

srijeda, 6. listopada 2021.

P9_TA(2021)0405

Umjetna inteligencija u kaznenom pravu i njezina primjena od strane policije i pravosudnih tijela u kaznenim stvarima**Rezolucija Europskog parlamenta od 6. listopada 2021. o umjetnoj inteligenciji u kaznenom pravu i njezinoj primjeni od strane policije i pravosudnih tijela u kaznenim stvarima (2020/2016(INI))**

(2022/C 132/02)

Europski parlament,

- uzimajući u obzir Ugovor o Europskoj uniji, a posebno njegove članke 2. i 6., kao i Ugovor o funkcioniranju Europske unije, a posebno njegov članak 16.,
- uzimajući u obzir Povelju Europske unije o temeljnim pravima („Povelja”), a posebno njezine članke 6., 7., 8., 11., 12., 13., 20., 21., 24. i 47.,
- uzimajući u obzir Konvenciju za zaštitu ljudskih prava i temeljnih sloboda,
- uzimajući u obzir Konvenciju Vijeća Europe za zaštitu pojedinaca u vezi s automatskom obradom osobnih podataka (ETS 108) i njezin protokol o izmjeni (Konvencija 108+),
- uzimajući u obzir Europsku etičku povelju Europske komisije za učinkovitost pravosuđa (CEPEJ) Vijeća Europe o upotrebi umjetne inteligencije u pravosudnim sustavima i povezanim područjima,
- uzimajući u obzir komunikaciju Komisije od 8. travnja 2019. naslovljenu „Izgradnja povjerenja u antropocentričnu umjetnu inteligenciju” (COM(2019)0168),
- uzimajući u obzir etičke smjernice za pouzdanu umjetnu inteligenciju koje je 8. travnja 2019. objavila Komisijina stručna skupina na visokoj razini za umjetnu inteligenciju,
- uzimajući u obzir bijelu knjigu Europske komisije od 19. veljače 2020. naslovljenu „Umjetna inteligencija – europski pristup izvrsnosti i povjerenju” (COM(2020)0065),
- uzimajući u obzir komunikaciju Komisije od 19. veljače 2020. pod naslovom „Europska strategija za podatke” (COM(2020)0066),
- uzimajući u obzir Uredbu (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka) ⁽¹⁾,
- uzimajući u obzir Direktivu (EU) 2016/680 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka od strane nadležnih tijela u svrhe sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Okvirne odluke Vijeća 2008/977/PUP ⁽²⁾,
- uzimajući u obzir Uredbu (EU) 2018/1725 Europskog parlamenta i Vijeća od 23. listopada 2018. o zaštiti pojedinaca u vezi s obradom osobnih podataka u institucijama, tijelima, uredima i agencijama Unije i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Uredbe (EZ) br. 45/2001 i Odluke br. 1247/2002/EZ ⁽³⁾,
- uzimajući u obzir Direktivu 2002/58/EZ Europskog parlamenta i Vijeća od 12. srpnja 2002. o obradi osobnih podataka i zaštiti privatnosti u području elektroničkih komunikacija („Direktiva o privatnosti i elektroničkim komunikacijama”) ⁽⁴⁾,

⁽¹⁾ SL L 119, 4.5.2016., str. 1.⁽²⁾ SL L 119, 4.5.2016., str. 89.⁽³⁾ SL L 295, 21.11.2018., str. 39.⁽⁴⁾ SL L 201, 31.7.2002., str. 37.

srijeda, 6. listopada 2021.

- uzimajući u obzir Uredbu (EU) 2016/794 Europskog parlamenta i Vijeća od 11. svibnja 2016. o Agenciji Europske unije za suradnju tijela za izvršavanje zakonodavstva (Europol) te zamjeni i stavljanju izvan snage odluka Vijeća 2009/371/PUP, 2009/934/PUP, 2009/935/PUP, 2009/936/PUP i 2009/968/PUP ⁽⁵⁾,
 - uzimajući u obzir svoju rezoluciju od 19. lipnja 2020. o prosvjedima protiv rasizma nakon smrti Georgea Floyda ⁽⁶⁾,
 - uzimajući u obzir svoju Rezoluciju od 14. ožujka 2017. o utjecaju velikih podataka na temeljna prava: privatnost, zaštita podataka, nediskriminacija, sigurnost i kazneni progon ⁽⁷⁾,
 - uzimajući u obzir saslušanje Odbora za građanske slobode, pravosuđe i unutarnje poslove (LIBE) od 20. veljače 2020. o umjetnoj inteligenciji u kaznenom pravu i njezinoj upotrebi od strane policije i pravosudnih tijela u kaznenim stvarima,
 - uzimajući u obzir izvješće o službenom putovanju odbora LIBE u Sjedinjene Američke Države u veljači 2020.,
 - uzimajući u obzir članak 54. Poslovnika,
 - uzimajući u obzir mišljenje Odbora za unutarnje tržište i zaštitu potrošača te Odbora za pravna pitanja,
 - uzimajući u obzir izvješće Odbora za građanske slobode, pravosuđe i unutarnje poslove (A9-0232/2021),
- A. budući da digitalne tehnologije općenito, a posebno širenje obrade i analize podataka koje omogućuje umjetna inteligencija, nude iznimna obećanja, ali donose i rizike; budući da je posljednjih godina zabilježen velik skok u razvoju umjetne inteligencije, koja je postala jedna od strateških tehnologija 21. stoljeća s potencijalom za stvaranje znatnih koristi u učinkovitosti, točnosti i prikladnosti, što donosi pozitivne promjene za europsko gospodarstvo i društvo, ali i goleme rizike za temeljna prava i demokracije zasnovane na vladavini prava; budući da umjetnu inteligenciju ne bi trebalo promatrati zasebno nego kao sredstvo koje treba služiti ljudima za ostvarenje krajnjeg cilja – povećanje dobrobiti ljudi, njihovih sposobnosti i njihove sigurnosti;
- B. budući da, unatoč stalnom napretku u pogledu brzine računalne obrade i kapaciteta memorije, još ne postoje programi koji bi mogli zamijeniti ljudsku fleksibilnost u širim domenama ili u zadacima koji zahtijevaju razumijevanje konteksta ili kritičku analizu; budući da su neke primjene umjetne inteligencije postigle razinu učinkovitosti ljudskih stručnjaka i profesionalaca u obavljanju određenih zadaća (npr. pravna tehnologija) te da mogu polučiti rezultate drastično brže i u širem razmjeru;
- C. budući da se neke zemlje, uključujući nekoliko država članica, u kaznenom progonu i pravosuđu više koriste primjenama umjetne inteligencije ili ugrađenim sustavima umjetne inteligencije od drugih, što je djelomično posljedica nedostatka propisa i regulatornih razlika kojima se omogućuje ili zabranjuje upotreba umjetne inteligencije u određene svrhe; budući da se umjetna inteligencija sve više upotrebljava u području kaznenog prava, u prvom redu zbog očekivanja da će se njome prorijediti određeni oblici kriminala i da će dovesti do objektivnijih odluka; budući da se ta očekivanja ne ostvare uvijek;
- D. budući da bi temeljna prava i slobode sadržane u Povelji trebalo zajamčiti tijekom cijelog životnog ciklusa umjetne inteligencije i povezanih tehnologija, posebno tijekom njihova osmišljavanja, razvoja, uvođenja i upotrebe, te da bi se trebali primjenjivati pri provedbi zakona u svim okolnostima;
- E. budući da bi se tehnologija umjetne inteligencije trebala razvijati tako da ljudi budu u središtu pozornosti, da zaslužuje povjerenje javnosti i da uvijek bude u službi ljudi; budući da bi sustavi umjetne inteligencije trebali imati krajnje sigurnosno jamstvo u smislu da su dizajnirani tako da ih ljudski operater koji njima upravlja uvijek može isključiti;
- F. budući da sustavi umjetne inteligencije trebaju biti dizajnirani za zaštitu i u korist svih članova društva (među ostalim, uzimanjem u obzir ranjivih, marginaliziranih grupa stanovništva prilikom dizajniranja), nediskriminirajući i sigurni, njihove odluke trebaju biti objašnjive i transparentne te trebaju poštovati ljudsku autonomiju i temeljna prava kako bi bili pouzdani, što je opisano u etičkim smjernicama Stručne skupine na visokoj razini za umjetnu inteligenciju;

⁽⁵⁾ SL L 135, 24.5.2016., str. 53.

⁽⁶⁾ SL C 362, 8.9.2021., str. 63.

⁽⁷⁾ SL C 263, 25.7.2018., str. 82.

srijeda, 6. listopada 2021.

- G. budući da Unija zajedno s državama članicama snosi ključnu odgovornost za jamčenje da se odluke oko životnog ciklusa i upotrebe primjena umjetne inteligencije u području pravosuđa i kaznenog progona donose na transparentan način, da se njima u potpunosti štite temeljna prava, a posebno da se njima ne perpetuira postojeća diskriminacija, pristranost ili predrasude; budući da bi se relevantnim političkim odlukama trebala poštovati načela nužnosti i proporcionalnosti kako bi se zajamčila ustavnost te pravedan i human pravosudni sustav;
- H. budući da primjene umjetne inteligencije mogu ponuditi sjajne prilike u području kaznenog progona, a osobito u poboljšanju metoda rada tijela za kazneni progon i pravosudnih tijela te u učinkovitijoj borbi protiv određenih oblika kriminala, osobito financijskog kriminala, pranja novca i financiranja terorizma, seksualnog zlostavljanja i iskorištavanja djece na internetu, kao i određenih oblika kiberkriminaliteta, čime doprinose sigurnosti i zaštiti građana EU-a, dok u isto vrijeme mogu prouzročiti znatne rizike za temeljna prava ljudi; budući da bi bilo kakva opća primjena umjetne inteligencije u svrhu masovnog nadzora bila nerazmjerna;
- I. budući da razvoj i rad sustava umjetne inteligencije za policiju i pravosudna tijela uključuje doprinose više pojedinaca, organizacija, strojnih komponenti, softverskih algoritama i ljudskih korisnika u često složenim i zahtjevnim okruženjima; budući da su primjene umjetne inteligencije u kaznenom progonu i pravosuđu u različitim fazama razvoja, od konceptualizacije preko izrade prototipa ili procjena do upotrebe nakon odobrenja; budući da bi se u budućnosti mogle pojaviti nove mogućnosti upotrebe jer tehnologije postaju zrelije zahvaljujući kontinuiranom znanstvenom istraživanju diljem svijeta;
- J. budući da je jasan model raspodjele zakonske odgovornosti za potencijalno štetne učinke sustava umjetne inteligencije u području kaznenog prava od ključne važnosti; budući da se regulatornim odredbama u tom području uvijek treba zadržati ljudska odgovornost i da se njima prije svega mora nastojati izbjeći uzrokovanje bilo kakvih štetnih učinaka;
- K. budući da je u konačnici odgovornost država članica da zajamče potpuno poštovanje temeljnih prava kada se sustavi umjetne inteligencije upotrebljavaju u području kaznenog progona i pravosuđa;
- L. budući da odnos između zaštite temeljnih prava i učinkovitog rada policije uvijek mora biti ključan element u raspravama o tome bi li se i na koji način sektor kaznenog progona trebao koristiti umjetnom inteligencijom s obzirom na to da odluke koje se donose u tom sektoru mogu imati dugotrajne posljedice za život i slobodu pojedinaca; budući da je to naročito važno jer umjetna inteligencija može biti trajni dio našeg kaznenopravnog ekosustava s obzirom na to da pruža istražnu analizu i pomoć;
- M. budući da se tijela kaznenog progona koriste umjetnom inteligencijom u primjenama poput tehnologija prepoznavanja lica, npr. za pretraživanje baza podataka o sumnjivim osobama i utvrđivanje žrtava trgovanja ljudima ili seksualnog iskorištavanja i zlostavljanja djece, automatizirano prepoznavanje registarskih tablica, prepoznavanje govornika, prepoznavanje govora, tehnologiju čitanja s usana, zvučni nadzor (tj. algoritmi prepoznavanja hitaca), autonomno istraživanje i analizu utvrđenih baza podataka, prognoziranje (prediktivno policijsko postupanje i analiza žarišta kriminala), alate za otkrivanje ponašanja, napredne virtualne alate za obdukciju koji pomažu u utvrđivanju uzroka smrti, autonomne alate za utvrđivanje financijske prijevare i financiranja terorista, praćenje društvenih medija (prikupljanje i ubiranje podataka za rudarenje veza) i automatizirane sustave nadzora koji objedinjuju različite sposobnosti otkrivanja (poput otkrivanja otkucaja srca i toplinskih kamera); budući da stupnjevi pouzdanosti i točnosti prethodno navedenih primjena, uz ostale potencijalne ili buduće primjene tehnologija umjetne inteligencije, mogu biti iznimno različiti i utjecati na zaštitu temeljnih prava i na dinamiku sustava kaznenog pravosuđa; budući da se mnogi od tih alata upotrebljavaju u zemljama izvan EU-a, dok bi u skladu s pravnom stečevinom i sudskom praksom Unije o zaštiti podataka bili nezakoniti; budući da rutinsko uvođenje algoritama, čak i uz malu stopu lažno pozitivnih rezultata, može dovesti do lažnih upozorenja koja znatno nadmašuju ispravna upozorenja;
- N. budući da se alati i primjene umjetne inteligencije upotrebljavaju i u pravosuđu nekoliko zemalja diljem svijeta, među ostalim, za potkrepljivanje odluka o pritvoru prije suđenja, pri izricanju kazni, izračunu vjerojatnosti ponavljanja kaznenog djela i pri utvrđivanju probacije, rješavanju sporova putem interneta, upravljanju sudskom praksom i omogućavanju lakšeg pristupa pravosuđu; budući da je to dovelo do iskrivljenih i smanjenih mogućnosti za nebijelce i druge manjine; budući da je u EU-u njihova upotreba trenutno ograničena uglavnom na građanske stvari, uz iznimku nekih država članica;
- O. budući da upotreba umjetne inteligencije u kaznenom progonu obuhvaća niz potencijalno visokih, a u nekim slučajevima neprihvatljivih rizika za zaštitu temeljnih prava pojedinaca, kao što su netransparentno donošenje odluka, različite vrste diskriminacije i pogreške svojstvene temeljnom algoritmu, koje se mogu povećati kanalima za povratne

srijeda, 6. listopada 2021.

informacije, kao i rizici za zaštitu privatnosti i osobnih podataka, zaštitu slobode izražavanja i informacija, pretpostavku nedužnosti, pravo na djelotvoran pravni lijek i pošteno suđenje, te rizici za slobodu i sigurnost pojedinaca;

- P. budući da su sustavi umjetne inteligencije kojima se koriste tijela kaznenog progona i pravosuđe također podložni napadima na informacijske sustave koji su potpomognuti umjetnom inteligencijom ili onečišćenju podataka, pri čemu se namjerno uključuje pogrešan skup podataka kako bi se postigli pristrani rezultati; budući da je u takvim situacijama posljedična šteta potencijalno još značajnija i može rezultirati eksponencijalno većim štetama i za pojedince i za skupine;
- Q. budući da se uvođenje umjetne inteligencije u području kaznenog progona i pravosuđa ne bi smjelo smatrati isključivo tehničkim pitanjem, već političkom odlukom o osmišljavanju i ciljevima kaznenog progona i kaznenopravnih sustava; budući da se moderno kazneno pravo temelji na ideji da vlasti reagiraju na kazneno djelo nakon njegova počinjenja, ne pretpostavljajući pritom da su svi ljudi opasni i da ih je potrebno stalno nadzirati kako bi se spriječili mogući prijestupi; budući da tehnike nadzora koje se temelje na umjetnoj inteligenciji ozbiljno dovode u pitanje taj pristup, zbog čega zakonodavci diljem svijeta hitno trebaju temeljito procijeniti posljedice uvođenja tehnologija koje umanjuju ulogu ljudi u provedbi zakona i donošenju presuda;

1. ponovno ističe da se, s obzirom na to da se umjetna inteligencija temelji na obradi velikih količina osobnih podataka, pravo na zaštitu privatnog života i pravo na zaštitu osobnih podataka primjenjuju na sva područja umjetne inteligencije te da je potrebno u potpunosti se pridržavati pravnog okvira Unije za zaštitu podataka i privatnosti; stoga podsjeća da je EU već uspostavio standarde zaštite podataka za kazneni progon, koji čine temelj za sve buduće propise o umjetnoj inteligenciji koja se upotrebljava u kaznenom progonu i pravosuđu; podsjeća da bi obrada osobnih podataka trebala biti zakonita i pravedna, da bi svrhe obrade trebale biti jasno navedene, izričite i legitimne, da bi obrada trebala biti primjerena, relevantna i ne prekomjerna u odnosu na svrhu u koju se provodi, da bi trebala biti točna, ažurna i da bi se netočni podaci trebali ispraviti ili izbrisati osim ako se primjenjuju ograničenja, da se podaci ne bi smjeli čuvati dulje nego što je potrebno, da bi trebalo utvrditi jasne i primjerene rokove za brisanje ili periodično preispitivanje potrebe za pohranom takvih podataka te da bi ih trebalo obrađivati na siguran način; također ističe da bi trebalo spriječiti moguću identifikaciju pojedinaca primjenom umjetne inteligencije koja se koristi podacima koji su prethodno bili anonimizirani;

2. ponovno potvrđuje da sva rješenja umjetne inteligencije za tijela kaznenog progona i pravosuđe trebaju u potpunosti poštovati načela ljudskog dostojanstva, nediskriminacije, slobode kretanja, pretpostavku nedužnosti i pravo na obranu, uključujući pravo na šutnju, pravo na slobodu izražavanja i informacija, slobodu okupljanja i udruživanja, jednakost pred zakonom, načelo jednakosti procesnih sredstava te pravo na djelotvoran pravni lijek i pošteno suđenje, u skladu s Poveljom i Europskom konvencijom o ljudskim pravima; naglašava da treba zabraniti primjene umjetne inteligencije ako su nespojive s temeljnim pravima;

3. priznaje da brzina razvoja primjena umjetne inteligencije diljem svijeta ne omogućuje iscrpno navođenje primjena, zbog čega je potreban jasan i dosljedan model upravljanja kojim se jamče i temeljna prava pojedinaca i pravna jasnoća za nositelje projekata s obzirom na kontinuirani razvoj tehnologije; međutim, s obzirom na ulogu i odgovornost policije i pravosudnih tijela te utjecaj njihovih odluka u svrhe sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenopravnih sankcija, smatra da se upotreba primjena umjetne inteligencije mora kategorizirati kao visokorizična u slučajevima u kojima postoji mogućnost znatnog utjecaja na živote pojedinaca;

4. u tom smislu smatra da je minimalni uvjet da svi alati umjetne inteligencije koje razviju tijela kaznenog progona i pravosudna tijela ili kojima se ta tijela koriste budu sigurni, pouzdani i prilagođeni svrsi, poštuju načela pravednosti, smanjenja količine podataka, odgovornosti, transparentnosti, nediskriminacije i objašnjivosti te da njihov razvoj, uvođenje i upotreba podliježu procjeni rizika te strogo ispitivanju nužnosti i proporcionalnosti, a zaštitni mehanizmi trebaju biti razmjerni utvrđenim rizicima; ističe da je povjerenje građana u upotrebu umjetne inteligencije koja se razvija, uvodi i upotrebljava u EU-u uvjetovano potpunim ispunjavanjem tih kriterija;

5. uviđa pozitivan doprinos određenih vrsta primjena umjetne inteligencije na rad tijela kaznenog progona i pravosudnih tijela diljem Unije; kao primjer ističe poboljšano upravljanje sudskom praksom s pomoću alata kojima se omogućuju dodatne opcije pretraživanja; smatra da postoji niz drugih mogućih primjena umjetne inteligencije za kazneni

srijeda, 6. listopada 2021.

progon i pravosuđe koje bi se mogle istražiti uzimajući u obzir pet načela Europske etičke povelje o upotrebi umjetne inteligencije u pravosudnim sustavima i povezanim područjima, koju je donijela Radna skupina Vijeća Europe za kvalitetu pravosuđa (CEPEJ), te obrađujući posebnu pozornost na „primjene koje treba razmotriti uz najveću moguću zadržku”, koje je utvrdio CEPEJ;

6. naglašava da se svaka tehnologija može prenamijeniti i stoga poziva na strogu demokratsku kontrolu i neovisni nadzor svih tehnologija omogućenih umjetnom inteligencijom kojima se koriste tijela kaznenog progona i pravosudna tijela, posebno onih koje se mogu prenamijeniti za masovni nadzor ili masovno profiliranje; stoga s velikom zabrinutošću primjećuje potencijal određenih tehnologija umjetne inteligencije koje se upotrebljavaju u sektoru kaznenog progona u svrhu masovnog nadzora; ističe pravnu obvezu sprečavanja masovnog nadzora s pomoću tehnologija umjetne inteligencije koje po definicije ne poštuju načela nužnosti i proporcionalnosti te zabrane upotrebe primjena koje bi mogle dovesti do toga;

7. naglašava da pristup koji se u nekim zemljama izvan EU-a zauzima u pogledu razvoja, uvođenja i upotrebe tehnologija masovnog nadzora nerazmjerno utječe na temeljna prava, zbog čega ga EU ne bi trebao primjenjivati; stoga ističe da mehanizmi zaštite od zlorabe tehnologije umjetne inteligencije od strane tijela kaznenog progona i pravosudnih tijela također trebaju biti jednako regulirani u cijeloj Uniji;

8. naglašava potencijal za pristranost i diskriminaciju kao rezultat upotrebe primjena umjetne inteligencije kao što je strojno učenje, uključujući algoritme na kojima se takve primjene temelje; napominje da pristranosti mogu biti svojstvene temeljnim skupovima podataka, posebice kada se upotrebljavaju povijesni podaci koje su unijeli razvojni programeri algoritama ili koji se generiraju kad se sustavi implementiraju u okruženju stvarnog svijeta; ističe da na rezultate primjena umjetne inteligencije nužno utječe kvaliteta korištenih podataka te da su takve inherentne pristranosti sklone postupnom rastu, čime se nastavlja i povećava postojeća diskriminacija, posebno za osobe koje pripadaju određenim etničkim skupinama ili etniciziranim zajednicama;

9. ističe činjenicu da mnoge algoritamski pogonjene tehnologije identifikacije koje su trenutačno u upotrebi nerazmjerno pogrešno identificiraju i klasificiraju etnicizirane osobe, pojedince koji pripadaju određenim etničkim skupinama, LGBTI osobe, djecu i starije osobe te žene i time im nanose štetu; podsjeća da pojedinci nemaju samo pravo na ispravnu identifikaciju, već i pravo da ih se uopće ne identificira, osim ako je to zakonom propisano radi važnih i legitimnih javnih interesa; naglašava da predviđanja umjetne inteligencije koja se temelje na značajkama određene skupine osoba u konačnici pojačavaju i reproduciraju postojeće oblike diskriminacije; smatra da treba uložiti velike napore kako bi se izbjegla automatizirana diskriminacija i pristranost; poziva na uvođenje pouzdanih dodatnih zaštitnih mehanizama kada se sustavi umjetne inteligencije u kaznenom progonu ili pravosuđu upotrebljavaju na maloljetnicima ili u vezi s njima;

10. ističe asimetriju moći između onih koji se koriste tehnologijama umjetne inteligencije i onih koji su im podložni; naglašava da je od ključne važnosti da upotreba alata umjetne inteligencije od strane tijela kaznenog progona i pravosudnih tijela ne postane čimbenik nejednakosti, društvenog raslojavanja ili isključenosti; ističe utjecaj upotrebe alata umjetne inteligencije na prava osumnjičenika na obranu, poteškoće u dobivanju smislenih informacija o njihovu funkcioniranju i posljedični problem osporavanja njihovih rezultata na sudu, posebno od strane pojedinaca pod istragom;

11. svjestan je rizika, naročito onih povezanih s curenjem podataka, povredama sigurnosti podataka i neovlaštenim pristupom osobnim podacima i drugim informacijama, primjerice, onima koje su povezane s kaznenim istragama ili sudskim predmetima koje obrađuju sustavi umjetne inteligencije; naglašava da treba pozorno razmotriti aspekte zaštite i sigurnosti sustava umjetne inteligencije koji se upotrebljavaju u tijelima kaznenog progona i pravosudnim tijelima te da oni trebaju biti dovoljno pouzdani i otporni da spriječe potencijalno katastrofalne posljedice zlonamjernih napada na sustave umjetne inteligencije; naglašava važnost integrirane sigurnosti, kao i specifičnog ljudskog nadzora prije upotrebe određenih ključnih primjena te stoga poziva tijela kaznenog progona i pravosudna tijela da se koriste samo primjenama umjetne inteligencije koje su u skladu s načelom integrirane privatnosti i integrirane zaštite podataka kako bi se izbjeglo nekontrolirano širenje primjene;

12. naglašava da se nijednom sustavu umjetne inteligencije koji se upotrebljava u kaznenom progonu ili pravosuđu ne bi smjelo omogućiti da nanosi štetu fizičkom integritetu ljudskih bića niti da dodjeljuje prava ili nameće pravne obveze pojedincima;

13. svjestan je izazova točnog utvrđivanja pravne odgovornosti i preuzimanja obveze za moguću štetu s obzirom na složenost razvoja i rada sustava umjetne inteligencije; smatra da je nužno stvoriti jasan i pošten režim dodjeljivanja pravne odgovornosti i preuzimanja obveza za potencijalno štetne posljedice tih naprednih digitalnih tehnologija; međutim,

srijeda, 6. listopada 2021.

naglašava da primarni cilj mora biti sprečavanje same pojave svih takvih posljedica; stoga poziva na primjenu načela predostrožnosti za sve primjene umjetne inteligencije u kontekstu kaznenog progona; ističe da pravnu odgovornost i obveze uvijek mora snositi fizička ili pravna osoba, koja se uvijek mora utvrditi kada se donose odluke uz potporu umjetne inteligencije; stoga naglašava da je potrebno zajamčiti transparentnost korporativnih struktura koje proizvode sustave umjetne inteligencije i upravljaju njima;

14. smatra da je za učinkovitost ostvarivanja prava na obranu i za transparentnost nacionalnih kazneno-pravnih sustava ključno da se konkretnim, jasnim i preciznim pravnim okvirom reguliraju uvjeti, modaliteti i posljedice upotrebe alata umjetne inteligencije u području kaznenog progona i pravosuđa, kao i prava ciljanih osoba, uključujući djelotvorne i lako dostupne postupke podnošenja pritužbi i obeštećenja, uključujući sudsku zaštitu; ističe pravo stranaka u kaznenom postupku na pristup procesu prikupljanja podataka i povezanim procjenama koje su provedene ili dobivene upotrebom primjena umjetne inteligencije; naglašava potrebu da izvršna tijela koja sudjeluju u pravosudnoj suradnji pri odlučivanju o zahtjevu za izručenje (ili predaju) drugoj državi članici ili zemlji izvan EU-a procijene bi li upotreba alata umjetne inteligencije u zemlji koja je podnijela zahtjev mogla očito ugroziti temeljno pravo na pošteno suđenje; poziva Komisiju da izda smjernice o tome kako provesti takvu procjenu u kontekstu pravosudne suradnje u kaznenim stvarima; inzistira na tome da se države članice, u skladu s mjerodavnim zakonima, pobrinu za to da pojedinci budu obaviješteni kada podliježu upotrebi primjena umjetne inteligencije od strane tijela kaznenog progona ili pravosuđa;

15. naglašava da ljudi neće moći provesti neovisnu procjenu ako se oslanjaju samo na podatke, profile i preporuke dobivene od strojeva; ističe da može doći do ozbiljnih i negativnih posljedica, osobito u području kaznenog progona i pravosuđa, u slučajevima kada pojedinci imaju previše povjerenja u naizgled objektivnu i znanstvenu prirodu alata umjetne inteligencije i ne uzimaju u obzir da rezultati tih alata mogu biti netočni, nepotpuni, nebitni ili diskriminirajući; naglašava da treba izbjegavati prekomjerno oslanjanje na rezultate sustava umjetne inteligencije i ističe da vlasti trebaju graditi povjerenje i znanje za preispitivanje ili poništavanje preporuka algoritama; smatra da je važno imati realna očekivanja u pogledu takvih tehnoloških rješenja, a ne obećavati savršena rješenja za kazneni progon i otkrivanje svih počinjenih kaznenih djela;

16. ističe da u kontekstu pravosuđa i tijela kaznenog progona, odluku s pravnim ili sličnim učinkom uvijek treba donijeti čovjek kojeg se može smatrati odgovornim za donesene odluke; smatra da bi onima koji ovise o sustavima koji se temelje na umjetnoj inteligenciji trebalo omogućiti pravni lijek; podsjeća da, u okviru prava EU-a, osoba ima pravo da se na nju ne odnosi odluka koja se temelji isključivo na automatiziranoj obradi podataka, a koja proizvodi pravne učinke za nju ili značajno na nju utječe; nadalje ističe da se automatizirano pojedinačno donošenje odluka ne smije temeljiti na posebnim kategorijama osobnih podataka, osim ako su uspostavljene odgovarajuće mjere zaštite prava i sloboda te legitimnih interesa osobe čiji se podaci obrađuju; ističe da se pravom EU-a zabranjuje profiliranje koje dovodi do diskriminacije pojedinaca na temelju posebnih kategorija osobnih podataka; naglašava da su odluke u području provedbe zakona gotovo uvijek odluke koje zbog izvršne prirode tijela kaznenog progona i njihova djelovanja imaju pravni učinak na dotičnu osobu; prima na znanje da upotreba umjetne inteligencije može utjecati na ljudske odluke i na sve faze kaznenih postupaka; stoga smatra da tijela koja se koriste sustavima umjetne inteligencije moraju poštovati visoke pravne standarde i zajamčiti ljudsku intervenciju, posebno pri analizi podataka dobivenih iz tih sustava; zahtijeva stoga suvereno diskrecijsko pravo sudaca i donošenje odluka na pojedinačnoj osnovi; poziva na zabranu uporabe umjetne inteligencije i povezanih tehnologija pri donošenju sudskih odluka;

17. poziva na algoritamsku objašnjivost, transparentnost, sljedivost i provjeru kako bi se osiguralo da su razvoj, uvođenje i upotreba sustava umjetne inteligencije u tijelima kaznenog progona i pravosuđu u skladu s temeljnim pravima te da im građani vjeruju, te kako bi se osiguralo da rezultati koje generiraju algoritmi umjetne inteligencije mogu biti razumljivi korisnicima i osobama koje o tim sustavima ovise i da postoji transparentnost izvornih podataka te načina na koji je sustav došao do određenog zaključka; ističe da bi, kako bi se zajamčila tehnička transparentnost, stabilnost i točnost, tijela kaznenog progona ili pravosudna tijela u Uniji trebala moći kupovati samo takve alate i sustave čiji algoritmi i logika podliježu reviziji te su dostupni barem policiji i pravosuđu te neovisnim revizorima, kako bi se omogućilo njihovo ocjenjivanje, revizija i provjera, a prodavači ih ne bi smjeli zatvarati niti označivati kao vlasništvo; nadalje ističe da bi trebalo osigurati dokumentaciju na jasnom i razumljivom jeziku o prirodi usluge, razvijenim alatima, izvedbi i uvjetima u kojima se može očekivati da će funkcionirati te rizicima koje bi mogli prouzročiti; stoga poziva pravosudna tijela i tijela kaznenog

srijeda, 6. listopada 2021.

progona da osiguraju proaktivnu i potpunu transparentnost u pogledu privatnih poduzeća koja ih opremaju sustavima umjetne inteligencije za potrebe kaznenog progona i pravosuđa; s tim u skladu preporučuje upotrebu softvera otvorenog koda kada je to moguće;

18. potiče tijela kaznenog progona i pravosudna tijela da utvrde i procijene područja u kojima bi neka prilagođena rješenja umjetne inteligencije mogla biti korisna te da razmjenjuju najbolje prakse o uvođenju umjetne inteligencije; poziva države članice i agencije EU-a da usvoje odgovarajuće postupke javne nabave za sustave umjetne inteligencije kada se koriste u okviru kaznenog progona ili u pravosudnom kontekstu kako bi se zajamčila njihova usklađenost s temeljnim pravima i mjerodavnim zakonodavstvom, uključujući jamstvo dostupnosti softverske dokumentacije i algoritama nadležnim i nadzornim tijelima u svrhu preispitivanja; posebno poziva na donošenje obvezujućih pravila kojima se propisuje javno objavljivanje javno-privatnih partnerstva, ugovora i preuzimanja te svrhe u koje se obrađuju; naglašava potrebu da se vlastima osiguraju potrebna financijska sredstva te da im se osigura potrebno stručno znanje kako bi se zajamčilo potpuno poštovanje etičkih, pravnih i tehničkih zahtjeva povezanih s uvođenjem umjetne inteligencije;

19. poziva da se s pomoću obvezne dokumentacije osigura sljedivost sustava umjetne inteligencije i postupaka donošenja odluka kojima se definiraju sposobnosti i ograničenja sustava te kojima se prati izvor atributa koji su definirajući za odluku; ističe da je važno u potpunosti dokumentirati podatke koji se tiču osposobljavanja, njihov kontekst, svrhu, točnost i nuspojave, kao i način na koji ih obrađuju konstruktori i programeri algoritama te njihovu usklađenost s temeljnim pravima; ističe da uvijek treba biti moguće prevesti izračune sustava umjetne inteligencije u oblik razumljiv ljudima;

20. poziva na obveznu procjenu učinka na ljudska prava prije implementacije ili uvođenja bilo kojeg sustava umjetne inteligencije u tijela kaznenog progona ili pravosuđa kako bi se procijenili svi potencijalni rizici za ljudska prava; podsjeća da je prethodna procjena učinka na zaštitu podataka obvezna za sve vrste obrade, posebno za upotrebu novih tehnologija, koja će vjerojatno predstavljati visok rizik za prava i slobode pojedinaca te smatra da je to slučaj s većinom tehnologija umjetne inteligencije u području kaznenog progona i pravosuđa; posebno ističe stručnost kojom tijela za zaštitu podataka i agencije za temeljna prava trebaju raspolagati prilikom procjene tih sustava; naglašava da bi te procjene učinka na temeljna prava trebalo provoditi na što otvoreniji način i uz aktivno sudjelovanje civilnog društva; zahtijeva da se u procjenama učinka jasno definiraju zaštitne mjere potrebne za rješavanje utvrđenih rizika te da se one u najvećoj mogućoj mjeri objave prije uvođenja bilo kakvog sustava umjetne inteligencije;

21. naglašava da samo snažno europsko upravljanje umjetnom inteligencijom popraćeno neovisnom procjenom omogućuje potrebnu operacionalizaciju načela temeljnih prava; poziva da neovisno tijelo periodično provede obveznu reviziju svih sustava umjetne inteligencije koji se upotrebljavaju u tijelima kaznenog progona ili pravosudnim tijelima kako bi se ispitali i ocijenili kontekst, svrha, točnost, uspješnost i razmjeri algoritamskih sustava nakon što budu stavljeni u rad radi utvrđivanja, ispitivanja, dijagnosticiranja i ispravljanja svih neželjenih i štetnih učinaka i kako bi se osiguralo da sustavi umjetne inteligencije rade kako bi trebali; stoga poziva na uspostavu jasnog institucijskog okvira u tu svrhu, uključujući odgovarajući regulatorni i nadzorni pregled, kako bi se osigurala potpuna provedba i zajamčila potpuno utemeljena demokratska rasprava o nužnosti i proporcionalnosti umjetne inteligencije u području kaznenog prava; ističe da bi rezultati tih revizija trebali biti dostupni u javnim registrima kako bi građani znali primjenjuju li se sustavi umjetne inteligencije i koje se mjere poduzimaju kako bi se ispravilo svako kršenje temeljnih prava;

22. naglašava da skupovi podataka i algoritamski sustavi koji se upotrebljavaju pri klasifikaciji, procjenama i predviđanjima u različitim fazama obrade podataka u razvoju umjetne inteligencije i povezanih tehnologija mogu dovesti i do različitog postupanja prema skupinama osoba sa sličnim obilježjima i njihove izravne i neizravne diskriminacije, naročito jer podaci koji se upotrebljavaju za učenje algoritama za predviđanje policijskog nadzora odražavaju sadašnje nadzorne prioritete te stoga mogu dovesti do reproduciranja i umnažanja postojećih pristranosti; naglašava stoga da tehnologija umjetne inteligencije, posebno kada se koristi u svrhu kaznenog progona i pravosuđa, iziskuje interdisciplinarna istraživanja i doprinos, uključujući znanstvene i tehnološke studije, ključne rasne studije, studije o invaliditetu i druge discipline prilagođene društvenom kontekstu, uključujući način nastanka razlika, klasifikacijski rad i njegove posljedice; stoga naglašava da je potrebno sustavno ulaganje u integraciju tih disciplina u studije i istraživanja umjetne inteligencije na svim razinama; naglašava da je također važno osigurati da timovi koji osmišljavaju, razvijaju, testiraju, održavaju, uvode i nabavljaju sustave umjetne inteligencije za tijela kaznenog progona i pravosudna tijela odražavaju, kada je to moguće, raznolikost društva općenito kao netehničkog načina za smanjenje rizika od diskriminacije;

srijeda, 6. listopada 2021.

23. ističe nadalje da odgovarajuća odgovornost, osobna i pravna odgovornost zahtijevaju značajno specijalizirano osposobljavanje u pogledu etičkih odredbi, potencijalnih opasnosti, ograničenja i pravilne upotrebe tehnologije umjetne inteligencije, posebno za policijsko i pravosudno osoblje; naglašava da bi se odgovarajućim stručnim osposobljavanjem i kvalifikacijama trebalo osigurati da su donositelji odluka osposobljeni u pogledu potencijala za pristranost, budući da se skupovi podataka mogu temeljiti na diskrimirajućim podacima i podacima na koje utječu predrasude; podržava pokretanje inicijativa za podizanje razine osviještenosti i obrazovnih inicijativa kako bi se osiguralo da su pojedinci koji rade u tijelima kaznenog progona i pravosuđu svjesni i razumiju ograničenja, sposobnosti i rizike koji proizlaze iz upotrebe sustava umjetne inteligencije, uključujući rizik od pristranosti u automatizaciji; podsjeća da će uključivanje primjera rasističkog ponašanja policijskih snaga prilikom izvršavanja dužnosti u skupove podataka za obuku sustava umjetne inteligencije neizbježno dovesti do rasističke pristranosti u nalazima, rezultatima i preporukama dobivenima umjetnom inteligencijom; stoga ponavlja svoj poziv državama članicama da u policijskom i pravosudnom sustavu promiču politike za borbu protiv diskriminacije te da razvijaju nacionalne akcijske planove protiv rasizma;

24. napominje da je prognostički rad policije među primjenama umjetne inteligencije koje se upotrebljavaju u području kaznenog progona, ali upozorava da, iako se prognostičkim policijskim aktivnostima mogu analizirati zadani skupovi podataka potrebni za utvrđivanje obrazaca i korelacija, njima se ne može odgovoriti na pitanje uzročnosti i ne može se pouzdano prognozirati individualno ponašanje te stoga ne mogu biti jedini temelj za intervenciju; ističe da je nekoliko gradova u Sjedinjenim Američkim Državama odustalo od svojih sustava predviđanja policijskog nadzora nakon revizije programa; podsjeća da su tijekom službenog putovanja odbora LIBE u Sjedinjene Američke Države u veljači 2020. policijske uprave grada New Yorka i Cambridgea, Massachusetts obavijestile zastupnike da su zbog nedostatka učinkovitosti, diskriminirajućeg učinka i neuspjeha u praksi postupno ukinule svoje programe predviđanja policijskog nadzora te su se umjesto toga okrenule radu policije u zajednici; prima na znanje da je to rezultiralo smanjenjem stope kriminala; protivni se tome da tijela kaznenog progona upotrebljavaju umjetnu inteligenciju za predviđanje ponašanja pojedinaca ili skupina na temelju arhivskih podataka i prošlog ponašanja, članstva u skupinama, lokacije ili drugih sličnih čimbenika, kojima se pokušava identificirati osobe za koje je vjerojatno da će počiniti kazneno djelo;

25. prima na znanje različite vrste upotrebe prepoznavanja lica, kao što su, među ostalim, verifikacija/autentifikacija (tj. uspoređivanje lica s fotografijom u identifikacijskoj ispravi, npr. pametne granice), identifikacija (tj. uspoređivanje fotografije s određenom bazom fotografija) i otkrivanje (tj. otkrivanje lica u stvarnom vremenu iz izvora kao što su snimke CCTV-a i njihovo uspoređivanje s bazama podataka, npr. nadzorom u stvarnom vremenu), od kojih svaka ima različite učinke na zaštitu temeljnih prava; snažno vjeruje da bi se upotreba sustava za prepoznavanje lica u tijelima kaznenog progona trebala ograničiti na jasno opravdane svrhe uz puno poštovanje načela proporcionalnosti i nužnosti te mjerodavnog prava; ponovno potvrđuje da barem upotreba tehnologije za prepoznavanje lica mora biti u skladu sa zahtjevima smanjenja količine podataka, točnosti podataka, ograničenja pohrane, sigurnosti i odgovornosti podataka te da mora biti zakonita, pravedna i transparentna te u skladu s posebnom, eksplicitnom i legitimnom svrhom koja je jasno definirana u pravu država članica ili Unije; smatra da se sustavi za verifikaciju i autentifikaciju mogu i dalje uspješno uvoditi i upotrebljavati samo ako se njihovi štetni učinci mogu ublažiti i ako su prethodno navedeni kriteriji ispunjeni;

26. nadalje poziva na trajnu zabranu korištenja automatskog analiziranja i/ili prepoznavanja ljudskih značajki u javnim prostorima primjerice hoda, otisaka prstiju, DNK, glasa i drugih biometrijskih i bihevioralnih signala;

27. poziva međutim na moratorij na upotrebu sustava za prepoznavanje lica kojima je funkcija identifikacija u svrhu kaznenog progona, osim ako se ne koriste isključivo u svrhu identifikacije žrtava kaznenog djela, dok se tehnički standardi ne budu mogli smatrati potpuno usklađenima s temeljnim pravima, dok dobiveni rezultati ne budu nepristrani i nediskriminirajući, dok zakonski okvir ne bude davao jasne zaštitne mjere protiv zlorabe i strogu demokratsku kontrolu i nadzor i dok ne bude empirijskih dokaza o nužnosti i proporcionalnosti upotrebe takvih tehnologija; napominje da se sustavi ne bi smjeli upotrebljavati ili uvoditi ako prethodno navedeni kriteriji nisu ispunjeni;

28. izražava veliku zabrinutost zbog toga što akteri kaznenog progona i obavještajne službe upotrebljavaju privatne baze podataka za prepoznavanje lica, kao što je Clearview AI, baza podataka s više od tri milijarde fotografija nezakonito prikupljenih s društvenih mreža i drugih internetskih stranica, uključujući fotografije građana EU-a; poziva države članice da obvežu aktere kaznenog progona da otkriju upotrebljavaju li tehnologiju Clearview AI ili neku istovrijednu tehnologiju iz drugih izvora; podsjeća na mišljenje Europskog odbora za zaštitu podataka da uporaba usluge kao što je Clearview AI od strane tijela kaznenog progona u Europskoj uniji „vjerojatno nije u skladu s režimom EU-a za zaštitu podataka”; poziva da se tijelima kaznenog progona zabrani upotreba privatnih baza podataka za prepoznavanje lica;

srijeda, 6. listopada 2021.

29. prima na znanje studiju izvedivosti Komisije o mogućim izmjenama odluke Prüm⁽⁸⁾, uključujući u pogledu slika lica; prima na znanje ranije istraživanje da nijedan potencijalni novi identifikator, npr. šarenica ili prepoznavanje lica, ne bi bio jednako pouzdan u forenzičkom kontekstu kao DNK ili otisci prstiju; podsjeća Komisiju da se svaki zakonodavni prijedlog mora temeljiti na dokazima i poštovati načelo proporcionalnosti; poziva Komisiju da ne proširi okvir odluke Prüm osim ako za to ne postoje čvrsti znanstveni dokazi o pouzdanosti prepoznavanja lica u forenzičkom kontekstu u usporedbi s DNK ili otiscima prstiju, i to nakon što provede cjelovitu procjenu učinka, uzimajući u obzir preporuke Europskog nadzornika za zaštitu podataka i Europskog odbora za zaštitu podataka;

30. ističe da je upotreba biometrijskih podataka u širem smislu povezana s načelom prava na ljudsko dostojanstvo, koje je osnova svih temeljnih prava koja su zajamčena Poveljom; smatra da upotreba i prikupljanje biometrijskih podataka za potrebe daljinske identifikacije, primjerice prepoznavanjem lica na javnim mjestima, kao i na izlazima za automatsku graničnu kontrolu koji se upotrebljavaju za granične kontrole u zračnim lukama, može predstavljati poseban rizik za temeljna prava čije se posljedice mogu značajno razlikovati ovisno o svrsi, kontekstu i području upotrebe; nadalje ističe spornu znanstvenu valjanost tehnologije prepoznavanja, kao što su kamere kojima se otkrivaju pokreti očiju i promjene u veličini zjenica, u području kaznenog progona; smatra da bi se upotreba biometrijske identifikacije u kontekstu kaznenog progona i pravosuđa uvijek trebala smatrati „visokorizičnom” i stoga podlijeagati dodatnim zahtjevima, u skladu s preporukama Komisijine stručne skupine na visokoj razini za umjetnu inteligenciju;

31. izražava duboku zabrinutost zbog istraživačkih projekata financiranih u okviru programa Obzor 2020. kojima se na vanjskim granicama uvodi umjetna inteligencija, kao što je projekt iBorderCtrl, „pametni sustav za otkrivanje laži” koji profilira putnika na temelju automatiziranog intervjua provedenog putem webcama prije putovanja i analize 38 mikropokreta temeljene na umjetnoj inteligenciji, koji je testiran u Mađarskoj, Latviji i Grčkoj; stoga poziva Komisiju da zakonodavnim i nezakonodavnim sredstvima te po potrebi postupcima zbog povrede prava provede zabranu svake biometrijske obrade podataka, uključujući slike lica, za potrebe kaznenog progona koji dovodi do masovnog nadzora u javno dostupnim prostorima; nadalje poziva Komisiju da prestane financirati biometrijska istraživanja, uvođenje biometrijske tehnologije ili biometrijske programe koji bi lako mogli doprinijeti neselektivnom masovnom nadzoru u javnim prostorima; u tom kontekstu ističe da bi posebnu pozornost trebalo posvetiti upotrebi bespilotnih letjelica u policijskim operacijama te da bi se za njih trebao primjenjivati strog okvir;

32. podržava preporuke stručne skupine Komisije na visokoj razini za umjetnu inteligenciju da se zabrani masovno vrednovanje pojedinaca putem umjetne inteligencije; smatra da se svakim oblikom normativnog vrednovanja građanina koji provode javna tijela, posebno u području kaznenog progona i pravosuđa, dovodi do gubitka autonomije, ugrožava načelo nediskriminacije te se ne može smatrati da je u skladu s temeljnim pravima, posebno ljudskim dostojanstvom, kako je kodificirano zakonom EU-a;

33. poziva na veću opću transparentnost kako bi se uspostavio sveobuhvatan sporazum u pogledu upotrebe primjena umjetne inteligencije u Uniji; traži od država članica da daju sveobuhvatne informacije o alatima kojima se koriste njihova tijela kaznenog progona i sudska tijela, o vrsti alata u uporabi, o svrhama u koje se koriste, o vrstama kaznenih djela na koja se primjenjuju i o nazivima društava ili organizacija koje su razvile te alate; poziva tijela kaznenog progona i pravosuđa da informiraju javnost i osiguraju dovoljnu transparentnost u pogledu uporabe umjetne inteligencije i srodnih tehnologija pri provedbi svojih ovlasti, uključujući otkrivanje lažno pozitivnih i lažno negativnih stopa predmetne tehnologije; od Komisije traži da prikupi i ažurira informacije koje bi se onda nalazile na jednom mjestu; poziva Komisiju da objavi te da ažurira informacije o uporabi umjetne inteligencije u agencijama Unije nadležnima za provedbu zakona i za ispunjavanje pravosudnih zadaća; poziva Europski odbor za zaštitu podataka da ocijeni zakonitost tih tehnologija umjetne inteligencije i načina na koji ih primjenjuju tijela kaznenog progona i pravosudna tijela;

34. podsjeća da se aplikacije umjetne inteligencije, uključujući one koje se upotrebljavaju u kontekstu kaznenog progona i pravosuđa, brzo razvijaju na globalnoj razini; potiče sve europske dionike, uključujući države članice i Komisiju, da u okviru međunarodne suradnje zajamče angažman partnera izvan EU-a kako bi se podigli standardi na međunarodnoj razini i pronašao zajednički i dopunski pravni i etički okvir za upotrebu umjetne inteligencije, posebno u području provedbe zakona i pravosuđa, kojim će se u potpunosti poštovati Povelja, europska pravna stečevina o zaštiti podataka i ljudska prava u širem smislu;

⁽⁸⁾ Odluka Vijeća 2008/615/PUP od 23. lipnja 2008. o produbljivanju prekogranične suradnje, posebno u suzbijanju terorizma i prekograničnog kriminala. (SL L 210, 6.8.2008., str. 1.).

srijeda, 6. listopada 2021.

35. poziva Agenciju EU-a za temeljna prava da u suradnji s Europskim odborom za zaštitu podataka i Europskim nadzornikom za zaštitu podataka izradi sveobuhvatne smjernice, preporuke i najbolje prakse kako bi se dodatno odredili kriteriji i uvjeti za razvoj, upotrebu i uvođenje aplikacija i rješenja umjetne inteligencije kojima se koriste tijela kaznenog progona i pravosudna tijela; obvezuje se provesti studiju o provedbi Direktive o izvršavanju zakonodavstva⁽⁹⁾ kako bi se utvrdilo na koji su način tijela kaznenog progona i pravosudna tijela osigurala zaštitu osobnih podataka prilikom njihove obrade, posebno u razvoju ili uvođenju novih tehnologija; nadalje, poziva Komisiju da razmotri je li potrebno provesti konkretno zakonodavno djelovanje za dodatno određivanje kriterija i uvjeta za razvoj, upotrebu i uvođenje aplikacija i rješenja umjetne inteligencije kojima se koriste tijela kaznenog progona i pravosudna tijela;

36. nalaže svojem predsjedniku da ovu Rezoluciju proslijedi Vijeću i Komisiji.

⁽⁹⁾ Direktiva (EU) 2016/680 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka od strane nadležnih tijela u svrhe sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Okvirne odluke Vijeća 2008/977/PUP. (SL L 119, 4.5.2016., str. 89.).