



PRIIMTI TEKSTAI

P9_TA(2021)0405

Dirbtinis intelektas baudžiamojoje teisėje ir jo naudojimas policijoje ir teisminėse institucijose baudžiamosiose bylose

2021 m. spalio 6 d. Europos Parlamento rezoliucija dėl dirbtinio intelekto baudžiamojoje teisėje ir jo naudojimo policijos ir teisminių institucijų reikmėms baudžiamosiose bylose (2020/2016(INI))

Europos Parlamentas,

- atsižvelgdamas į Europos Sąjungos sutartį, ypač į jos 2 ir 6 straipsnius, ir į Sutartį dėl Europos Sąjungos veikimo, ypač į jos 16 straipsnį,
- atsižvelgdama į Europos Sąjungos pagrindinių teisių chartiją (toliau – Chartija), ypač į jos 6, 7, 8, 11, 12, 13, 20, 21, 24 ir 47 straipsnius,
- atsižvelgdamas į Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvenciją,
- atsižvelgdamas į Europos Tarybos konvenciją dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu (ETS 108) ir į ją iš dalies keičiantį protokolą („Konvencija 108+“),
- atsižvelgdamas į Europos Tarybos Europos veiksmingo teisingumo komisijos (CEPEJ) Europos dirbtinio intelekto naudojimo teismų sistemose ir jų aplinkoje etikos chartiją,
- atsižvelgdamas į 2019 m. balandžio 8 d. Komisijos komunikatą „Pasitikėjimo į žmogų orientuotu dirbtiniu intelektu didinimas“ (COM(2019)0168),
- atsižvelgdamas į 2019 m. balandžio 8 d. Komisijos Aukšto lygio ekspertų grupės dirbtinio intelekto klausimais patikimo dirbtinio intelekto etikos gaires,
- atsižvelgdamas į 2020 m. vasario 19 d. Komisijos baltąją knygą „Dirbtinis intelektas. Europos požiūris į kompetenciją ir pasitikėjimą“ (COM(2020)0065),
- atsižvelgdamas į 2020 m. vasario 19 d. Komisijos komunikatą „Europos duomenų strategija“ (COM(2020)0066),
- atsižvelgdamas į 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentą (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis

duomenų apsaugos reglamentas)¹,

- atsižvelgdamas į 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos direktyvą (ES) 2016/680 dėl fizinių asmenų apsaugos kompetentingoms institucijoms tvarkant asmens duomenis nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas arba bausmių vykdymo tikslais ir dėl laisvo tokių duomenų judėjimo, ir kuria panaikinamas Tarybos pamatinis sprendimas 2008/977/TVR²,
- atsižvelgdamas į 2018 m. spalio 23 d. Europos Parlamento ir Tarybos reglamentą (ES) 2018/1725 dėl fizinių asmenų apsaugos Sąjungos institucijoms, organams, tarnyboms ir agentūroms tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo, kuriuo panaikinamas Reglamentas (EB) Nr. 45/2001 ir Sprendimas Nr. 1247/2002/EB³,
- atsižvelgdamas į 2002 m. liepos 12 d. Europos Parlamento ir Tarybos direktyvą 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje (Direktyva dėl privatumo ir elektroninių ryšių)⁴,
- atsižvelgdamas į 2016 m. gegužės 11 d. Europos Parlamento ir Tarybos reglamentą (ES) 2016/794 dėl Europos Sąjungos teisėsaugos bendradarbiavimo agentūros (Europol), kuriuo pakeičiami ir panaikinami Tarybos sprendimai 2009/371/TVR, 2009/934/TVR, 2009/935/TVR, 2009/936/TVR ir 2009/968/TVR⁵,
- atsižvelgdamas į 2020 m. birželio 19 d. rezoliuciją dėl antirasistinių protestų po George'o Floyd'o mirties⁶,
- atsižvelgdamas į savo 2017 m. kovo 14 d. rezoliuciją „Didelių duomenų kiekių poveikis pagrindinėms teisėms: privatumas, duomenų apsauga, nediskriminavimas, saugumas ir teisėsauga“⁷,
- atsižvelgdamas į 2020 m. vasario 20 d. Piliečių laisvių, teisingumo ir vidaus reikalų (LIBE) komiteto klausymą dėl dirbtinio intelekto baudžiamojoje teisėje ir jo naudojimo policijos ir teisminių institucijų reikmėms baudžiamosiose bylose,
- atsižvelgdamas į 2020 m. vasario mėn. LIBE komiteto komandiruotės į Jungtines Amerikos Valstijas ataskaitą,
- atsižvelgdamas į Darbo tvarkos taisyklių 54 straipsnį,
- atsižvelgdamas į Vidaus rinkos ir vartotojų apsaugos komiteto ir Teisės reikalų komiteto nuomones,
- atsižvelgdamas į Piliečių laisvių, teisingumo ir vidaus reikalų komiteto pranešimą (A9-0232/2021),

¹ OL L 119, 2016 5 4, p. 1.

² OL L 119, 2016 5 4, p. 89.

³ OL L 295, 2018 11 21, p. 39.

⁴ OL L 201, 2002 7 31, p. 37.

⁵ OL L 135, 2016 5 24, p. 53.

⁶ OL C 362, 2021 9 8, p. 63.

⁷ OL C 263, 2018 7 25, p. 82.

- A. kadangi skaitmeninės technologijos apskritai ir ypač duomenų tvarkymo ir analizavimo paplitimas dėl dirbtinio intelekto kelia išskirtinius lūkesčius ir riziką; kadangi pastaraisiais metais plėtojant dirbtinį intelektą buvo toli pažengta į priekį ir dirbtinis intelektas tapo viena iš strateginių XXI amžiaus technologijų, galinčių duoti didelės naudos veiksmingumo, tikslumo ir patogumo aspektais, taigi, jis teigiamai keičia visuomenę, tačiau kartu kelia didžiulę riziką pagrindinėms teisėms ir demokratijai, grindžiamoms teisinės valstybės principais; kadangi dirbtinis intelektas neturėtų būti tikslas pats savaime, o žmonėms pasitarnauti skirta priemonė, kurios pagrindinė paskirtis – didinti žmonių gerovę, jų galimybes ir saugumą;
- B. kadangi, nepaisant nuolatinės pažangos kompiuterinio apdorojimo greičio ir atminties talpos srityse, dar nepavyko sukurti programų, kurios atitiktų žmogaus lankstumą dirbant platesnėse srityse ar atliekant užduotis, kurioms reikia konteksto suvokimo ar kritinės analizės; kadangi kai kurios dirbtinio intelekto taikomosios programos pasiekė žmonių ekspertų ir specialistų našumo lygį atliekant tam tikras konkrečias užduotis (pavyzdžiui, teisės technologijos) ir gali pateikti rezultatus daug greičiau ir platesniu mastu;
- C. kadangi kai kurios šalys, įskaitant keletą valstybių narių, daugiau nei kitos šalys naudoja dirbtinio intelekto taikomąsias programas arba įterptąsias dirbtinio intelekto sistemas teisės saugos sistemoje ir teisminėse institucijose, ir taip iš dalies yra dėl reglamentavimo stokos ir reglamentavimo skirtumų, dėl kurių dirbtinio intelekto naudojimas tam tikrais tikslais gali būti leidžiamas arba draudžiamas; kadangi vis dažnesnis dirbtinio intelekto naudojimas baudžiamojoje teisėje visų pirma yra grindžiamas lūkesčiais, kad tai padės sumažinti tam tikrų rūšių nusikalstamumą ir lems objektyvesnių sprendimų priėmimą; kadangi vis dėlto šie lūkesčiai ne visada pasiteisina;
- D. kadangi Chartijoje įtvirtintos pagrindinės teisės ir laisvės turėtų būti užtikrinamos per visą dirbtinio intelekto ir susijusių technologijų gyvavimo ciklą, visų pirma jų kūrimo, plėtojimo, diegimo ir naudojimo metu, ir turėtų būti visuomet taikomos užtikrinant teisės aktų vykdymą;
- E. kadangi dirbtinio intelekto technologijos turėtų būti kuriamos pirmiausia atsižvelgiant į žmones, užsitarnautų visuomenės pasitikėjimą ir visuomet tarnautų žmonėms; kadangi dirbtinio intelekto sistemoms turėtų būti suteikta svarbiausia garantija, kad jos būtų sukurtos taip, kad jas žmogus visada galėtų išjungti;
- F. kadangi dirbtinio intelekto sistemos turi būti sukurtos visų žmonių apsaugai ir naudai (kūrimo proceso metu atsižvelgiant taip pat ir į pažeidžiamas, marginalizuotas gyventojų grupes), turi būti nediskriminacinės, saugios, jų sprendimai turi būti paaiškinami ir skaidrūs, taip pat turi būti gerbiamas žmonių autonomiškumas ir pagrindinės teisės tam, kad tokios sistemos būtų patikimos, kaip nurodyta Aukšto lygio ekspertų grupės dirbtinio intelekto klausimais etikos gairėse,
- G. kadangi Sąjungai kartu su valstybėmis narėmis tenka esminė atsakomybė užtikrinti, kad sprendimai, susiję su dirbtinio intelekto taikomųjų programų gyvavimo ciklu ir naudojimu teismų veiklos ir teisės saugos srityse, būtų priimami skaidriai, visapusiškai apsaugotų pagrindines teises ir visų pirma neįtvirtintų esamos diskriminacijos, šališkumo ar išankstinio nusistatymo; kadangi priimant atitinkamus politinius sprendimus turėtų būti laikomasi būtinumo ir proporcingumo principų, siekiant užtikrinti konstitucingumą ir teisingą bei humanišką teisingumo sistemą;

- H. kadangi dirbtinio intelekto taikomosios programos gali suteikti daug galimybių teisėsaugos srityje, visų pirma gerinant teisėsaugos ir teisminių institucijų darbo metodus ir veiksmingiau kovojant su tam tikrų rūšių nusikaltimais, visų pirma finansiniais nusikaltimais, pinigų plovimu, teroristų finansavimu, seksualine prievarta prieš vaikus ir seksualiniu jų išnaudojimu internete, taip pat tam tikrų rūšių elektroniniais nusikaltimais, taip prisidedant prie ES piliečių saugos ir saugumo, nors jos taip pat kelia didelę grėsmę pagrindinėms žmonių teisėms; kadangi bet koks bendras dirbtinio intelekto naudojimas masinio sekimo tikslais būtų neproporcingas;
- I. kadangi kuriant ir naudojant dirbtinio intelekto sistemas policijos ir teisminių institucijų reikmėms reikia daugelio skirtingų subjektų, organizacijų, įrenginių komponentų, programinės įrangos algoritmų ir juos naudojančių žmonių indėlio dažnai sudėtingomis ir problemiškomis aplinkybėmis; kadangi dirbtinio intelekto taikomųjų programų naudojimas teisėsaugos ir teisminėse institucijose yra skirtinguose vystymo etapuose – nuo konceptualizacijos, prototipų kūrimo ir vertinimo iki naudojimo po patvirtinimo; kadangi ateityje gali atsirasti naujų galimybių, nes šios technologijos dėl visame pasaulyje vykdomų mokslinių tyrimų tampa vis brandesnės;
- J. kadangi būtinas aiškus teisinės atsakomybės už galimą žalingą dirbtinio intelekto sistemų poveikį baudžiamosios teisės srityje priskyrimo modelis; kadangi šios srities reguliavimo nuostatomis visada turėtų būti užtikrinama žmogaus atskaitomybė ir jomis visų pirma turi būti siekiama nesukelti jokio žalingo poveikio;
- K. kadangi atsakomybė užtikrinti visišką pagrindinių teisių laikymąsi, kai dirbtinio intelekto sistemos naudojamos teisėsaugos srityje, galiausiai tenka valstybėms narėms;
- L. kadangi pagrindinių teisių užtikrinimo ir veiksmingo viešosios tvarkos palaikymo santykio klausimas visada yra svarbus diskusijose dėl dirbtinio intelekto naudojimo teisėsaugos sektoriuje, kuriame sprendimai gali turėti ilgalaikių padarinių asmenų gyvybei ir laisvei; kadangi tai yra itin svarbu, nes dirbtinis intelektas gali tapti nuolatine baudžiamosios teisės ekosistemos dalis atliekant tiriamąją analizę ir teikiant pagalbą;
- M. kadangi teisėsaugos institucijos naudoja dirbtinį intelektą tokiose taikomose programose kaip veido atpažinimo technologijos, pvz., ieškant įtariamų asmenų duomenų bazėse ir nustatant prekybos žmonėmis ar vaikų seksualinio išnaudojimo ir prievartos aukas, automatinis transporto priemonės registracijos numerio atpažinimas, kalbėtojo tapatybės nustatymas, sakytinės kalbos atpažinimas, lūpų judesių nuskaitymo technologijos, garsinės aplinkos stebėjimas (t. y. šūvio garso aptikimo algoritmai), savarankiški nustatytų duomenų bazių tyrimai ir analizė, prognozavimas (kriminologiniu prognozavimu grindžiamas policijos darbas ir nusikalstamumo centrų analizė), elgsenos nustatymo priemonės, pažangios virtualiosios autopsijos priemonės, padedančios nustatyti mirties priežastį, savarankiškos finansinio sukčiavimo ir teroristų finansavimo nustatymo priemonės, socialinės žiniasklaidos stebėsena (duomenų perėmimas ir rinkimas siekiant sudaryti duomenų gavybos rinkinius) ir automatinės stebėjimo sistemos, apimančios įvairias nustatymo galimybes (pavyzdžiui, širdies plakimo nustatymą ir termines kameras); kadangi minėtų taikomųjų programų, kartu su kitokiu galimu ar būsimu dirbtinio intelekto technologijų taikymu teisėsaugoje, patikimumas bei tikslumas ir poveikis pagrindinėms teisėms ir baudžiamojo teisingumo sistemų dinamikai gali labai skirtis; kadangi daugelis šių priemonių yra naudojamos ES nepriklausančiose šalyse, tačiau jos būtų neteisėtos pagal Sąjungos duomenų apsaugos teisės *acquis* ir teismų praktiką; kadangi įprastas algoritmų diegimas, net ir esant mažai

klaidingai teigiamų rezultatų daliai, gali lemti klaidingus perspėjimus, nors bus pateikta kur kas daugiau teisingų perspėjimų;

- N. kadangi dirbtinio intelekto priemonės ir taikomosios programos ne vienoje šalyje visame pasaulyje naudojamos ir teisminėse institucijose, be kita ko, priimant sprendimus dėl kardomojo kalinimo, priimant nuosprendžius, apskaičiuojant recidyvo tikimybę ir nustatant lygtinį paleidimą, sprendžiant ginčus internetu, valdant teismų praktiką ir sudarant lengvesnes sąlygas naudotis teisės aktais; kadangi tai lėmė iškreiptas ir mažesnes nebaltaodžių ir kitų mažumų galimybes; kadangi šiuo metu Europos Sąjungoje, išskyrus kelias valstybes nares, jos daugiausia naudojamos tik civilinėse bylose;
- O. kadangi dirbtinio intelekto naudojimas teisėsaugos srityje kelia potencialiai didelės, o kai kuriais atvejais nepriimtinos įvairios rizikos asmenų pagrindinių teisių apsaugai, pavyzdžiui, susijusios su neskaidriu sprendimų priėmimu, įvairių rūšių diskriminacija ir klaidomis, būdingomis pagrindiniam algoritmui, kurį galima sustiprinti grįžtamuoju tarpusavio poveikiu, taip pat pavojumi privatumo ir asmens duomenų apsaugai, saviraiškos ir informacijos laisvės apsaugai, nekaltumo prezumpcijai, teisei į veiksmingą teisinę gynybą ir teisingą bylos nagrinėjimą, taip pat rizikos asmenų laisvei ir saugumui;
- P. kadangi teisėsaugos ir teisminių institucijų naudojamos dirbtinio intelekto sistemos taip pat yra pažeidžiamos, turint omenyje išpuolius, vykdomus prieš informacines sistemas pasitelkiant dirbtinį intelektą, arba duomenų užkrėtimą (angl. *data poisoning*), kai įtraukiamas neteisingas duomenų rinkinys siekiant gauti neobjektyvius rezultatus; kadangi tokiais atvejais padaryta žala gali būti dar didesnė ir lemti eksponentiškai didesnę žalą tiek asmenims, tiek grupėms;
- Q. kadangi dirbtinio intelekto diegimas teisėsaugos srityje ir teisminių institucijų reikmėms neturėtų būti laikomas vien techniškai įgyvendinama galimybe, bet politiniu sprendimu dėl teisėsaugos ir baudžiamosios teisenos sistemų struktūros ir tikslų; kadangi šiuolaikinė baudžiamoji teisė yra grindžiama idėja, kad valdžios institucijos reaguoja į pažeidimą tik tada, kai jis jau yra įvykdytas, nedarant prielaidos, kad visi žmonės yra pavojingi ir juos reikia nuolat stebėti, kad būtų užkirstas kelias galimam pažeidimui; kadangi dirbtiniu intelektu grindžiami sekimo metodai kelia didelį pavojų šiam požiūriui ir dėl to būtina, kad teisės aktų leidėjai visame pasaulyje nuodugniai įvertintų leidimo diegti technologijas, mažinančias žmogaus vaidmenį teisėsaugos ir teismo sprendimų priėmimo procesuose, pasekmes;
- 1. pakartoja, jog turint omenyje tai, kad didelio kiekio asmens duomenų tvarkymas yra dirbtinio intelekto pagrindas, teisė į privataus gyvenimo apsaugą ir teisė į asmens duomenų apsaugą taikomos visose dirbtinio intelekto srityse ir kad turi būti visapusiškai laikomasi Sąjungos duomenų apsaugos ir privatumo teisinės sistemos; todėl primena, kad teisėsaugos srityje ES jau yra nustačiusi duomenų apsaugos standartus, kurie yra būtimo dirbtinio intelekto naudojimo teisėsaugos srityje ir teisminių institucijų reikmėms reglamentavimo pagrindas; primena, kad asmens duomenų tvarkymas turėtų būti teisėtas ir sąžiningas, duomenų tvarkymo tikslai turėtų būti konkretūs, aiškūs ir legitimūs, duomenų tvarkymas turėtų būti adekvatus, reikalingas ir neviršyti tikslo, kuriuo jie tvarkomi, jis turėtų būti tikslus, nuolat atnaujinamas ir netikslūs duomenys, išskyrus atvejus, kai taikomi apribojimai, turėtų būti ištaisomi arba ištrinami, duomenys neturėtų būti saugomi ilgiau nei būtina, turėtų būti nustatyti aiškūs ir tinkami tokių

duomenų ištrynimo arba periodiškai tokių duomenų saugojimo poreikio peržiūros terminai ir jie turėtų būti tvarkomi saugiai; taip pat pabrėžia, kad turėtų būti užkirstas kelias galimam asmenų tapatybės nustatymui naudojant dirbtinio intelekto taikomąją programą, naudojant duomenis, kurie prieš tai buvo nuasmeninti;

2. dar kartą patvirtina, kad visi dirbtinio intelekto sprendimai teisėsaugos ir teismų srityse taip pat turi visapusiškai atitikti žmogaus orumo, nediskriminavimo, judėjimo laisvės, nekaltumo prezumpcijos ir teisės į gynybą, įskaitant teisę į tylėjimą, saviraiškos ir informacijos laisvės, susirinkimų ir asociacijų laisvės, lygybės prieš įstatymą, procesinės lygybės, teisės į veiksmingą teisinę gynybą ir teisingą bylos nagrinėjimą principus, laikantis Chartijos ir Europos žmogaus teisių konvencijos; pabrėžia, kad dirbtinio intelekto programų naudojimas turi būti draudžiamas, jeigu jis nesuderinamas su pagrindinėmis teisėmis;
3. pripažįsta, kad dėl spartos, kuria visame pasaulyje kuriamos dirbtinio intelekto taikomosios programos, neįmanoma sudaryti išsamaus jų sąrašo, todėl reikia aiškaus ir nuoseklaus valdymo modelio, kuriuo būtų užtikrintos pagrindinės asmenų teisės ir teisinis aiškumas kūrėjams, atsižvelgiant į nuolatinę technologijų raidą; vis dėlto, atsižvelgdamas į policijos ir teisminių institucijų vaidmenį ir užduotis, taip pat į sprendimų, kuriuos jos priima nusikalstamų veikų prevencijos, tyrimo, nustatymo ar traukimo baudžiamajon atsakomybėn už jas arba baudžiamųjų sankcijų vykdymo tikslais, poveikį, mano, kad dirbtinio intelekto taikomųjų programų naudojimas turi būti laikomas didele rizika tais atvejais, kai yra galimybė daryti didelį poveikį asmenų gyvenimui;
4. atsižvelgdamas į tai, mano, kad bet kokios teisėsaugos arba teisminių institucijų sukurtos arba naudojamos dirbtinio intelekto priemonės turėtų būti bent jau saugios, tvarios, patikimos ir atitinkančios paskirtį, jos turi atitikti sąžiningumo, duomenų kiekio mažinimo, atskaitomybės, skaidrumo, nediskriminavimo ir paaiškinamumo principus, ir kad jos turėtų būti kuriamos, diegiamos ir naudojamos tik atlikus rizikos vertinimą ir griežtą būtinumo ir proporcingumo patikrą, o apsaugos priemonės turi būti proporcingos nustatyta rizikai; pabrėžia, kad piliečių pasitikėjimas ES kuriamu, diegiamu ir naudojamu dirbtiniu intelektu priklauso nuo visiško šių kriterijų įgyvendinimo;
5. pripažįsta teigiamą tam tikrų rūšių dirbtinio intelekto taikomųjų programų indėlį į teisėsaugos ir teisminių institucijų darbą visoje Sąjungoje; kaip į pavyzdį, atkreipia dėmesį į patobulintą teismų praktikos valdymą, kuris buvo sustiprintas taikant papildomas paieškos galimybes suteikiančias priemones; mano, kad yra daug kitų galimų dirbtinio intelekto naudojimo teisėsaugos ir teisminėse institucijose galimybių, kurias būtų galima išnagrinėti atsižvelgiant į penkis CEPEJ priimtos Europos dirbtinio intelekto naudojimo teismų sistemose ir jų aplinkoje etikos chartijos principus ir ypatingą dėmesį skiriant CEPEJ nustatytiems naudojimo atvejams, kurie turi būti vertinami kiek įmanoma apdairiau;
6. pabrėžia, kad visos technologijos gali būti modifikuotos, todėl ragina nustatyti griežtą teisėsaugos ir teisminių institucijų naudojamų dirbtiniu intelektu paremtų technologijų, ypač tų, kurios gali būti modifikuotos ir panaudotos masinio sekimo arba masinio profiliavimo tikslais, demokratinę kontrolę bei nepriklausomą priežiūrą; todėl labai susirūpinęs atkreipia dėmesį į tam tikrų dirbtinio intelekto technologijų, naudojamų teisėsaugos sektoriuje masinio sekimo tikslais, potencialą; atkreipia dėmesį į teisinį reikalavimą užkirsti kelią masiniam stebėjimui naudojant dirbtinio intelekto

technologijas, kurios iš esmės neatitinka būtinumo ir proporcingumo principų, ir uždrausti naudoti taikomas programas, kurios galėtų tai lemti;

7. pabrėžia, kad kai kuriose ES nepriklausančiose šalyse taikomas požiūris į masinio sekimo technologijų kūrimą, diegimą ir naudojimą neproporcingai pažeidžia pagrindines teises, todėl ES jo neturi laikytis; todėl pabrėžia, kad apsaugos nuo teisės saugos ir teisminių institucijų piktnaudžiavimo dirbtinio intelekto technologijomis priemonės taip pat turi būti vienodai reglamentuojamos visoje Sąjungoje;
8. pabrėžia šališkumo ir diskriminacijos, atsirandančių naudojant dirbtinio intelekto taikomas programas, pvz., mašinų mokymąsi, įskaitant algoritmus, kuriais tokios taikomosios programos grindžiamos, potencialą; pažymi, kad šališkumą gali lemti pagrindiniai duomenų rinkiniai, ypač kai naudojami ankstesni duomenys, tokį šališkumą gali nustatyti algoritmų kūrėjai arba jis gali atsirasti diegiant sistemas realiomis sąlygomis; atkreipia dėmesį į tai, kad dirbtinio intelekto taikomųjų programų teikiams rezultatams visada turi įtakos naudojamų duomenų kokybė ir kad toks būdingas šališkumas linkęs palaipsniui didėti ir taip įtvirtinti ir sustiprinti esamą diskriminaciją, ypač tam tikrų etninių grupių ar rasinės diskriminacijos paveiktų bendruomenių diskriminaciją;
9. pabrėžia, kad daugelis dabartinių algoritminių identifikavimo technologijų neproporcingai neteisingai nustato ir klasifikuoja, taigi daro žalą skirtingų rasių asmenims, tam tikroms etninėms bendruomenėms priklausantiems asmenims, LGBTI asmenims, vaikams ir vyresnio amžiaus žmonėms, taip pat moterims; primena, kad asmenys ne tik turi teisę būti teisingai identifikuoti, bet ir teisę būti visiškai neidentifikuoti, išskyrus atvejus, kai to reikalaujama pagal teisės aktus siekiant įtikinamo ir teisėto viešojo intereso; pabrėžia, kad konkrečių grupių asmenų savybėmis pagrįstas dirbtinio intelekto prognozavimas sustiprina ir atkartoja esamas diskriminacijos formas; mano, kad reikėtų dėti tvirtas pastangas siekiant išvengti automatizuotos diskriminacijos ir šališkumo; ragina imtis tvirtų papildomų apsaugos priemonių, kai teisės saugos ar teisminėse institucijose dirbtinio intelekto sistemos yra naudojamos nepilnamečiams arba yra su jais susijusios;
10. atkreipia dėmesį į asimetrišką jėgų pusiausvyrą tarp subjektų, naudojančių dirbtinio intelekto technologijas, ir subjektų, kuriems šios technologijos daro įtaką; pabrėžia, jog nepaprastai svarbu užtikrinti, kad teisės saugos ir teisminių institucijų naudojamos dirbtinio intelekto priemonės netaptų nelygybės, socialinio susiskaldymo ar atskirties veiksniais; atkreipia dėmesį į dirbtinio intelekto priemonių naudojimo poveikį įtariamųjų teisėms į gynybą, į tai, kad sunku gauti prasmingos informacijos apie šių priemonių veikimą ir dėl to atsirandančius sunkumus ginčijant jų pateiktus rezultatus teisme, ypač asmenims, kurių atžvilgiu atliekamas tyrimas;
11. ypač atkreipia dėmesį į riziką, kuri susijusi su duomenų nutekėjimu, duomenų saugumo pažeidimais ir neteisėta prieiga prie asmens duomenų ar kitos, pavyzdžiui, su baudžiamosios veikos tyrimais ar teismo bylomis susijusios informacijos, kuri tvarkoma naudojant dirbtinio intelekto sistemas; pabrėžia, kad teisės saugos srityje ar teisminių institucijų naudojamų dirbtinio intelekto sistemų saugumo ir saugos aspektai turi būti atidžiai apsvarstyti ir būti pakankamai patikimi bei atsparūs, kad būtų užkirstas kelias galimai katastrofiškoms piktavališkų išpuolių prieš dirbtinio intelekto sistemas pasekmėms; pabrėžia integruotojo saugumo ir konkrečios žmogaus vykdomos priežiūros svarbą prieš pradedant naudoti tam tikras svarbias programas, todėl ragina

teisėsaugos ir teismines institucijas naudoti tik tas dirbtinio intelekto taikomasias programas, kurios atitinka privatumo ir duomenų apsaugos principą, kad būtų išvengta nemotyvuoto nukrypimo nuo funkcijų (angl. *function creep*);

12. pabrėžia, kad jokiai teisėsaugos ir teisminių institucijų naudojamai dirbtinio intelekto sistemai neturėtų būti suteikta galimybė pakenkti žmonių fiziniam neliečiamumui, paskirstyti teises ar nustatyti teises prievolos asmenims;
13. pripažįsta, kad sunku teisingai nustatyti vietą, kurioje kyla atsakomybė už galimą žalą, atsižvelgiant į dirbtinio intelekto programų kūrimo ir veikimo sudėtingumą; mano, kad būtina sukurti aiškią ir teisingą tvarką, pagal kurią būtų nustatomi teisiniai įsipareigojimai ir atsakomybė už galimus neigiamus šių pažangių skaitmeninių technologijų sukeltus padarinius; tačiau pabrėžia, kad svarbiausias tikslas turi būti bet kokių tokių pasekmių atsiradimo prevencija; todėl ragina įgyvendinti atsargumo principą visose teisėsaugos naudojamose dirbtinio intelekto taikomosiose programose; pabrėžia, kad teisiniai įsipareigojimai ir atsakomybė visada turi tekti fiziniam arba juridiniam asmeniui, kuris visada turi būti identifikuojamas priimant sprendimus naudojantis dirbtiniu intelektu; todėl pabrėžia, kad reikia užtikrinti įmonių, kurios kuria ir valdo dirbtinio intelekto sistemas, struktūrų skaidrumą;
14. mano, kad tiek siekiant veiksmingai naudotis gynybos teisėmis, tiek užtikrinti nacionalinių baudžiamosios teisenos sistemų skaidrumą būtina sukurti konkrečią, aiškią ir tikslią teisinę sistemą, kuria būtų reglamentuojamos dirbtinio intelekto priemonių naudojimo teisėsaugos srityje ir teisminėse institucijose sąlygos, metodai ir pasekmės, taip pat susijusių asmenų teisės ir veiksmingos bei lengvai prieinamos skundų nagrinėjimo ir teisių gynimo procedūros, įskaitant teisminių teisių gynimą; pabrėžia baudžiamojo proceso šalių teisę susipažinti su duomenų rinkimo procesu ir susijusiais vertinimais, atliktais arba gautais naudojant dirbtinio intelekto taikomasias programas; pabrėžia, kad būtina, jog teisminiame bendradarbiavime dalyvaujančios vykdančiosios institucijos, priimdamos sprendimus dėl ekstradicijos (ar perdavimo) į kitą valstybę narę ar ES nepriklausančią šalį, įvertintų, ar dirbtinio intelekto priemonių naudojimas prašančioje šalyje nekelia akivaizdus pavojaus pagrindinei teisei į teisingą bylos nagrinėjimą; ragina Komisiją paskelbti rekomendacijas, kaip atlikti tokį vertinimą vykdant teisminį bendradarbiavimą baudžiamosiose bylose; primygtinai reikalauja, kad valstybės narės, laikydamosi taikytinų teisės aktų, užtikrintų, kad asmenys būtų informuojami, kai teisėsaugos arba teisminės institucijos jų atžvilgiu naudoja dirbtinio intelekto taikomasias programas;
15. pabrėžia, kad žmonės nebegalės atlikti nepriklausomo vertinimo, jei pasikliaus tik mašinų sukurtais duomenimis, profiliais ir rekomendacijomis; pabrėžia, kad pernelyg didelis asmenų pasitikėjimas iš pažiūros objektyviomis ir mokslinėmis dirbtinio intelekto priemonėmis neatsižvelgiant į tai, kad jų rezultatai gali būti neteisingi, neišsamūs, neaktualūs ar diskriminaciniai ir gali turėti sunkių neigiamų padarinių, ypač teisėsaugos ir teisingumo srityse; pabrėžia, kad nereikėtų pernelyg pasikliauti dirbtinio intelekto sistemų teikiamais rezultatais ir kad valdžios institucijos turi didinti pasitikėjimą ir žinias, kad būtų galima suabejoti algoritminėmis rekomendacijomis ar jų nepaisyti; mano, kad svarbu turėti realių lūkesčių dėl tokių technologinių sprendimų ir nežadėti, kad teisėsaugos sprendimai bus tobuli ir visos padarytos nusikalstamos veikos bus nustatytos;
16. pabrėžia, kad teismų ir teisėsaugos srityje kiekvieną sprendimą, turintį teisinį ar panašų

poveikį, visada turi priimti žmogus, kurio atsakomybės už priimtus sprendimus galėtų būti reikalaujama; mano, kad asmenys, kurių atžvilgiu pasitelkiamos dirbtiniu intelektu grindžiamos sistemos, turi turėti galimybę imtis taisomųjų veiksmų; primena, kad pagal ES teisę asmuo turi teisę į tai, kad jam nebūtų taikomas sprendimas, kuris jam sukelia teisinių pasekmių arba daro jam didelį poveikį ir kuris grindžiamas tik automatizuotu duomenų tvarkymu; taip pat pabrėžia, kad automatizuotas atskirų sprendimų priėmimas negali būti grindžiamas specialių kategorijų asmens duomenimis, nebent yra nustatytos tinkamos priemonės duomenų subjekto teisėms bei laisvėms ir teisėtiems interesams apsaugoti; pažymi, kad ES teisės aktais draudžiamas profiliavimas, kuris lemia fizinių asmenų diskriminaciją atsižvelgiant į specialias asmens duomenų kategorijas; pabrėžia, kad sprendimai teisėsaugos srityje beveik visada turi teisinį poveikį atitinkamam asmeniui dėl vykdomojo teisėsaugos institucijų ir jų veiksmų pobūdžio; pažymi, kad dirbtinio intelekto naudojimas gali daryti įtaką žmonių sprendimams ir turėti poveikį visais baudžiamojo proceso etapais; todėl mano, kad dirbtinio intelekto sistemomis besinaudojančios institucijos turi laikytis itin aukštų teisinių standartų ir užtikrinti žmogaus įsikišimą, ypač analizuojant iš tokių sistemų gautus duomenis; todėl reikalauja, kad būtų išlaikyta suvereni teisėjų veiksmų laisvė ir galimybė priimti sprendimus kiekvienu konkrečiu atveju; ragina uždrausti naudoti dirbtinio intelekto ir susijusias technologijas tam, kad jos siūlytų teismo sprendimus;

17. ragina užtikrinti algoritmų paaiškinamumą, skaidrumą, atsekamumą ir tikrinimą, kaip būtiną priežiūros elementą, siekiant užtikrinti, kad teismams ir teisėsaugai skirtų dirbtinio intelekto sistemų kūrimas, diegimas ir naudojimas atitiktų pagrindines teises ir jomis pasitikėtų piliečiai, taip pat siekiant užtikrinti, kad dirbtinio intelekto algoritmų generuotus rezultatus būtų galima padaryti suprantamus naudotojams ir tiems, kuriems taikomos šios sistemos, ir kad būtų užtikrintas duomenų šaltinių skaidrumas ir tai, kaip sistema padarė tam tikrą išvadą; atkreipia dėmesį į tai, kad siekiant užtikrinti techninį skaidrumą, tvarumą ir tikslumą, Sąjungos teisėsaugos ar teisminės institucijos turėtų turėti galimybę įsigyti tik tokias priemones ir sistemas, kurių algoritmus ir logiką galima patikrinti ir kurios būtų prieinamos bent jau policijai ir teismams, taip pat nepriklausomiems auditoriams, kad jie galėtų jas įvertinti, audituoti ir tikrinti, o pardavėjai neturėtų jų uždaryti ar pažymėti, kad jos yra jų nuosavybė; be to, pabrėžia, kad turėtų būti aiškia bei suprantama kalba pateikiami dokumentai apie paslaugos pobūdį, sukurtas priemonės, veiklos rezultatus ir sąlygas, kurioms esant jos turėtų veikti, bei riziką, kurią jos gali sukelti; todėl ragina teismines ir teisėsaugos institucijas aktyviai užtikrinti visišką privačių įmonių, teikiančių joms dirbtinio intelekto sistemas teisėsaugos ir teisingumo reikmėms, skaidrumą; todėl rekomenduoja, kai įmanoma, naudoti atvirojo kodo programinę įrangą;
18. ragina teisėsaugos ir teismines institucijas nustatyti ir įvertinti sritis, kuriose tam tikri specialiai pritaikyti dirbtinio intelekto sprendimai galėtų būti naudingi, ir keistis geriausia dirbtinio intelekto diegimo patirtimi; ragina valstybes nares ir ES agentūras patvirtinti atitinkamas teisėsaugos ar teismų institucijose naudojamų dirbtinio intelekto sistemų viešojo pirkimo procedūras, siekiant užtikrinti, kad jos atitiktų pagrindines teises ir taikomus teisės aktus, be kita ko, užtikrinant, kad programinės įrangos dokumentai ir algoritmai būtų pateikiami ir prieinami kompetentingoms ir priežiūros institucijoms peržiūrėti; visų pirma ragina nustatyti privalomas taisykles, pagal kurias būtų reikalaujama viešai skelbti informaciją apie viešojo ir privačiojo sektorių partnerystes, sutartis ir pirkimus, taip pat apie jų įsigijimo tikslą; pabrėžia, kad institucijoms reikia skirti reikiamą finansavimą, taip pat suteikti būtiną kompetenciją, kad būtų užtikrintas visapusiškas su bet koku dirbtinio intelekto diegimu susijusių

etinių, teisinių ir techninių reikalavimų laikymasis;

19. ragina užtikrinti dirbtinio intelekto sistemų ir jų veikimą lemiančių sprendimų priėmimo procesų atsekamumą, kuris padėtų apibrėžti sistemų pajėgumus ir trūkumus ir stebėti, kaip atsiranda esminiai sprendimo elementai remiantis privaloma dokumentacija; pabrėžia, kad svarbu visuomet dokumentuoti mokymų duomenis, jų kontekstą, paskirtį, tikslumą ir šalutinį poveikį, taip pat algoritmų kūrėjų ir plėtotojų atliekamą šių duomenų tvarkymą ir jų atitiktį pagrindinėms teisėms; pabrėžia, kad visada turi būti įmanoma dirbtinio intelekto sistemos skaičiavimus sumažinti iki žmonėms suprantamos formos;
20. ragina prieš įgyvendinant ar diegiant visas dirbtinio intelekto sistemas, skirtas teisėsaugos ar teisminėms institucijoms, atlikti privalomą poveikio pagrindinėms teisėms vertinimą, siekiant įvertinti bet kokią galimą riziką pagrindinėms teisėms; primena, kad išankstinis duomenų apsaugos poveikio vertinimas vykdant visų rūšių duomenų tvarkymo veiklą yra privalomas, visų pirma naudojant naujausias technologijas, nes kyla galimos didelės rizikos fizinių asmenų teisėms ir laisvėms grėsmė, ir mano, kad tai ypač aktualu daugumos teisėsaugos srityje ir teisminių institucijų reikmėms naudojamų dirbtinio intelekto technologijų atveju; pabrėžia duomenų apsaugos institucijų ir pagrindinių teisių agentūrų kompetenciją vertinant šias sistemas; pabrėžia, kad šie poveikio pagrindinėms teisėms vertinimai turėtų būti atliekami kuo atviriau ir aktyviai dalyvaujant pilietinei visuomenei; reikalauja, kad poveikio vertinimuose taip pat būtų aiškiai apibrėžtos apsaugos priemonės, būtinos siekiant pašalinti nustatytą riziką, ir kad jos būtų kuo plačiau viešai paskelbtos prieš įdiegiant bet kokią dirbtinio intelekto sistemą;
21. pabrėžia, kad tik patikimas Europos dirbtinio intelekto valdymas kartu su nepriklausomu vertinimu sudarytų sąlygas būtinam pagrindinių teisių principų įgyvendinimui; ragina reguliariai atlikti privalomą visų dirbtinio intelekto sistemų, kurias naudoja teisėsaugos ir teisminės institucijos ir kai jos gali turėti didelės įtakos asmenų gyvenimui, auditą, kurį turi atlikti nepriklausoma institucija, kad būtų patikrintos ir įvertintos veikiančios algoritminės sistemos, jų kontekstas, paskirtis, tikslumas, našumas ir mastas, siekiant nustatyti, iširti, diagnozuoti ir ištaisyti bet kokią nepageidaujamą ir neigiamą poveikį, taip pat užtikrinti, kad dirbtinio intelekto sistemos veiktų taip, kaip numatyta; todėl ragina šiuo tikslu sukurti aiškią institucinę sistemą, įskaitant tinkamą reguliavimą ir priežiūrą, siekiant užtikrinti visapusišką įgyvendinimą ir užtikrinti visapusiškai informacija pagrįstas demokratines diskusijas dėl dirbtinio intelekto būtinybės ir proporcingumo baudžiamosios teisenos srityje; pabrėžia, kad šių auditų rezultatai turi būti skelbiami viešuosiuose registruose, kad piliečiai žinotų, kad yra diegiamos dirbtinio intelekto sistemos ir kokių priemonių imamasi siekiant pašalinti bet kokius pagrindinių teisių pažeidimus;
22. pabrėžia, kad duomenų rinkiniai ir algoritminės sistemos, naudojamos klasifikavimui, vertinimui ir prognozavimui skirtingais duomenų tvarkymo etapais kuriant dirbtinio intelekto ir susijusias technologijas taip pat gali lemti skirtingą traktavimą ir tiesioginę bei netiesioginę žmonių grupių diskriminaciją, ypač dėl to, kad duomenys, naudojami nusikalstamumo prognozavimo algoritmo mokymui atspindi vykdomo stebėjimo prioritetus, todėl galiausiai gali atkartoti ir sustiprinti esamą šališkumą; todėl pabrėžia, kad dirbtinio intelekto technologijos, ypač tos, kurios diegiamos teisėsaugos ir teisminių institucijų reikmėms, reikalauja tarpdisciplininių tyrimų ir indėlio, įskaitant mokslinius ir technologinius tyrimus, esminius su rasių klausimais susijusius tyrimus, neįgalumo tyrimus ir kitas socialiniams mokslams priskiriamas disciplinas, įskaitant skirtumų

kūrimo nustatymo būdus, klasifikavimo veikimą ir jo pasekmes; todėl pabrėžia, kad reikia sistemingai investuoti į šių disciplinų integravimą į visus dirbtinio intelekto mokslo darbus ir mokslinius tyrimus visais lygmenimis; taip pat pabrėžia, jog svarbu, kad dirbtinio intelekto sistemos teisėsaugos ir teisingumo reikmėms kuriančios, vystančios, testuojančios, prižiūrinčios, diegiančios ir jas įsigyjančios komandos, kai įmanoma, bendrai atspindėtų visuomenės įvairovę kaip netechinę diskriminacijos rizikos mažinimo priemonę;

23. taip pat pabrėžia, kad siekiant užtikrinti tinkamą atskaitomybę, įsipareigojimų laikymąsi ir atsakomybę būtina rengti svarbius specializuotus mokymus, kuriuose būtų nagrinėjamos dirbtinio intelekto technologijos etinės nuostatos, galimi pavojai, apribojimai ir tinkamas jų naudojimas, visų pirma policijos ir teisminių institucijų darbuotojams; pabrėžia, kad teikiant tinkamą sprendimus priimančių asmenų profesinį mokymą ir keliant jų kvalifikaciją reikėtų mokyti apie šališkumo galimybes, nes duomenų rinkiniai gali būti grindžiami diskriminaciniais ir išankstinėmis nuostatomis pagrįstai duomenimis; remia informuotumo didinimo ir švietimo iniciatyvas, siekiant užtikrinti, kad teisėsaugos ir teisminės institucijose dirbantys darbuotojai žinotų ir suvoktų naudojamų dirbtinio intelekto sistemų apribojimus, jų teikiamas galimybes ir keliamas grėsmes, įskaitant automatizuoto šališkumo riziką; primena, kad policijos pajėgų, vykdančių savo pareigas, rasizmo atvejų įtraukimas į dirbtinio intelekto mokymo duomenų rinkinius neišvengiamai lems rasistinį šališkumą dirbtinio intelekto sukurtuose rezultatuose, vertinimuose ir rekomendacijose; todėl pakartoja raginimą valstybėms narėms skatinti kovos su diskriminacija politikos kryptis ir parengti nacionalinius kovos su rasizmu veiksmų planus viešosios tvarkos palaikymo ir teisingumo sistemos srityje;
24. pažymi, kad nusikalstamumo prognozavimas yra vienas iš teisėsaugoje naudojamų dirbtinio intelekto naudojimo būdų, tačiau įspėja, kad jos gali padėti teisėsaugos institucijoms veiksmingiau ir aktyviau dirbti, bet įspėja, kad nors nusikalstamumo prognozavimo technologijos gali analizuoti tam tikrus duomenis, kad nustatytų modelius ir sąsajas, jos negali nustatyti priežastinio ryšio, taip pat negali rengti patikimų asmens elgesio prognozių, todėl negali būti laikomos vienintele intervencijos priemone; pažymi, kad keletas Jungtinių Amerikos Valstijų miestų nutraukė kriminologinio prognozavimo sistemų naudojimą po to, kai buvo atliktas auditas; primena, kad 2020 m. vasario mėn. vykusios Piliečių laisvių, teisingumo ir vidaus reikalų komiteto misijos į Jungtines Amerikos Valstijas metu komiteto nariai gavo iš Niujorko ir Kembridžo miesto Masačusetse policijos departamentų informaciją, kad jie sustabdė kriminologinio prognozavimo sistemų naudojimą dėl veiksmingumo stokos, diskriminacinio poveikio ir praktinio netinkamumo ir perėjo prie viešosios tvarkos palaikymo bendruomenės pastangomis; pažymi, kad tai lėmė nusikalstamumo sumažėjimą; todėl prieštarauja tam, kad teisėsaugos institucijos naudotų dirbtinį intelektą, kad, remiantis istoriniais duomenimis ir ankstesniu elgesiu, priklausymu grupėms, vieta ar bet kokiais kitais tokiais požymiais, būtų teikiamos asmenų ar grupių elgesio prognozės, taip mėginant nustatyti asmenis, kurie gali padaryti nusikaltimą;
25. atkreipia dėmesį į skirtingus veido atpažinimo būdus, pvz., patikrinimą ir (arba) tapatumo nustatymą (t. y. gyvo asmens palyginimą su nuotrauka asmens tapatybės dokumente, pvz., pažangiai valdomos sienos), tapatybės nustatymą (t. y. nuotraukos palyginimą su tam tikra nuotraukų duomenų baze) ir aptikimą (t. y. veido atvaizdų aptikimą realiuoju laiku iš tokių šaltinių, kaip AVSS įrašai, ir jų palyginimą su duomenų bazėmis, pvz., stebėjimas realiuoju laiku), kurių kiekvienas turi skirtingą poveikį

pagrindinių teisių apsaugai; yra tvirtai įsitikinęs, kad veido atpažinimo sistemų diegimas teisėsaugos srityje turėtų būti vykdomas tik aiškiai apibrėžtais tikslais, visapusiškai laikantis proporcingumo ir būtinumo principų bei galiojančių teisės aktų; dar kartą patvirtina, kad naudojant veido atpažinimo technologijas turi būti laikomasi bent jau duomenų kiekio mažinimo, duomenų tikslumo, jų saugojimo apribojimo, duomenų saugumo ir atskaitomybės reikalavimų ir kad toks naudojimas turi būti teisėtas, skaidrus ir atitikti konkretų, aiškų bei teisėtą tikslą, aiškiai apibrėžtą valstybės narės ar Sąjungos teisės aktuose; laikosi nuomonės, kad tikrinimo ir tapatumo nustatymo sistemos gali būti toliau diegiamos ir sėkmingai naudojamos tik tuo atveju, jei jų neigiamas poveikis gali būti sumažintas ir tenkinami pirmiau nurodyti kriterijai;

26. be to, ragina visam laikui uždrausti naudoti automatizuotą analizę ir (arba) viešai prieinamose erdvėse atpažinti kitus žmogaus požymius, pvz., eiseną, pirštų atspaudus, DNR, balsą ir kitas biometrines bei elgsenos savybes;
27. vis dėlto ragina paskelbti veido atpažinimo sistemų, kurios atlieka identifikavimo funkciją, nebent jos naudojamos tik nusikaltimo aukoms identifikuoti, diegimo teisėsaugos tikslais moratoriumą tol, kol techniniai standartai galės būti pripažinti visiškai atitinkančiais pagrindines teises, gauti rezultatai bus nešališki ir nediskriminaciniai, teisinėje sistemoje bus numatytos griežtos apsaugos priemonės dėl netinkamo naudojimo ir griežta demokratinė kontrolė bei priežiūra ir bus pateikta empirinių įrodymų dėl tokių technologijų diegimo būtinumo ir proporcingumo; pažymi, kad tais atvejais, kai pirmiau minėti kriterijai netenkinami, sistemos neturėtų būti naudojamos ar diegiamos;
28. reiškia didelį susirūpinimą tuo, kad teisėsaugos ir žvalgybos tarnybos naudoja privačias veido atpažinimo duomenų bazes, pvz., „Clearview“ dirbtinio intelekto technologiją, kurios duomenų bazėje yra nelegaliai sukaupta daugiau kaip trys milijardai iš socialinių tinklų ir kitų interneto vietų gautų nuotraukų, įskaitant ES piliečių nuotraukas; ragina valstybės nares įpareigoti teisėsaugos subjektus atskleisti, ar jie naudojami „Clearview“ dirbtinio intelekto technologija ar kita lygiaverte kitų tiekėjų technologija; primena Europos duomenų apsaugos valdybos (EDPB) nuomonę, kad tokių paslaugų, kaip antai „Clearview“ dirbtinio intelekto technologija, naudojimas teisėsaugos institucijose Europos Sąjungoje tikriausiai būtų nesuderinamas su ES duomenų apsaugos teisės aktais; ragina uždrausti naudoti privačias veido atpažinimo duomenų bazes teisėsaugos srityje;
29. atkreipia dėmesį į Komisijos galimybių studiją dėl galimų Priumo sprendimo pakeitimų¹, taip pat susijusių su veido atvaizdais; atkreipia dėmesį į ankstesnius mokslinius tyrimus, kuriuose nurodyta, kad jokie nauji potencialūs identifikatoriai, pvz., akies rainelės ar veido atpažinimo, teismo ekspertizės srityje nebus tokie patikimi kaip DNR ar pirštų antspaudai; primena Komisijai, kad bet koks pasiūlymas dėl teisėkūros procedūra priimamo akto turi būti pagrįstas įrodymais ir atitikti proporcingumo principą; primygtinai ragina Komisiją išplėsti Priumo sprendimo sistemą tik tuo atveju, jei bus gauta patikimų mokslinių įrodymų apie teismo ekspertizės srityje naudojamų veido atpažinimo programų patikimumą, palyginti su DNR ar pirštų antspaudais, po to, kai ji atliks visapusišką poveikio vertinimą ir atsižvelgiant į Europos duomenų apsaugos

¹ 2008 m. birželio 23 d. Tarybos sprendimas 2008/615/TVR dėl tarpvalstybinio bendradarbiavimo gerinimo, visų pirma kovos su terorizmu ir tarpvalstybiniu nusikalstamumu srityje (OL L 210, 2008 8 6, p. 1).

priežiūros pareigūno (EDAPP) ir Europos duomenų apsaugos valdybos rekomendacijas;

30. pabrėžia, kad biometrinių duomenų naudojimas plačiau susijęs su teisės į žmogaus orumą principu, kuris yra visų Chartijoje garantuojamų pagrindinių teisių pagrindas; mano, kad bet kokių biometrinių duomenų naudojimas ir rinkimas nuotolinio identifikavimo tikslais, pvz., atliekant veido atpažinimą viešosiose erdvėse, taip pat juos naudojant prie oro uostų pasienio patikros punktuose esančių automatinių sienos kontrolės vartų, gali kelti specifinę riziką pagrindinėms teisėms, o padariniai gali skirtis priklausomai nuo tikslo, aplinkybių ir naudojimo masto; be to, atkreipia dėmesį į ginčytiną afekto atpažinimo technologijų mokslinį pagrįstumą, pvz., kai teisėsaugos srityje naudojamos vaizdo kameros akių judesiams ir vyzdžio dydžio pokyčiams nustatyti; laikosi nuomonės, kad biometrinių identifikatorių naudojimas teisėsaugos ir teismų sistemoje visada turėtų būti laikomas „didele rizika“, todėl jam turėtų būti taikomi papildomi reikalavimai, kaip nurodyta Komisijos aukšto lygio ekspertų grupės dirbtinio intelekto klausimais rekomendacijose;
31. yra labai susirūpinęs dėl mokslinių tyrimų projektų, kurie finansuojami pagal programą „Horizontas 2020“ ir pagal kuriuos dirbtinio intelekto programos diegiamos prie išorinių sienų, pvz., dėl „iBorderCtrl“ projekto, vadinamosios „išmaniosios melo aptikimo sistemos“, pagal kurią keleiviai profiliuojami remiantis kompiuterinės sistemos automatiškai atliktu interviu keleivio internetinėje vaizdo kameroje, ir dėl dirbtiniu intelektu pagrįstos 38 mikrogestų analizės, išbandytos Vengrijoje, Latvijoje ir Graikijoje; todėl ragina Komisiją, taikant teisėkūros ir ne teisėkūros priemones, o prireikus – pažeidimo nagrinėjimo procedūras, uždrausti bet kokių biometrinių duomenų, įskaitant veido atvaizdus, tvarkymą teisėsaugos tikslais, kuris lemia masinio sekimo priemonių taikymą viešose erdvėse; taip pat ragina Komisiją nutraukti biometrinių mokslinių tyrimų, diegimo ar programų, kurie galėtų lemti nediferencijuotą masinį sekimą viešose erdvėse, finansavimą; atsižvelgdamas į tai pabrėžia, kad ypatingą dėmesį reikėtų skirti ir taikyti griežtą sistemą bepiločių orlaivių naudojimui policijos operacijose;
32. pritaria Komisijos aukšto lygio ekspertų grupės dirbtinio intelekto klausimais rekomendacijoms uždrausti dirbtinio intelekto pagalba vykdomą masinį asmenų reitingavimą; mano, kad bet kokia viešųjų institucijų plačiai taikoma normatyvinio piliečių reitingavimo forma, ypač teisėsaugos ir teisminėse institucijose, lemia savarankiškumo praradimą, kelia pavojų nediskriminavimo principui, ir tai negali būti laikoma suderinama su pagrindinėmis teisėmis, visų pirma, pagarba žmogaus orumui, kodifikuotomis Europos teisėse;
33. ragina užtikrinti didesnę bendrą skaidrumą, kad būtų pasiektas visapusiškas supratimas apie dirbtinio intelekto taikomųjų programų naudojimą Sąjungoje; prašo valstybių narių pateikti išsamią informaciją apie teisėsaugos ir teisminių institucijų naudojamas priemones, naudojamų priemonių rūšį, jų naudojimo paskirtį, apie tai, kokių rūšių nusikaltimams jos taikomos, ir šias priemones sukūrusių bendrovių arba organizacijų pavadinimus; ragina teisėsaugos ir teismines institucijas taip pat informuoti visuomenę ir užtikrinti pakankamą skaidrumą dėl dirbtinio intelekto ir susijusių technologijų naudojimo vykdant savo įgaliojimus, įskaitant šių technologijų klaidingai teigiamų rezultatų ir klaidingai neigiamų rezultatų rodiklių atskleidimą; prašo Komisijos surinkti ir atnaujinti informaciją vienoje vietoje; ragina Komisiją taip pat skelbti ir atnaujinti informaciją apie tai, kaip Sąjungos agentūros, kurioms pavestos teisėsaugos ir teisminės užduotys, naudoja dirbtinį intelektą; ragina Europos duomenų apsaugos valdybą

įvertinti šių dirbtinio intelekto technologijų ir taikomųjų programų, kurias naudoja teisėsaugos ir teisminės institucijos, teisėtumą;

34. primena, kad dirbtinio intelekto taikomosios programos, įskaitant teisėsaugos ir teisminėse institucijose naudojamas taikomosias programas, yra labai sparčiai vystomos pasauliniu lygmeniu; primygtinai ragina visus Europos suinteresuotuosius subjektus, įskaitant valstybes nares ir Komisiją, bendradarbiaujant tarptautiniu mastu užtikrinti partnerių už ES ribų dalyvavimą, kad būtų sugriežtinti standartai tarptautiniu lygmeniu ir sukurta bendra ir suteikianti papildomumo teisinė ir etinė dirbtinio intelekto naudojimo sistema, visų pirma skirta teisėsaugos ir teisminėms institucijoms, pagal kurią būtų visapusiškai laikomasi Chartijos, Europos duomenų apsaugos *acquis* ir gerbiamos žmogaus teisės;
35. ragina ES pagrindinių teisių agentūrą, bendradarbiaujant su Europos duomenų apsaugos valdyba ir Europos duomenų apsaugos priežiūros pareigūnu, parengti išsamias gaires, rekomendacijas ir geriausios praktikos pavyzdžius, kad būtų galima tiksliau apibrėžti dirbtinio intelekto taikomųjų programų ir sprendimų, skirtų teisėsaugos ir teisminių institucijų reikmėms, kūrimo, naudojimo ir diegimo kriterijus bei sąlygas; įsipareigoja atlikti Teisėsaugos direktyvos įgyvendinimo tyrimą¹ siekiant nustatyti, kaip teisėsaugos ir teisminės institucijos užtikrina asmens duomenų apsaugą, visų pirma kurdamos ar diegdamos naujas technologijas; be to, ragina Komisiją apsvarstyti, ar reikia imtis konkrečių teisėkūros veiksmų siekiant išsamiau apibrėžti dirbtinio intelekto taikomųjų programų ir sprendimų, skirtų teisėsaugos ir teisminių institucijų reikmėms, kūrimo, naudojimo ir diegimo kriterijus bei sąlygas;
36. paveda Pirmininkui perduoti šią rezoliuciją Tarybai ir Komisijai.

¹ 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos direktyva (ES) 2016/680 dėl fizinių asmenų apsaugos kompetentingoms institucijoms tvarkant asmens duomenis nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas arba bausmių vykdymo tikslais ir dėl laisvo tokių duomenų judėjimo, ir kuria panaikinamas Tarybos pamatinis sprendimas 2008/977/TVR (OL L 119, 2016 5 4, p. 89).