudenmukaista oikeudenkäyntiä koskeviin perusoikeuksiin.

Tässä mietinnössä pyritään käsittelemään kysymyksiä, jotka liittyvät tekoälyn käyttöön rikosoikeudessa ja sen käyttöön poliisi- ja oikeusviranomaisten toimesta rikosasioissa. Vaikka mietinnössä tunnustetaan tekoälyn mahdolliset hyödyt ja edut, siinä tuodaan esiin myös tekoälyyn mahdollisesti liittyvät merkittävät riskit ja seuraukset.

Mietinnössä korostetaan tarvetta kunnioittaa täysimääräisesti perusoikeuksia, sellaisina kuin ne on vahvistettu EU:n perusoikeuskirjassa, yksityisyyttä ja tietosuojaa koskevassa unionin lainsäädännössä, erityisesti direktiivissä (EU) 2016/680 (poliisidirektiivi), ja tarvetta sijoittaa tekoälyn elinkaareen useita keskeisiä periaatteita, kuten algoritmien käytettävyys ja avoimuus, jäljitettävyys, pakolliset perusoikeuksia koskevat vaikutustenarvioinnit ennen tekoälyjärjestelmien täytäntöönpanoa tai käyttöönottoa sekä pakolliset tarkastukset. Kaikki nämä vaatimukset ovat tarpeen paitsi tekoälyjärjestelmien laillisuuden varmistamiseksi myös siksi, että yksityishenkilöt voivat luottaa lainvalvonta- ja rikosoikeusviranomaisten valintaan käyttää niitä.

Lopuksi esittelijä kehottaa keskeyttämään kasvojentunnistusjärjestelmien käytön lainvalvontatarkoituksissa. Näiden teknologioiden nykytilanne ja merkittävät vaikutukset perusoikeuksiin edellyttävät perusteellista ja avointa yhteiskunnallista keskustelua, jotta voidaan tarkastella esiin nousseita kysymyksiä ja teknologioiden käyttöönoton perusteita.

3.9.2020

SISÄMARKKINA- JA KULUTTAJANSUOJAVALIOKUNNAN LAUSUNTO

kansalaisvapauksien sekä oikeus- ja sisäasioiden valiokunnalle

tekoälystä rikosoikeudessa ja sen käytöstä poliisi- ja oikeusviranomaisten suorittamassa rikosasioiden käsittelyssä
(2020/2016(INI))

Valmistelija: Marcel Kolaja

EHDOTUKSET

Sisämarkkina- ja kuluttajansuojavaliokunta pyytää asiasta vastaavaa kansalaisvapauksien sekä oikeus- ja sisäasioiden valiokuntaa sisällyttämään seuraavat ehdotukset päätöslauselmaesitykseen, jonka se myöhemmin hyväksyy:

- A. katsoo, että kun otetaan huomioon tekoälyn myönteinen yhteiskunnallinen potentiaali ja sen luontaiset riskit, digitaalisten sisämarkkinoiden toimintaa olisi parannettava vahvistamalla oikeusvarmuutta tekoälyjärjestelmien tarjoajille ja lisäämällä kuluttajien luottamusta ja turvallisuutta siten, että lujitetaan suojatoimenpiteitä, joilla varmistetaan oikeusvaltioperiaatteen ja perusoikeuksien, erityisesti oikeuden yksityisyyteen ja henkilötietojen suojeluun, oikeuden yhdenvertaisuuteen ja syrjimättömyyteen, oikeuden hyvään hallintoon ja oikeudenmukaiseen oikeudenkäyntiin sekä oikeuden korkeatasoiseen kuluttajansuojaan, kunnioittaminen; toteaa, että tekoäly edellyttää yhteistä eurooppalaista lähestymistapaa ja sen käyttöä poliisin ja lainvalvontaviranomaisten toimesta rikosasioissa on säänneltävä, jotta vältetään toiminnan hajanaisuus sisämarkkinoilla;
- B. toteaa, että poliisi- ja oikeusviranomaiset testaavat ja käyttävät tekoälyä laajasti ja että tällaiseen käyttöön, kuten kasvojentunnistusjärjestelmät, DNA-profilointi, ennakoiva rikoskartoitus ja matkapuhelintietojen poiminta, edistyneet oikeuskäytännön hakukoneet, verkkovälitteinen riidanratkaisu sekä oikeudenkäytön koneoppiminen, liittyy erilaisia käyttötapoja, seurauksia ja riskejä;
- C. katsoo, että tekoälyn käyttö voi muodostaa paradigmanmuutoksen rikosoikeuden hallinnoinnissa;

- D. toteaa, että perusoikeusviraston raportin mukaan saatavilla on edelleen vain rajallisesti tietoa kasvojentunnistusteknologian mahdollisesta käytöstä tai testauksesta jäsenvaltioissa¹;
- E. toteaa, että niissä jäsenvaltioissa, joissa oli saatavilla jonkin verran tietoa kasvojentunnistusteknologian käytöstä, tietosuojaviranomaiset katsoivat, että kyseisen teknologian käyttö ei ollut tietosuojalainsäädännön mukaista eikä sen käyttöönotolla ollut oikeusperustaa;
- F. toteaa, että uudistamalla julkisia hankintoja koskevia menettelyjä sisämarkkinoiden alalla unioni voi vaikuttaa perustavanlaatuisella tavalla siihen, että hallitusten toimet ja menettelyt vastaavat toissijaisia poliittisia tavoitteita, kuten tietosuojaa ja syrjimättömyyttä;
- G. katsoo, että syrjintää voi esiintyä dataohjatun algoritmisen päätöksenteon suunnittelu-, testaus- ja täytäntöönpanovaiheen aikana data-aineistoihin tai algoritmeihin sisältyvien vinoutumien kautta;
- H. katsoo, että tekoälyn teknisen kehittämisen ja soveltamisen on oltava periaatelähtöistä, jotta varmistetaan ihmis- ja perusoikeuksien kunnioittaminen;
- I. toteaa, että oikeuslaitoksen toimivuutta tarkasteleva Euroopan neuvoston pysyvä komitea (CEPEJ) julkaisi 4. joulukuuta 2018 tekoälyn käytöstä oikeusjärjestelmissä eettisen peruskirjan, jossa esitetään eettiset periaatteet tekoälyn käytölle oikeusjärjestelmissä;
- J. toteaa, että tekoälyteknologian tietyt käyttötarkoitukset ovat erityisen herkkiä ja alttiita väärinkäytöksille ja että tämä on hiljattain johtanut siihen, että eräät teknologiayritykset päättivät lopettaa näiden ohjelmistojen tarjonnan;
1. katsoo, että poliisi- ja oikeusviranomaisten käyttämä tekoäly on yleisesti luokiteltava riskialttiiksi ja sitä on käsiteltävä erittäin huolellisesti ja erittäin tiukkoja tietosuojastandardeja noudattaen, kun otetaan huomioon näiden viranomaisten tehtävä yleisen edun puolustajana ja heidän vastuidensa luonne; katsoo, että sisämarkkinoilla tarvitaan pikaisesti tekoälyä koskeva yhteinen eurooppalainen sääntelykehys; katsoo, että EU:n olisi otettava johtoasema selkeisiin sääntöihin, perusoikeuksiin ja etiikkaan perustuvan unionin tason sääntelyn vahvistamisessa tekoälyn kehittämisessä ja käytössä, myös julkisissa hankinnoissa, jotta voidaan varmistaa sama korkea kuluttajansuojataso ja yhdenmukaiset teollisuusstandardit kaikkialla EU:ssa ja jotta mahdollistetaan sisämarkkinoiden parempi toiminta samalla kun kannustetaan innovointiin ja edistetään yritysten, erityisesti pk-yritysten, oikeusvarmuutta; kehottaa komissiota tarkastelemaan nykyisen lainsäädännön soveltamista ja valvontaa ennen mahdollisten uusien lainsäädäntöehdotusten esittämistä;
2. on tietoinen, että tekoälyn käyttö oikeusalalla voi auttaa parantamaan menettelyjen tehokkuutta ja laatua; painottaa tässä yhteydessä, että erityisesti Euroopan

¹ Euroopan unionin perusoikeusvirasto: Facial recognition technology: fundamental rights considerations in the context of law enforcement, (FRA Focus), 27. marraskuuta 2019.
https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf

ihmisoikeussopimuksessa ja yksilöiden suojelusta henkilötietojen automaattisessa tietojenkäsittelyssä tehdyssä Euroopan neuvoston yleissopimuksessa esitettyjä sääntöjä on noudatettava;

3. kehottaa komissiota arvioimaan markkinoilla saatavilla olevaa tekoälyteknologiaa ja sen käyttötasoa poliisi- ja oikeusviranomaisissa maakohtaisesti;
4. korostaa, että tekoälyn olisi autettava keventämään viranomaisten hallinnollista taakkaa ja lisättävä viranomaisten päätöksenteon tehokkuutta ja että tekoälyjärjestelmien olisi aina perustuttava ihmisen suorittamaan valvontaan, yhteistyöhön ja koordinointiin; korostaa tässä yhteydessä, että ihmisten olisi aina viime kädessä oltava vastuussa kaikesta rikosasioita koskevasta päätöksenteosta; painottaa paikkansa pitävien data-aineistojen merkitystä, kun niitä käytetään apuna sähköisen hallinnon prosesseissa ja hallinnollisessa päätöksenteossa kaikkialla unionissa;
5. korostaa, että on tärkeää mahdollistaa innovointi, avoimuus, jäljitettävyyys ja todentaminen; korostaa, että avoimen lähdekoodin tekoäly voisi edistää tätä ja vahvistaa samalla yhteistyötä ja edistää algoritmien käyttöön ja luomiseen liittyvien ideoiden ja kokemusten vaihtoa;
6. katsoo, että poliisin ja lainvalvontaviranomaisten rikosoikeudellisissa asioissa käyttämä tekoäly olisi julkistettava mahdollisuuksien mukaan avoimen lähdekoodin ohjelmistona julkisia hankintoja koskevassa menettelyssä ja sovellettavan lainsäädännön mukaisesti, mukaan lukien tekijänoikeudesta ja lähioikeuksista digitaalisilla sisämarkkinoilla 17. huhtikuuta 2019 annettu Euroopan parlamentin ja neuvoston direktiivi 2019/790/EU, siten että ohjelmistoasiakirjat ja algoritmit ovat saatavilla, jolloin toimivaltaiset viranomaiset voivat tarkistaa, miten tekoälyjärjestelmä on päättynyt tiettyyn ratkaisuun; korostaa, että perusoikeuksia koskevan tarkastuksen olisi oltava osa ennalta toteutettavaa vaatimustenmukaisuuden arviointia; korostaa, että samalla kun varmistetaan unionin oikeuden ja arvojen sekä sovellettavien tietosuojasääntöjen noudattaminen eikä vaaranneta rikostutkintaa tai syytteiden nostamista, selitettävissä olevat ja puolueettomat algoritmit, jotka täyttävät riittävän avoimuuden velvoitteen, ja avoimen datan käyttäminen avoimesta datasta ja julkisen sektorin hallussa olevien tietojen uudelleenkäytöstä annetun direktiivin (EU) 2019/1024 mukaisesti ja rajoittamatta asetuksen (EU) 2016/679 soveltamista ovat olennaisen tärkeitä sen varmistamiseksi, että yritykset ja kuluttajat voivat luottaa parempiin, helposti saatavilla oleviin, syrjimättömiin ja luotettaviin julkisiin palveluihin ja hyötyä niistä kohtuullisin kustannuksin;
7. korostaa, että tekoälyyn perustuva tiedonkeruu ja yksilöiden seuranta olisi rajoitettava rikoksesta epäiltyihin ja tuomioistuimen hyväksymään valvontaan sovellettavan kansallisen lainsäädännön mukaisesti ottaen huomioon yksityiselämän kunnioittaminen ja syyttömyysolettama, mukaan lukien niiden muiden käyttäjien ja kuluttajien osalta, joihin tällaiset järjestelmät ja käytännöt voivat tahattomasti vaikuttaa; korostaa, että kun päätöksentekoa tuetaan tilastollisilla laskelmilla, olisi varmistettava soveltuvan koulutuksen ja pätevyyksien avulla, että päätöksentekijät ovat perillä vinoutumien mahdollisuudesta, sillä data-aineistot voivat perustua syrjivään ja ennakoasenteisiin perustuvaan dataan; korostaa tässä yhteydessä algoritmien ja alkuperäisen datan laadun merkitystä ja muistuttaa, että tekoälyn käytön on perustuttava syrjimättömyyden

periaatteeseen tietojen syöttämisessä ja analysoinnissa; vaatii, että tällaisia sovelluksia koskeissa hankintamenettelyissä on suojauduttava mahdollisilta vinoutumilta; kehottaa vaihtamaan tietoja ja parhaita käytäntöjä siitä, miten jäsenvaltioiden oikeus- ja poliisiviranomaiset soveltavat tekoälytekniikoita ja -välineitä, jotta vältetään hajanainen lähestymistapa sisämarkkinoilla ja varmistetaan kuluttajien ja kansalaisten suojele kaikkialla unionissa;

8. vaatii, että jäsenvaltioiden olisi sovellettavan rikoslainsäädännön mukaisesti varmistettava, että kansalaisille ja kuluttajille tiedotetaan tekoälyn käytöstä ja että kansalaisten saatavilla olisi oltava yksinkertaisia, tehokkaita ja helposti saatavilla olevia valitus- ja muutoksenhakumenettelyjä, oikeudelliset muutoksenhakekeinot mukaan lukien, jotta he voivat tehokkaasti puolustaa oikeuksiaan;
9. palauttaa mieliin, että tietyn tyyppisen tekoälyn riskit ovat suuria, mukaan lukien kasvojen tunnistusteknologia julkisissa tiloissa, automatisoitu käyttäytymisen havaitseminen ja profilointi ihmisten jakamiseksi riskiluokkiin rajoilla, biometrinen havaitseminen ja tunnistaminen joukkovalvontaa varten, kansalaisten laajamittainen pisteyttäminen ja ennakoiva poliisitoiminta, ja kehottaa komissiota säätämään niiden hankintaa ja käyttöä väärinkäyttöriskin poistamiseksi; on tässä yhteydessä tyytyväinen komission jatkuvaan työhön biometrinen teknologioiden käytön arvioimiseksi sekä sääntelyvaihtoehtojen, kuten riskiin perustuva lähestymistapa ja niiden kieltäminen erityistilanteissa, tarkastelemiseksi ja tarvittavien takeiden käyttöönottamiseksi silloin, kun niiden käyttö on perusteltua;
10. korostaa, että tuomareiden suvereeni harkinta ja tapauskohtainen päätöksenteko on säilytettävä, jotta puhtaasti tilastollisiin laskelmiin perustuvat päätökset eivät muodostuisi normiksi.

**TIEDOT HYVÄKSYMISESTÄ
LAUSUNNON ANTAVASSA VALIOKUNNASSA**

Hyväksytty (pvä)	3.9.2020
Lopullisen äänestyksen tulos	+: 40 -: 4 0: 0
Lopullisessa äänestyksessä läsnä olleet jäsenet	Alex Agius Saliba, Andrus Ansip, Alessandra Basso, Brando Benifei, Adam Bielan, Hynek Blaško, Biljana Borzan, Vlad-Marius Botoș, 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-Ștefan Motreanu, Kris Peeters, Anne-Sophie Pelletier, Christel Schaldemose, Andreas Schwab, Tomislav Sokol, Ivan Štefanec, Kim Van Sparrentak, Marion Walsmann, Marco Zullo
Lopullisessa äänestyksessä läsnä olleet varajäsenet	Maria da Graça Carvalho, Anna Cavazzini, Krzysztof Hetman

**LOPULLINEN ÄÄNESTYS NIMENHUUTOÄÄNESTYKSENÄ
LAUSUNNON ANTAVASSA VALIOKUNNASSA**

40	+
EPP	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
GREENS/EFA	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
---	---

Symbolien selitys:

+ : puolesta

- : vastaan

0 : tyhjää

15.9.2020

OIKEUDELLISTEN ASIOIDEN VALIOKUNNAN LAUSUNTO

kansalaisvapauksien sekä oikeus- ja sisäasioiden valiokunnalle

tekoälystä rikosoikeudessa ja sen käytöstä poliisi- ja oikeusviranomaisten suorittamassa rikosasioiden käsittelyssä
(2020/2016(INI))

Valmistelija: Angel Dzhambazki

EHDOTUKSET

Oikeudellisten asioiden valiokunta pyytää asiasta vastaavaa kansalaisvapauksien sekä oikeus- ja sisäasioiden valiokuntaa sisällyttämään seuraavat ehdotukset päätöslauselmaesitykseen, jonka se myöhemmin hyväksyy:

- A. toteaa, että oikeus oikeudenmukaiseen oikeudenkäyntiin on perusoikeus ja juridisesti sitova oikeus, joka on vahvistettu Euroopan unionin perusoikeuskirjassa ja Euroopan ihmisoikeussopimuksessa lainvalvontatarkoituksessa; ottaa huomioon, että sitä sovelletaan koko rikosoikeudellisen menettelyn ajan, myös lainvalvonnassa, ja sen turvaaminen sulkee menettelyn kaikissa vaiheissa pois sellaisten toimenpiteiden toteuttamisen, tekniset toimenpiteet mukaan lukien, joiden välittömänä tai välillisenä seurauksena on se, että puolustautumisoikeudet menettävät merkityksensä; toteaa, että tähän periaatteeseen liittyvät takeet, erityisesti riippumaton tuomioistuin, yhdenvertaisuus lain edessä ja syyttömyysolettama, ovat tiukemmat rikosoikeuden alalla; katsoo, että näitä oikeuksia on kunnioitettava kaikissa olosuhteissa, etenkin tekoälyn käytön yhteydessä, erityisesti kun otetaan huomioon, että tekoälyyn perustuva teknologia voi vaikuttaa eri ihmisoikeuksiin;
- B. toteaa, että henkilötietojen suoja sovelletaan yleisen tietosuojasetuksen¹ ja soveltuvissa tapauksissa muun asiaan liittyvän lainsäädännön mukaisesti aina;
- C. toteaa, että tekoäly ja siihen liittyvä teknologia, myös sen itseoppimiskyky, edellyttää aina tietyssä määrin osallistumista;
- D. katsoo, että tekoälystä voi tulla pysyvä osa rikosoikeusjärjestelmiä;

¹ Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, annettu 27. huhtikuuta 2016, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (EUVL L 119, 4.5.2016, s. 1).

- E. toteaa, että tekoäly ja siihen liittyvä teknologia ovat unionin painopiste, koska teknologia-ala kehittyy nopeasti ja on tärkeää seurata tarkasti, mikä vaikutus kyseisillä teknologioilla on nyt ja jatkossa EU:n ainutlaatuisen teollis- ja tekijänoikeusjärjestelmään; toteaa, että tekoälyn ja siihen liittyvän teknologian käyttö on jo aloitettu monilla aloilla, muun muassa robotiikassa, liikenteessä ja terveydenhuoltoalalla;
- F. ottaa huomioon, että tekoälyn ja siihen liittyvän teknologian kaltaista teknologiaa voitaisiin hyödyntää rikosoikeuden alalla vähentämään rikosten määrää käyttämällä sitä tilastollisen tiedon analysoinnissa rikosten analysoimiseksi ja ehkäisemiseksi sekä havaitsemiseksi ja tutkimiseksi; katsoo, että unionin olisi kehitettävä edelleen ohjelmistoja, datan tallentamista ja tekoälyteknologiaa koskevia valmiuksiaan, jotta voidaan korjata puutteet tietosuojan ja yksityisyyden alalla;
- G. toteaa, että tällä teknologialla voidaan luoda anonymisoituja tilastotietokantoja, jotka auttavat viranomaisia, tiedemaailmaa ja lainsäätäjiä analysoimaan lukuja ja laatimaan tehokkaasti toimia, joilla ehkäistään rikollisuutta ja autetaan rikosentekijöitä sopeutumaan takaisin yhteiskuntaan;
- H. toteaa, että tekoälyn oikeudellisen kehyksen ja sen rikosoikeuteen soveltamisen olisi sisällettävä tarvittaessa lainsäädäntötoimia alkaen pakollisista toimenpiteistä sellaisten käytäntöjen ehkäisemiseksi, jotka kiistatta heikentäisivät perusoikeuksia ja -vapauksia;
- I. ottaa huomioon, että tekoälyjärjestelmien luontaisesti vaikeaselkoisen luonteen vuoksi rikosoikeudellisissa yhteyksissä käytettävät uudet välineet voivat olla ristiriidassa joidenkin perusvapauksien kanssa;
- J. ottaa huomioon, että tekoälyjärjestelmien soveltamiseen rikosoikeusalalla liittyviä mahdollisia riskejä on ehkäistävä ja lievennettävä, jotta turvataan epäiltyjen ja syytettyjen henkilöiden perusoikeudet rikosoikeudellisessa menettelyssä;
1. korostaa, että on ratkaisevan tärkeää arvioida asianmukaisesti tekoälyjärjestelmien käytön riskit, kuten syrjintä ja yksityisyyden loukkaus, sekä ottaa huomioon tekoälyn ja siihen liittyvän teknologian käytön kaikki eettiset ja operatiiviset vaikutukset yhteiskunnassa, erityisesti kun valtion viranomaiset ja poliisi- ja oikeusviranomaiset käyttävät sitä rikosoikeusjärjestelmissä, sekä vastuuta ja todisteita koskevat kysymykset, kun tekoälyjärjestelmien toimintaan liittyy mahdollisia virheitä; katsoo, että tarvitaan selkeä sääntelykehys, jotta voidaan asettaa rajat ja tarjota asianmukaiset suojakeinot; painottaa eettisiä periaatteita, kuten Euroopan neuvoston tekoälyn käyttöä rikosoikeudessa käsittelevässä asiakirjassa ”European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and their environment” vahvistetut periaatteet, jotka tekoälyvälineiden ja -palvelujen alkuperäisestä suunnittelusta ja kehittämisestä vastaavien julkisten ja yksityisten tahojen on otettava huomioon ja joita niiden on noudatettava, jotta kaikki yhteiskunnalliset toimijat voivat saada kattavasti tietoa tekoälyohjelmia tuottavien yritysten yritysraakenteesta; korostaa inhimillisen tekijän merkitystä ja toteaa, että ihmisen on aina oltava lopullinen päätöksentekijä tekoälyteknologiaan perustuvissa ohjelmistoissa ja rikosoikeudellisessa järjestelmässä, olipa kyseessä sitten lainvalvonta tai rikosoikeus; toistaa, että biometrisiä tunnistusohjelmistoja olisi käytettävä vain tilanteissa, joissa se on selvästi perusteltua;

2. korostaa tarvetta pyrkiä tasapainoon ja säilyttää tasapaino rikosoikeusmenettelyihin liittyvän tekoälyjärjestelmien käytön ja toisaalta kaikkien eurooppalaisessa ja kansainvälisessä lainsäädännössä vahvistettujen perusoikeuksien ja menettelyllisten takeiden noudattamisen välillä;
3. painottaa tarvetta käyttää tekoälyä siten, että päätöksentekoprosessissa noudatetaan asianmukaisesti oikeusvaltioperiaatetta ja oikeuslaitoksen riippumattomuutta koskevaa periaatetta;
4. kehottaa komissiota selventämään edelleen tekoälyn ja siihen liittyvän teknologian välityksellä kerätyn datan suojaamiseen ja yhteiskäyttöön liittyviä sääntöjä, silloin kun tätä dataa keräävät keräämiseen ja/tai käsittelyyn valtuutetut viranomaiset, ja toteaa, että tämä kattaa myös muut kuin henkilötiedot ja anonymisoidut tiedot, joissa henkilöt tunnistetaan suoraan tai välillisesti, yleistä tietosuojaa-asetusta ja sähköisen viestinnän tietosuojadirektiiviä kaikilta osin noudattaen²; korostaa edelleen, että oikeudenmukaista oikeudenkäyntiä koskevaan oikeuteen olisi sisällytettävä kansalaisten ja osapuolten kyky tutustua tällaiseen dataan, erityisesti kun se on kerätty heidän henkilökohtaisista laitteistaan tai laitteistostaan, yleisen tietosuojaa-asetuksen mukaisesti, mutta myös heidän puolustus oikeutensa toteutumiseksi heti, jos asiaan liittyy heidän oikeudellinen vastuunsa;
5. korostaa, että on tärkeää lisätä rikosoikeudellisissa asioissa käytettävien tekoälyjärjestelmien avoimuutta, jotta mahdollistetaan oikeudellinen valvonta, ja varmistaa, että tekoälyn ja siihen liittyvän teknologian kehittäjät toteuttavat algoritmien ja algoritmien tuottamien päätösten riittävän avoimuuden toimivaltaisten viranomaisten ja kansalaisten hyödyksi; korostaa osapuolten yleistä oikeutta saada tutustua prosesseihin, jotka liittyvät datan keruuseen, rikosten ehkäisemisessä käytettäviin ennusteisiin, rikosoikeudellisen todistusaineiston luettelointiin ja arviointiin sekä sen määrittämiseen, voiko epäilty olla vaaraksi yhteiskunnalle, ellei sitä rajoiteta voimassa olevalla EU:n lainsäädännöllä, kuten direktiivillä (EU) 2016/680³; korostaa lisäksi, että on tärkeää päästä käsiksi tekoälyn tuottamiin tai tekoälyn avulla tuotettuihin tuotoksiin ja viime kädessä määritellä vastuu ilmoitusmenettelyistä sekä tekoälyn ja siihen liittyvän teknologian rooli rikosasioiden käsittelyssä, erityisesti kun on kyse suurten todistusmäärien analysoinnista rikostutkinnassa ja rikoksesta epäiltyjen tai rikoksen uhrien tunnistamisesta; muistuttaa sellaisten kysymysten merkityksestä, jotka liittyvät tekoälyn ja siihen liittyvän teknologian hallintoon, perusoikeuksiin ja menettelyllisiin takeisiin, syrjimättömyyteen, vastuuvollisuuteen, avoimuuteen, puolueettomuuteen, oikeudenmukaisuuteen ja älylliseen rehellisyyteen, ja korostaa samalla tarvetta varmistaa ihmisen suorittama valvonta kaikkina aikoina; vaatii, että oikeusviranomaiset on veloitettava perustelemaan päätöksensä, myös silloin, kun käytetään tekoälyä hyödyntävän teknologian tarjoamia todisteita, jotka edellyttävät tiukkaa oikeudellista valvontaa ja tiukkoja hyväksyttävyysskriteerejä, robotiikasta 16. helmikuuta 2017

² Euroopan parlamentin ja neuvoston direktiivi 2002/58/EY, annettu 12. heinäkuuta 2002, henkilötietojen käsittelystä ja yksityisyyden suojasta sähköisen viestinnän alalla (EYVL L 201, 31.7.2002, s. 37).

³ Euroopan parlamentin ja neuvoston direktiivi (EU) 2016/680, annettu 27. huhtikuuta 2016, luonnollisten henkilöiden suojelusta toimivaltaisten viranomaisten suorittamassa henkilötietojen käsittelyssä rikosten ennalta estämistä, tutkimista, paljastamista tai rikoksiin liittyviä syytetoimia tai rikosoikeudellisten seuraamusten täytäntöönpanoa varten sekä näiden tietojen vapaasta liikkuvuudesta (EUVL L 119, 4.5.2016, s. 89).

antamansa päätöslauselman⁴ mukaisesti, jossa korostetaan, että kaikkien tekoälyn avulla tehtyjen päätösten, joilla voi olla vaikutusta yhden tai useamman henkilön elämään, perusteet olisi aina oltava mahdollista esittää; muistuttaa, että on erotettava tekoälyn ja siihen liittyvän teknologian käyttö rikosten ehkäisemisessä ja rikosoikeuden alalla; korostaa, että tekoälyteknologialla on aina oltava toissijainen rooli;

6. muistuttaa, että tekoälyn ja siihen liittyvän teknologian, kuten laajamittainen valvonta, profilointi ja sellaiset ennakoivaan poliisitoimintaan liittyvät ohjelmat, joilla voitaisiin arvioida, missä rikos todennäköisesti tapahtuu, missä uhrit todennäköisesti sijaitsevat, mikä on henkilön todennäköisyys joutua uhriksi, olla altis rikokselle, tulla ilmoitetuksi kadonneeksi tai joutua perheväkivallan tai seksuaalirikoksen uhriksi tai olla tällaisten rikosten tekijä, sekä oikeudenmukaista menettelyä koskevien oikeuksien rikkominen, vakavimmat väärinkäyttötavat voivat olla lähtöisin viranomaisista, jotka harjoittavat lainvalvontaa;
7. korostaa, että todisteiden keräämisessä ja analysoinnissa on tärkeää käyttää automaattisesti tuotettua dataa; muistuttaa, että sekä rikosten ehkäisemisessä että rikosoikeudessa virheet data-analyysissa ja sen tulkinnassa tai sen mahdollinen väärinkäytös voivat aiheutua siihen liittyvästä inhimillisestä tekijästä, ja kehottaa siksi noudattamaan varovaisuutta, kun analysoidaan tekoälyteknologian käytön vaikuttavuutta ja asianmukaisuutta kaikissa päätöksentekoprosesseissa;
8. kehottaa kaikkia toimivaltaisia viranomaisia, erityisesti lainvalvontaviranomaisia, kuten poliisia ja oikeuslaitosta, tiedottamaan kansalaisille tekoälyn ja siihen liittyvän teknologian käytöstä näiden viranomaisten toimivaltuuksien toteuttamisessa erityisesti rikosoikeusasioissa;
9. pitää keskeisenä, että tekoälyjärjestelmien soveltaminen rikosoikeudellisen menettelyn yhteydessä takaa rikosoikeudellisen menettelyn perusperiaatteiden, kuten oikeus oikeudenmukaiseen oikeudenkäyntiin, syyttömyysolettamaa koskeva periaate ja oikeus tehokkaisuuteen oikeussuojakeinoihin noudattamisen sekä automaattisten päätöksentekojärjestelmien seurannan ja riippumattoman valvonnan varmistamisen;
10. pitää tärkeänä ihminen määrää -periaatetta sekä tekoälypohjaisten tai -avusteisten tuloksien varmentamista; muistuttaa hallintaan, avoimuuteen, selitettävyyteen ja vastuuvollisuuteen liittyvien kysymysten tärkeydestä, jotta varmistetaan perusoikeuksien noudattaminen ja vältetään mahdolliset virheet tekoälyssä;
11. korostaa suhtautuvansa varovaisesti biometrisen tunnistusohjelmiston käyttöön; tuo esiin epäselvyyden, joka johtuu luontaisista puutteista tietosuoja alalla sekä tietosuojaan loukkauksista; pitää huolestuttavana ulkomaisten harjoittamaa EU:n kansalaisten henkilötietojen kokoamista, joka toteutetaan yksityissektorin kehittäjien ja tarjoajien välityksellä;
12. muistuttaa, että nykyisten EU:n tietosuojasääntöjen ja unionin perusoikeuskirjan mukaisesti tekoälyä voidaan käyttää biometriseen etätunnistukseen vain silloin, kun tällainen käyttö on asianmukaisesti perusteltua ja oikeasuhteista ja siihen sovelletaan

⁴ Euroopan parlamentin päätöslauselma, annettu 16. helmikuuta 2017, suosituksista komissiolle robotiikkaa koskevista yksityisoikeudellisista säännöistä (EUVL C 252, 18.7.2018, s. 239).

riittäviä suojatoimia; suhtautuu myönteisesti tekoälyä käsittelevän komission korkean tason asiantuntijaryhmän suosituksiin biometrisen tunnistusteknologian oikeasuhteisesta, harkitusta ja riskiperusteisesta käytöstä henkilötietosuojaa koskevan lainsäädännön mukaisesti; ehdottaa, että tällaisen teknologian soveltamisen on oltava selvästi perusteltu voimassa olevassa lainsäädännössä, ja kehottaa komissiota arvioimaan, miten nämä suositukset voidaan ottaa tehokkaasti huomioon, kiinnittäen erityistä huomiota yksityisyyden takaavaan oikeuteen ja henkilötietojen suojaan;

13. on vahvasti sitä mieltä, että tekoälyn tai siihen liittyvän teknologian tuottamiin päätöksiin erityisesti oikeus- ja lainvalvonta-aloilla, joilla niillä on suora ja merkittävä vaikutus luonnollisten tai oikeushenkilöiden oikeuksiin ja velvollisuuksiin, olisi sovellettava tiukkaa ihmisen tekemää varmistusta ja asianmukaista prosessia;
14. pitää tarpeellisena tarkastella, onko tarkoituksenmukaista voida delegoida lainvalvontapäätökset osittain tekoälylle, ja jos näin on, missä olosuhteissa ja missä yhteyksissä tällainen tekoälyn käyttö voitaisiin sallia; katsoo, että on suhtauduttava erittäin varovaisesti sellaiseen tekoälyyn ja siihen liittyvään teknologiaan, jolla voidaan korvata viranomaispäätökset; korostaa, että on kehitettävä tiukkoja eettisiä periaatteita ja käytäntösääntöjä tekoälyn suunnittelua ja käyttöä varten, jotta voidaan tukea lainvalvojia ja oikeusviranomaisia siinä tapauksessa, että lainvalvontapäätöksiä delegoitaisiin tekoälylle; viittaa oikeudellisten asioiden valiokunnan meneillään olevaan työhön.

**TIEDOT HYVÄKSYMISESTÄ
LAUSUNNON ANTAVASSA VALIOKUNNASSA**

Hyväksytty (pvä)	10.9.2020
Lopullisen äänestyksen tulos	+: 22 -: 3 0: 0
Lopullisessa äänestyksessä läsnä olleet jäsenet	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
Lopullisessa äänestyksessä läsnä olleet varajäsenet	Heidi Hautala, Emil Radev

**LOPULLINEN ÄÄNESTYS NIMENHUUTOÄÄNESTYKSENÄ
LAUSUNNON ANTAVASSA VALIOKUNNASSA**

22	+
EPP	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
---	---

Symbolien selitys:

+ : puolesta

- : vastaan

0 : tyhjää

**TIEDOT HYVÄKSYMISESTÄ
ASIESTA VASTAAVASSA VALIOKUNNASSA**

Hyväksytty (pvä)	29.6.2021
Lopullisen äänestyksen tulos	+: 36 -: 24 0: 6
Lopullisessa äänestyksessä läsnä olleet jäsenet	Magdalena Adamowicz, Konstantinos Arvanitis, Malik Azmani, Katarina Barley, Fernando 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 Skytvedal, 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
Lopullisessa äänestyksessä läsnä olleet varajäsenet	Tanja Fajon, Miguel Urbán Crespo

**LOPULLINEN ÄÄNESTYS NIMENHUUTOÄÄNESTYKSENÄ
ASIASTA VASTAAVASSA VALIOKUNNASSA**

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, Dragoș 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-Rareș 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

Symbolien selitys:

+ : puolesta

- : vastaan

0 : tyhjää