P9_TA(2021)0405

Mākslīgais intelekts krimināltiesībās un policijas un tiesu iestāžu īstenotā mākslīgā intelekta izmantošana krimināllietās

Eiropas Parlamenta 2021. gada 6. oktobra rezolūcija par mākslīgo intelektu krimināltiesībās un policijas un tiesu iestāžu īstenoto mākslīgā intelekta izmantošanu krimināllietās (2020/2016(INI))

(2022/C 132/02)

Eiropas Parlaments,

— ņemot vērā Līgumu par Eiropas Savienību, jo īpaši tā 2. un 6. pantu, un Līgumu par Eiropas Savienības darbību, jo īpaši tā 16. pantu,

— ņemot vērā Eiropas Savienības Pamattiesību hartu (Harta), jo īpaši tās 6., 7., 8., 11., 12., 13., 20., 21., 24. un 47. pantu;

— ņemot vērā Cilvēktiesību un pamatbrīvību aizsardzības konvenciju,

— ņemot vērā Eiropas Padomes Konvenciju par personu aizsardzību attiecībā uz personas datu automātisko apstrādi (ETS 108) un to grozošo protokolu (Konvencija 108+),

— ņemot vērā Eiropas Padomes Tiesu sistēmas efektivitātes komisijas (*CEPEJ*) Eiropas Ētikas hartu par mākslīgā intelekta izmantošanu tiesu sistēmās un to vidē,

— ņemot vērā Komisijas 2019. gada 8. aprīļa paziņojumu "Vairojot uzticēšanos antropocentriskam mākslīgajam intelektam" (COM(2019)0168),

— ņemot vērā Komisijas Mākslīgā intelekta augsta līmeņa ekspertu grupas 2019. gada 8. aprīlī publicētās ētikas vadlīnijas uzticamam MI,

— ņemot vērā Komisijas 2020. gada 19. februāra balto grāmatu par mākslīgo intelektu "Eiropiska pieeja — izcilība un uzticēšanās" (COM(2020)0065),

— ņemot vērā Komisijas 2020. gada 19. februāra paziņojumu "Eiropas Datu stratēģija" (COM(2020)0066),

— ņemot vērā Eiropas Parlamenta un Padomes Regulu (ES) 2016/679 (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (Vispārīgā datu aizsardzības regula) ([1]),

— ņemot vērā Eiropas Parlamenta un Padomes Direktīvu (ES) 2016/680 (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi, ko veic kompetentās iestādes, lai novērstu, izmeklētu, atklātu noziedzīgus nodarījumus vai sauktu pie atbildības par tiem vai izpildītu krimināLsodus, un par šādu datu brīvu apriti, ar ko atceļ Padomes Pamatlēmumu 2008/977/TI ([2]),

— ņemot vērā Eiropas Parlamenta un Padomes Regulu (ES) 2018/1725 (2018. gada 23. oktobris) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi Savienības iestādēs, struktūrās, birojos un aģentūrās un par šādu datu brīvu apriti un ar ko atceļ Regulu (EK) Nr. 45/2001 un Lēmumu Nr. 1247/2002/EK ([3]),

— ņemot vērā Eiropas Parlamenta un Padomes Direktīvu 2002/58/EK (2002. gada 12. jūlijs) par personas datu apstrādi un privātās dzīves aizsardzību elektronisko komunikāciju nozarē (direktīva par privāto dzīvi un elektronisko komunikāciju) ([4]),

([1]) OV L 119, 4.5.2016., 1. lpp.
([2]) OV L 119, 4.5.2016., 89. lpp.
([3]) OV L 295, 21.11.2018., 39. lpp.
([4]) OV L 201, 31.7.2002., 37. lpp.

— ņemot vērā Eiropas Parlamenta un Padomes Regulu (ES) 2016/794 (2016. gada 11. maijs) par Eiropas Savienības Aģentūru tiesībaizsardzības sadarbībai (Eiropolu) un ar kuru aizstāj un atceļ Padomes Lēmumus 2009/371/TI, 2009/934/TI, 2009/935/TI, 2009/936/TI un 2009/968/TI ([5]),

— ņemot vērā 2020. gada 19. jūnija rezolūciju par protestiem pret rasismu pēc Džordža Floida nāves ([6]),

— ņemot vērā 2017. gada 14. marta rezolūciju par lielo datu ietekmi uz pamattiesībām — privātums, datu aizsardzība, nediskriminācija, drošība un tiesībaizsardzība ([7]),

— ņemot vērā 2020. gada 20. februāra uzklausīšanu Pilsoņu brīvību, tieslietu un iekšlietu komitejā (LIBE) par mākslīgo intelektu krimināltiesībās un par to, kā to krimināllietās izmanto policija un tiesu iestādes,

— ņemot vērā ziņojumu par LIBE komitejas darba braucienu uz Amerikas Savienotajām Valstīm 2020. gada februārī,

— ņemot vērā Reglamenta 54. pantu,

— ņemot vērā Iekšējā tirgus un patērētāju aizsardzības komitejas un Juridiskās komitejas atzinumu,

— ņemot vērā Pilsoņu brīvību, tieslietu un iekšlietu komitejas ziņojumu (A9-0232/2021),

A. tā kā digitālajām tehnoloģijām kopumā un konkrēti datu apstrādes un analīzes uzplaukumam, ko dara iespējamu mākslīgais intelekts (MI), ir raksturīgs ārkārtīgs potenciāls un risks; tā kā MI attīstība pēdējos gados ir ievērojami progresējusi, MI kļūstot par vienu no 21. gadsimta stratēģiskajām tehnoloģijām ar potenciālu sniegt būtiskus ieguvumus efektivitātes, precizitātes un ērtības ziņā un tādējādi radīt pozitīvas pārmaiņas Eiropas ekonomikā un sabiedrībā, bet arī ar lieliem riskiem pamattiesībām un demokrātijai, kuras pamatā ir tiesiskums; tā kā MI būtu jāuztver nevis kā pašmērķis, bet gan kā instruments, kas kalpo cilvēkiem, ar galīgo mērķi palielināt cilvēku labbūtību, spējas un drošību;

B. tā kā par spīti pastāvīgajiem sasniegumiem datorapstrādes ātruma un atmiņas aspektā vēl nav tādu programmu, kam piemistu cilvēka spēja elastīgi darboties plašākā mērogā vai tikt galā ar uzdevumiem, kuru izpilde prasa konteksta izpratni vai kritisku analīzi; tā kā dažas MI lietotnes ir sasniegušas cilvēku ekspertu un speciālistu snieguma līmeni konkrētu specifisku uzdevumu veikšanā (piemēram, juridisko tehnoloģiju jomā) un var dot rezultātus daudz ātrāk un plašākā mērogā;

C. tā kā dažas valstis, tostarp vairākas dalībvalstis, vairāk nekā citas tiesībaizsardzībā un tiesu sistēmā izmanto MI lietotnes vai iegultās MI sistēmas un tas daļēji ir skaidrojams ar regulējuma trūkumu un regulējuma atšķirībām, kas ļauj vai aizliedz MI izmantošanu konkrētiem mērķiem; tā kā pieaugošā MI izmantošana krimināltiesību jomā ir balstīta jo īpaši uz solījumiem, ka tas samazinās noteiktu veidu noziedzību un ļaus pieņemt objektīvākus lēmumus; tā kā šie solījumi tomēr ne vienmēr piepildās;

D. tā kā Hartā nostiprinātās pamattiesības un pamatbrīvības būtu jāgarantē visā MI un saistīto tehnoloģiju dzīves ciklā, it īpaši to projektēšanas, izstrādes, ieviešanas un izmantošanas laikā, un tās būtu jāpiemēro tiesību aktu izpildes panākšanai jebkuros apstākļos;

E. tā kā MI tehnoloģija būtu jāizstrādā tā, lai tās centrā būtu cilvēki, tā būtu pelnījusi sabiedrības uzticēšanos un vienmēr kalpotu cilvēkiem; tā kā MI sistēmām vajadzētu būt ar garantiju, ka tās ir izstrādātas tā, lai tās vienmēr varētu izslēgt cilvēks;

F. tā kā MI sistēmas ir jāprojektē tā, ka tās nodrošina aizsardzību un sniedz labumu visiem sabiedrības locekļiem (cita starpā ņemot vērā neaizsargātus, marginalizētus iedzīvotājus), tām jābūt nediskriminējošām, drošām, to lēmumiem jābūt izskaidrojamiem un pārredzamiem, kā arī jāievēro cilvēka autonomija un pamattiesības, lai tās būtu uzticamas, kā aprakstīts Mākslīgā intelekta augsta līmeņa ekspertu grupas ētikas vadlīnijās;

([5]) OV L 135, 24.5.2016., 53. lpp.
([6]) OV C 362, 8.9.2021., 63. lpp.
([7]) OV C 263, 25.7.2018., 82. lpp.

G. tā kā Savienība kopā ar dalībvalstīm ir izšķirīgi atbildīga par to, lai nodrošinātu, ka lēmumi, kas attiecas uz MI lietotņu dzīves ciklu un izmantošanu tiesu un tiesībaizsardzības jomā, tiek pieņemti pārredzami, pilnībā sargā pamattiesības un it īpaši neturpina pastāvošo diskrimināciju, neobjektīvu attieksmi vai aizspriedumus; tā kā attiecīgajām rīcībpolitiskajām izvēlēm būtu jāatbilst nepieciešamības un proporcionalitātes principiem, lai garantētu konstitucionalitāti un taisnīgu un humānu tiesu sistēmu;

H. tā kā MI lietotnes var pavērt lielas iespējas tiesībaizsardzības jomā, jo īpaši — uzlabot tiesībaizsardzības un tiesu iestāžu darba metodes un efektīvāk apkarot konkrētu veidu noziegumus, it sevišķi finanšu noziegumus, nelikumīgi iegūtu līdzekļu legalizāciju un teroristu finansēšanu, seksuālu vardarbību pret bērniem un bērnu seksuālu izmantošanu tiešsaistē, kā arī konkrētus kibernoziedzības veidus, tādējādi uzlabojot ES iedzīvotāju drošību, bet reizē tās var arī būtiski apdraudēt cilvēku pamattiesības; tā kā jebkāda vispārēja MI izmantošana masveida novērošanai būtu nesamērīga;

I. tā kā MI sistēmu izstrāde un darbība policijas un tiesu iestāžu vajadzībām nozīmē daudzu personu, organizāciju, iekārtu komponentu, programmatūras algoritmu un lietotāju devumu bieži vien kompleksā un sarežģītā vidē; tā kā MI izmantošana tiesībaizsardzības un tiesu iestādēs ir dažādos attīstības posmos — no konceptualizācijas, prototipu izstrādes vai izvērtēšanas līdz izmantošanai pēc apstiprināšanas; tā kā, visā pasaulē notiekošo zinātnisko pētījumu rezultātā tehnoloģijām nobriestot, nākotnē var rasties jaunas izmantošanas iespējas;

J. tā kā obligāti vajadzīgs skaidrs modelis, kā noteikt juridisko atbildību par MI sistēmu iespējamo kaitīgo ietekmi krimināltiesību jomā; tā kā reglamentējošiem noteikumiem šajā jomā vienmēr būtu jāsaglabā cilvēku atbildība un pirmām kārtām jācenšas nepieļaut nekādu kaitīgu seku rašanos;

K. tā kā dalībvalstīm ir pienākums garantēt pilnīgu pamattiesību ievērošanu MI sistēmu izmantošanā tiesībaizsardzības un tiesu jomā;

L. tā kā saiknei starp pamattiesību aizsardzību un rezultatīvu policijas darbību vienmēr ir jābūt būtiskam elementam diskusijās par to, vai un kā MI būtu jāizmanto tiesībaizsardzības nozarē, kurā lēmumiem var būt ilgstoša ietekme uz personu dzīvi un brīvību; tā kā tas ir īpaši svarīgi, jo MI var kļūt par pastāvīgu mūsu krimināltiesību ekosistēmas daļu, kas nodrošina analīzi un palīdzību izmeklēšanā;

M. tā kā tiesībaizsardzības iestādēs MI tiek izmantots, piemēram, sejas atpazīšanas tehnoloģijās, kur to lieto, piem., lai meklētu aizdomās turēto personu datubāzēs un identificētu cilvēku tirdzniecības upurus vai bērnus, kuri cietuši no seksuālas izmantošanas un vardarbības, automātiskajā numura zīmes atpazīšanā, runātāja identifikācijā, runas identifikācijā, lūpu nolasīšanas tehnoloģijās, skaniskajā novērošanā (šāvienu detektēšanas algoritmi), identificēto datubāzu autonomā izpētē un analīzē, prognozēšanā (kriminoloģiskā prognozēšana un noziedzības karsto punktu analīze), uzvedības detektēšanas rīkos, mūsdienīgos virtuālās autopsijas rīkos, kuri palīdz noteikt nāves cēloni, autonomos finanšu krāpniecības un teroristu finansēšanas identifikācijas instrumentos, sociālo mediju uzraudzībā (rasmošana un datu ievākšana kontaktu izpētes nolūkos) un automatizētās novērošanas sistēmās, kurās iekļautas dažādas detektēšanas spējas (piemēram, sirdspukstu detektēšana un termokameras); tā kā līdzās citiem potenciāliem vai turpmākiem MI tehnoloģijas lietojumiem tiesībaizsardzības jomā iepriekš minētajiem lietojumiem var būt ļoti dažāda uzticamības un precizitātes pakāpe un ietekme uz pamattiesību aizsardzību un krimināltiesību sistēmu dinamiku; tā kā daudzus no šiem rīkiem izmanto trešās valstīs, bet saskaņā ar Savienības datu aizsardzības *acquis* un judikatūru tie būtu nelikumīgi; tā kā algoritmu rutīnveida izmantošana, pat ja pseidopozitīvu rezultātu īpatsvars ir neliels, var novest pie tā, ka kļūdainu brīdinājumu ir daudz vairāk nekā pareizu;

N. tā kā MI rīkus un lietotnes vairākās pasaules valstīs izmanto arī tiesu iestādes, piemēram, lai atbalstītu lēmumu pieņemšanu par pirmstiesas apcietinājumu, notiesāšanā, atkārtotu pārkāpumu varbūtības aprēķināšanā un probācijas noteikšanā, strīdu izšķiršanā tiešsaistē, judikatūras pārvaldībā un piekļuves tiesību aktiem atvieglošanā; tā kā tas ir vājinājis un mazinājis citas ādaskrāsas cilvēku un citu minoritāšu iespējas; tā kā pašlaik Eiropas Savienībā, izņemot dažas dalībvalstis, šos rīkus un lietotnes izmanto galvenokārt tikai civillietās;

O. tā kā MI izmantošana tiesībaizsardzības jomā nozīmē dažādus potenciāli lielus un dažos gadījumos nepieņemamus riskus cilvēku pamattiesību aizsardzībai, piemēram, nepārredzamu lēmumu pieņemšanu, dažādu diskrimināciju un kļūdas, kas raksturīgas pamatā esošajam algoritmam un ko var pastiprināt atgriezeniskās saites, kā arī riskus privātuma

un persondatu aizsardzībai, vārda un informācijas brīvības aizsardzībai, nevainīguma prezumpcijai, tiesībām uz efektīvu tiesību aizsardzību un taisnīgu tiesu, kā arī riskus cilvēku brīvībai un drošībai;

P. tā kā MI sistēmas, ko izmanto tiesībaizsardzības un tiesu iestādes, ir arī neaizsargātas pret MI balstītiem uzbrukumiem informācijas sistēmām vai datu saindēšanu, kas izpaužas kā nepareizas datu kopas iekļaušana nolūkā radīt neobjektīvus rezultātus; tā kā šajās situācijās radītais kaitējums potenciāli ir vēl būtiskāks un var izraisīt eksponenciāli lielāku kaitējumu gan atsevišķiem cilvēkiem, gan grupām,

Q. tā kā MI ieviešana tiesībaizsardzības un tiesu jomā būtu jāuzskata nevis tikai par tehnisku iespējamību, bet gan drīzāk par politisku lēmumu attiecībā uz tiesībaizsardzības un krimināltiesību sistēmu veidolu un mērķiem; tā kā mūsdienu krimināltiesību pamatā ir ideja, ka iestādes reaģē uz nodarījumu pēc tā izdarīšanas, nepieņemot, ka visi cilvēki ir bīstami un pastāvīgi jāuzrauga, lai nepieļautu iespējamus pārkāpumus; tā kā uz MI balstītas novērošanas metodes šai pieejai ir liels izaicinājums un liek likumdevējiem visā pasaulē steidzami rūpīgi novērtēt sekas, kas rodas, ja ir ļauts ieviest tehnoloģijas, kuras mazina cilvēka lomu tiesībaizsardzības un iztiesāšanas procesos,

1. atkārto, ka — tā kā MI pamatā ir liela persondatu apjoma apstrāde — tiesības uz privātās dzīves aizsardzību un tiesības uz personas datu aizsardzību attiecas uz visām MI jomām un ka ir pilnībā jāievēro Savienības tiesiskais regulējums datu aizsardzības un privātuma jomā; tādēļ atgādina, ka ES jau ir izstrādājusi datu aizsardzības standartus tiesībaizsardzības jomā, kas veido pamatu jebkādiem turpmākiem noteikumiem par MI izmantošanu tiesībaizsardzības un tiesu iestāžu vajadzībām; atgādina, ka persondatu apstrādei vajadzētu būt likumīgai un godprātīgai, apstrādes nolūkiem vajadzētu būt precizētiem, skaidri formulētiem un leģitīmiem, apstrādei vajadzētu būt adekvātai, relevantai un samērīgai ar nolūku, kādā tā notiek, tai vajadzētu būt precīzai un atjauninātai un neprecīzi dati, ja vien nav piemērojami ierobežojumi, būtu jālabo vai jādzēš, dati nebūtu jāglabā ilgāk, nekā nepieciešams, būtu jānosaka skaidri un piemēroti termiņi dzēšanai vai periodiskai šādu datu glabāšanas nepieciešamības pārskatīšanai un tie būtu jāapstrādā drošā veidā; uzsver arī, ka nedrīkstētu pieļaut iespēju, ka MI lietotne identificē personas, izmantojot iepriekš anonimizētus datus;

2. vēlreiz apstiprina, ka visos MI risinājumos tiesībaizsardzības un tiesu jomā ir arī pilnībā jāievēro tādi principi kā cilvēka cieņa, nediskriminēšana, pārvietošanās brīvība, nevainīguma prezumpcija un tiesības uz aizstāvību, tostarp tiesības klusēt, vārda un informācijas brīvība, pulcēšanās un biedrošanās brīvība, vienlīdzība likuma priekšā, pušu procesuālo tiesību vienlīdzība un tiesības uz efektīvu tiesību aizsardzību un taisnīgu tiesu saskaņā ar Hartu un Eiropas Cilvēktiesību konvenciju; uzsver, ka tad, ja MI lietotņu izmantošana nav saderīga ar pamattiesībām, tā ir jāaizliedz;

3. atzīst, ka ātrums, kādā visā pasaulē tiek izstrādātas MI lietotnes, neļauj lietotnes izsmeļoši uzskaitīt un tādēļ ir vajadzīgs skaidrs un saskanīgs pārvaldības modelis, kas garantē gan indivīdu pamattiesības, gan tiesisko skaidrību izstrādātājiem, ņemot vērā tehnoloģiju nepārtraukto attīstību; tomēr, ņemot vērā policijas un tiesu iestāžu lomu un atbildību, kā arī to lēmumu ietekmi, kurus tās pieņem, lai nepieļautu, izmeklētu, atklātu noziedzīgus nodarījumus vai sauktu pie atbildības par tiem, vai izpildītu kriminālsodus, uzskata, ka gadījumos, kad pastāv iespēja būtiski ietekmēt cilvēka dzīvi, MI lietotņu izmantošana ir jāklasificē kā liela riska darbība;

4. šajā sakarā uzskata, ka jebkuram MI rīkam, ko izstrādā vai izmanto tiesībaizsardzības vai tiesu iestādes, vajadzētu būt vismaz drošam, noturīgam, aizsargātam un piemērotam paredzētajam mērķim un atbilst taisnīguma, datu minimizēšanas, pārskatatbildības, pārredzamības, nediskriminēšanas un izskaidrojamības principiem un ka to izstrādei, ieviešanai un izmantošanai būtu jāpiemēro riska novērtējums un stingra nepieciešamības un proporcionalitātes pārbaude, kur aizsardzības pasākumiem jābūt samērīgiem ar identificētajiem riskiem; uzsver, ka iedzīvotāju uzticēšanās Eiropas Savienībā izstrādāta, ieviesta un lietota MI izmantošanai ir atkarīga no pilnīgas šo kritēriju izpildes;

5. atzīst dažu veidu MI lietotņu pozitīvo devumu tiesībaizsardzības un tiesu iestāžu darbā Savienībā; kā piemēru uzsver uzlabotu judikatūras pārvaldību, kas panākta ar rīkiem, kuri piedāvā papildu meklēšanas iespējas; uzskata, ka ir virkne citu potenciālu MI lietojumu tiesībaizsardzības un tiesu iestāžu vajadzībām, kurus varētu izpētīt, vienlaikus ņemot vērā piecus

principus, kas ietverti *CEPEJ* pieņemtajā Ētikas hartā par mākslīgā intelekta izmantošanu tiesu sistēmās un to vidē, un īpašu uzmanību pievēršot *CEPEJ* apzinātajiem "lietojumiem, pret kuriem jāattiecas maksimāli atturīgi";

6. uzsver, ka jebkuru tehnoloģiju var izmantot neparedzētam nolūkam, un tādēļ aicina īstenot stingru demokrātisko kontroli un neatkarīgu uzraudzību pār jebkuru MI balstītu tehnoloģiju, ko izmanto tiesībaizsardzības un tiesu iestādes, it īpaši tām tehnoloģijām, kuras var izmantot masveida novērošanai vai masveida profilēšanai; tādēļ ar lielām bažām norāda, ka konkrētas MI tehnoloģijas, ko izmanto tiesībaizsardzības nozarē, ir iespējams izmantot masveida novērošanas nolūkos; uzsver juridisko prasību nepieļaut masveida novērošanu ar MI tehnoloģijām, kura pēc definīcijas neatbilst nepieciešamības un proporcionalitātes principiem, un aizliegt tādu lietotņu izmantošanu, ar kurām tā varētu notikt;

7. uzsver, ka dažās trešās valstīs izmantotā pieeja attiecībā uz masveida novērošanas tehnoloģiju izstrādi, ieviešanu un izmantošanu nesamērīgi ietekmē pamattiesības un tāpēc ES nedrīkst tādu īstenot; tādēļ uzsver, ka Savienībā ir vienādi jāreglamentē arī aizsardzības pasākumi pret MI tehnoloģiju nepareizu izmantošanu, ko veic tiesībaizsardzības un tiesu iestādes;

8. uzsver neobjektivitātes un diskriminācijas potenciālu, ko rada tādu MI lietotņu izmantošana kā mašīnmācīšanās, ieskaitot algoritmus, kuri ir pamatā šādām lietotnēm; atzīmē, ka neobjektivitāte var būt raksturīga pamatā esošajām datu kopām (sevišķi tad, ja tiek izmantoti vēsturiski dati), algoritmu izstrādātāju ieviesta vai radīta tad, kad sistēmas tiek izmantotas reālās pasaules apstākļos; norāda, ka MI lietotņu sniegtos rezultātus neizbēgami ietekmē izmantoto datu kvalitāte un ka šāda raksturīga neobjektivitāte tiecas pakāpeniski palielināties un tādējādi turpināt un pastiprināt pastāvošo diskrimināciju, jo īpaši attiecībā uz personām, kas pieder pie noteiktām etniskām grupām vai rasu diskriminācijai pakļautām kopienām;

9. uzsver, ka daudzas pašlaik izmantotās algoritmiskās identifikācijas tehnoloģijas nesamērīgi nepareizi identificē un klasificē un tādējādi kaitē rasu diskriminācijai pakļautiem cilvēkiem, pie konkrētām etniskām kopienām piederīgām personām, LGBTI, bērniem un veciem cilvēkiem, kā arī sievietēm; atgādina, ka indivīdiem ir ne tikai tiesības tikt pareizi identificētiem, bet arī tiesības netikt identificētiem vispār, ja vien tas nav prasīts tiesību aktos prioritārās un leģitīmās sabiedrības interesēs; uzsver, ka MI prognozes, kuru pamatā ir konkrētas personu grupas iezīmes, pastiprina un turpina pastāvošās diskriminācijas formas; uzskata, ka būtu jāpieliek lielas pūles, lai nepieļautu automatizētu diskrimināciju un neobjektivitāti; aicina ieviest stingrus papildu aizsardzības pasākumus gadījumiem, kad MI sistēmas tiesībaizsardzībā vai tiesu iestādēs tiek izmantotas attiecībā uz nepilngadīgajiem vai saistībā ar tiem;

10. uzsver varas asimetriju starp tiem, kas izmanto MI tehnoloģijas, un tiem, kas ir šo tehnoloģiju objekti; uzsver, ka ir ļoti svarīgi, lai MI rīku izmantošana tiesībaizsardzības un tiesu iestādēs nekļūtu par nelīdztiesības, sociālās plaisas vai atstumtības faktoru; uzsver MI rīku izmantošanas ietekmi uz aizdomās turēto personu tiesībām uz aizstāvību, grūtības iegūt jēgpilnu informāciju par to darbību un no tā izrietošās grūtības apstrīdēt to rezultātus tiesā, it īpaši cilvēkiem, kuri pakļauti izmeklēšanai;

11. pieņem zināšanai riskus, kuri it īpaši saistīti ar datu noplūdēm, datu drošības pārkāpumiem un neatļautu piekļuvi persondatiem un citai informācijai, kas saistīta, piemēram, ar kriminālizmeklēšanu vai tiesas lietām un ko apstrādā MI sistēmas; uzsver, ka tiesībaizsardzībā un tiesu iestādēs izmantoto MI sistēmu drošības un drošuma aspekti ir rūpīgi jāapdomā un tiem jābūt pietiekami stabiliem un noturīgiem, lai novērstu ļaunprātīgu uzbrukumu MI sistēmām iespējamās katastrofālās sekas; uzsver, cik svarīga ir integrētā drošība, kā arī īpaša cilvēka virsvadība pirms konkrētu kritiski svarīgu lietotņu izmantošanas, un tādēļ aicina tiesībaizsardzības un tiesu iestādes izmantot tikai tādas MI lietotnes, kas atbilst privātuma un integrētās datu aizsardzības principam, lai izvairītos no funkciju nesamērīga pieauguma;

12. uzsver, ka nevienai MI sistēmai, ko izmanto tiesībaizsardzības vai tiesu iestādes, nevajadzētu būt iespējai nedz kaitēt cilvēku fiziskajai integritātei, nedz sadalīt tiesības vai uzlikt juridiskas saistības indivīdiem;

13. atzīst, ka, ņemot vērā MI sistēmu izstrādes un darbības sarežģītību, ir grūti pareizi noteikt juridisko atbildību par iespējamo kaitējumu; uzskata, ka ir jāizveido skaidrs un taisnīgs režīms juridiskās atbildības noteikšanai par šo augsto digitālo tehnoloģiju iespējamajām negatīvajām sekām; tomēr uzsver, ka pirmām kārtām ir jācenšas šādas sekas vispār

nepieļaut; tādēļ aicina visās MI lietotnēs tiesībaizsardzības kontekstā piemērot piesardzības principu; uzsver, ka juridiskajai atbildībai vienmēr jāgulstas uz fizisku vai juridisku personu, kurai vienmēr jābūt identificētai attiecībā uz lēmumiem, kas pieņemti ar MI palīdzību; tādēļ uzsver, ka ir jānodrošina to korporatīvo struktūru pārredzamība, kuras ražo un pārvalda MI sistēmas;

14. uzskata, ka gan aizstāvības tiesību īstenošanas efektivitātes, gan valstu krimināltiesību sistēmu pārredzamības aspektā ir nepieciešams īpašs, skaidrs un precīzs tiesiskais regulējums, kas paredz MI rīku izmantošanas nosacījumus, kārtību un sekas tiesībaizsardzības un tiesu iestāžu jomā, kā arī skarto personu tiesības un efektīvas un viegli pieejamas sūdzību un pārsūdzību procedūras, tostarp tiesiskās aizsardzības līdzekļus; uzsver kriminālprocesa pušu tiesības piekļūt datu vākšanas procesam un saistītajiem novērtējumiem, ko veic vai kas iegūti, izmantojot MI lietotnes; uzsver, ka tiesu iestāžu sadarbībā iesaistītajām izpildiestādēm, lemjot par izdošanas (vai nodošanas) pieprasījumu citai dalībvalstij vai trešai valstij, ir jānovērtē, vai MI rīku izmantošana pieprasījuma iesniedzējā valstī varētu klaji apdraudēt pamattiesības uz taisnīgu tiesu; aicina Komisiju publicēt vadlīnijas par to, kā veikt šādu novērtējumu tiesu iestāžu sadarbības krimināllietās kontekstā; uzstāj, ka dalībvalstīm saskaņā ar piemērojamajiem tiesību aktiem būtu jānodrošina, ka indivīdi tiek informēti par to, ka attiecībā uz viņiem tiesībaizsardzības vai tiesu iestādes izmanto MI lietotnes;

15. norāda, ka tad, ja cilvēki paļausies tikai uz mašīnu ģenerētiem datiem, profiliem un ieteikumiem, viņi nevarēs veikt neatkarīgu novērtējumu; uzsver potenciāli smagās negatīvās sekas, īpaši tiesībaizsardzības un tiesu jomā, kas rastos, ja cilvēki pārmērīgi uzticētos MI rīku šķietami objektīvajam un zinātniskajam raksturam un neņemtu vērā iespēju, ka to rezultāti varētu būt nepareizi, nepilnīgi, nerelevanti vai diskriminējoši; uzsver, ka būtu jāizvairās no pārmērīgas paļaušanās uz MI sistēmu rezultātiem, un uzsver, ka iestādēm ir jāstiprina pārliecība un zināšanas, kas ļauj apšaubīt vai ignorēt algoritmisku ieteikumu; uzskata, ka ir svarīgi, lai ekspektācijas par šādiem tehnoloģiskiem risinājumiem būtu reālistiskas, un nesolīt ideālus tiesībaizsardzības risinājumus un visu izdarīto pārkāpumu atklāšanu;

16. uzsver, ka tiesu un tiesībaizsardzības kontekstā lēmums, kam ir juridiskas vai līdzīgas sekas, vienmēr ir jāpieņem cilvēkam, kuru var saukt pie atbildības par pieņemtajiem lēmumiem; uzskata, ka tiem, kuriem piemēro MI sistēmas, ir jādod iespēja izmantot tiesiskās aizsardzības līdzekļus; atgādina, ka saskaņā ar ES tiesību aktiem personai ir tiesības netikt pakļautai lēmumam, kurš viņai rada juridiskas sekas vai viņu būtiski ietekmē un kura pamatā ir tikai automatizēta datu apstrāde; turklāt uzsver, ka automatizēta individuālu lēmumu pieņemšana nedrīkst būt balstīta uz īpašām persondatu kategorijām, izņemot, ja tiek nodrošināti atbilstīgi pasākumi, ar ko aizsargā datu subjekta tiesības un brīvības, un leģitīmās intereses; uzsver, ka ES tiesību akti aizliedz profilēšanu, kas izraisa fizisku personu diskrimināciju, balstoties uz īpašām persondatu kategorijām; uzsver, ka, ņemot vērā tiesībaizsardzības iestāžu un to darbību izpildu raksturu, lēmumi tiesībaizsardzības jomā gandrīz vienmēr ir lēmumi, kam ir juridiskas sekas attiecīgajai personai; atzīmē, ka MI izmantošana var ietekmēt cilvēku lēmumus un visus kriminālprocesa posmus; tādēļ uzskata, ka iestādēm, kas izmanto MI sistēmas, ir jāievēro ārkārtīgi augsti juridiskie standarti un jānodrošina cilvēka iejaukšanās, īpaši tad, kad tiek analizēti no šādām sistēmām iegūti dati; tādēļ prasa ievērot tiesnešu suverēno rīcības brīvību un lēmumu pieņemšanu katrā gadījumā atsevišķi; aicina aizliegt MI un saistīto tehnoloģiju izmantošanu tiesas nolēmumu ierosināšanai;

17. aicina nodrošināt algoritmu izskaidrojamību, pārredzamību, izsekojamību un verifikāciju, lai panāktu, ka tiesu un tiesībaizsardzības iestādēm paredzēto MI sistēmu izstrāde, ieviešana un izmantošana atbilst pamattiesībām un ka iedzīvotāji tām uzticas, kā arī lai nodrošinātu, ka MI algoritmu radītos rezultātus ir iespējams padarīt saprotamus lietotājiem un tiem, kas ir pakļauti šīm sistēmām, un nodrošinātu pārredzamību attiecībā uz pirmdatiem un to, kā sistēma nonāk pie konkrēta secinājuma; norāda, ka, lai nodrošinātu tehnisko pārredzamību, noturību un precizitāti, tiesībaizsardzības un tiesu iestādēm Savienībā būtu jāļauj iegādāties tikai tādus rīkus un sistēmas, kuru algoritmi un loģika ir pārbaudāma un pieejama vismaz policijai un tiesu iestādēm, kā arī neatkarīgajiem revidentiem, lai tos varētu novērtēt, revidēt un pārbaudīt, un pārdevēji nedrīkst tos slēgt vai marķēt kā īpašumtiesību objektus; turklāt norāda, ka būtu jāsniedz skaidrā, saprotamā valodā sagatavota dokumentācija par pakalpojuma būtību, izstrādātajiem rīkiem, veiktspēju un apstākļiem, kādos tos paredzēts izmantot, un riskiem, ko tie varētu radīt; tādēļ aicina tiesu un tiesībaizsardzības iestādes nodrošināt proaktīvu un pilnīgu

pārredzamību attiecībā uz privātiem uzņēmumiem, kas tiem nodrošina MI sistēmas tiesībaizsardzības un tiesu iestāžu vajadzībām; tādēļ iesaka pēc iespējas izmantot atvērtā pirmkoda programmatūru;

18. mudina tiesībaizsardzības un tiesu iestādes apzināt un novērtēt jomas, kurās daži īpaši pielāgoti MI risinājumi varētu būt noderīgi, un apmainīties ar MI ieviešanas paraugpraksēm; aicina dalībvalstis un ES aģentūras pieņemt attiecīgus publiskā iepirkuma procesus MI sistēmām, kuras izmanto tiesībaizsardzības vai tiesu iestāžu kontekstā, tā, lai nodrošinātu to atbilstību pamattiesībām un piemērojamajiem tiesību aktiem, cita starpā nodrošinot, ka programmatūras dokumentācija un algoritmi ir pieejami un piekļūstami izskatīšanai kompetentajām un uzraudzības iestādēm; īpaši prasa pieņemt saistošus noteikumus, kas prasa publiski atklāt publiskā un privātā sektora partnerības, līgumus un iegādes, kā arī iegādes mērķus; uzsver nepieciešamību nodrošināt iestādēm nepieciešamo finansējumu, kā arī nepieciešamās zināšanas, lai garantētu pilnīgu atbilstību ētikas, juridiskajām un tehniskajām prasībām, kas saistītas ar MI ieviešanu;

19. aicina nodrošināt MI sistēmu un lēmumu pieņemšanas procesa izsekojamību, kas izklāsta to funkcijas, nosaka sistēmu spējas un ierobežojumus un ļauj sekot līdzi lēmuma pamatelementu izcelsmei, izmantojot obligātu dokumentāciju; uzsver, ka ir svarīgi saglabāt pilnīgu apmācības datu dokumentāciju, to kontekstu, mērķi, precizitāti un blakusparādības, kā arī to apstrādi, ko veic algoritmu veidotāji un izstrādātāji, un to atbilstību pamattiesībām; uzsver, ka vienmēr ir jābūt iespējai MI sistēmas aprēķinus reducēt līdz formai, kas ir saprotama cilvēkiem;

20. aicina ieviest obligātu pamattiesību ietekmējuma novērtējumu, kas jāveic pirms ikvienas tiesībaizsardzības vai tiesu iestāžu MI sistēmas ierīkošanas vai ieviešanas, lai novērtētu visus potenciālos riskus pamattiesībām; atgādina, ka iepriekšējs novērtējums par ietekmi uz datu aizsardzību ir obligāts jebkāda veida apstrādei, īpaši tad, ja tiek izmantotas jaunas tehnoloģijas, kas, ļoti iespējams, rada lielu risku fizisku personu tiesībām un brīvībām, un uzskata, ka tas attiecas uz lielāko daļu MI tehnoloģiju tiesībaizsardzības un tiesu jomā; uzsver datu aizsardzības iestāžu un pamattiesību aģentūru īpašās zināšanas šo sistēmu novērtēšanā; uzsver, ka šie pamattiesību ietekmējuma novērtējumi būtu jāveic pēc iespējas atklāti un aktīvi iesaistot pilsonisko sabiedrību; prasa, lai ietekmes novērtējumos būtu arī skaidri definēti aizsardzības pasākumi, kas vajadzīgi, lai novērstu konstatētos riskus, un lai tie, cik vien iespējams, būtu publiski pieejami pirms jebkuras MI sistēmas ieviešanas;

21. uzsver, ka tikai stabila Eiropas MI pārvaldība, kas ietver neatkarīgu izvērtēšanu, var nodrošināt nepieciešamo pamattiesību principu ieviešanu praksē; prasa, lai visas MI sistēmas, kuras izmanto tiesībaizsardzības un tiesu iestādes un kuras var būtiski ietekmēt indivīdu dzīvi, periodiski obligāti revidē neatkarīga iestāde, lai pārbaudītu un izvērtētu algoritmiskās sistēmas, to kontekstu, mērķi, precizitāti, veiktspēju un mērogu un, tiklīdz tās sāk darboties, lai atklātu, izmeklētu, diagnosticētu un labotu jebkādu nevēlamu un nelabvēlīgu ietekmi un nodrošinātu, ka MI sistēmas darbojas, kā paredzēts; tādēļ aicina šajā nolūkā izveidot skaidru institucionālo satvaru, tostarp pienācīgu regulatīvo un uzraudzības kontroli, lai nodrošinātu pilnīgu īstenošanu un garantētu pilnībā informētas demokrātiskas debates par MI nepieciešamību un proporcionalitāti krimināltiesību jomā; uzsver, ka šo revīziju rezultāti būtu jādara pieejami publiskajos reģistros, lai iedzīvotāji zinātu, kādas MI sistēmas tiek ieviestas un kādi pasākumi tiek veikti, lai novērstu pamattiesību pārkāpumus;

22. uzsver, ka datu kopas un algoritmiskās sistēmas, ko izmanto, veicot klasificēšanu, novērtējumus un prognozes dažādos datu apstrādes posmos MI un saistīto tehnoloģiju izstrādē, var arī izraisīt atšķirīgu attieksmi un gan tiešu, gan netiešu diskrimināciju pret cilvēku grupām, īpaši tāpēc, ka dati, ko izmanto, lai apmācītu kriminoloģiskās prognozēšanas algoritmus, atspoguļo pastāvīgās novērošanas prioritātes un tādējādi var novest pie pašreizējo neobjektivitātes formu turpināšanas un pastiprināšanas; tādēļ uzsver, ka MI tehnoloģijām, īpaši tām, ko izmanto tiesībaizsardzības un tiesu iestāžu vajadzībām, ir vajadzīgi starpdisciplīnu pētījumi un ieguldījums, tostarp zinātnes un tehnoloģiju studijās, kritiskajās rases studijas, invaliditātes studijās un citās disciplīnās, kas pielāgoti sociālajam kontekstam, cita starpā par to, kā tiek veidota atšķirība, noris klasifikācijas darbs un kādas ir tā sekas; tādēļ uzsver nepieciešamību sistemātiski investēt šo disciplīnu integrēšanā MI studijās un pētniecībā visos līmeņos; uzsver arī to, ka ir svarīgi, lai komandas, kas projektē, izstrādā, testē, uztur, ievieš un iepērk šīs MI sistēmas tiesībaizsardzības un tiesu iestāžu vajadzībām, pēc iespējas atspoguļotu sabiedrības vispārējo daudzveidību — tas netehniski samazina diskriminācijas risku;

23. turklāt uzsver, ka pienācīga pārskatatbildība, pienākumi un atbildība prasa ievērojamu specializētu apmācību par ētikas normām, iespējamiem draudiem, ierobežojumiem un pareizu MI tehnoloģijas izmantošanu, īpaši policijas un tiesu iestāžu darbiniekiem; uzsver, ka ar pienācīgu apmācību un kvalifikāciju būtu jāpanāk, ka lēmumu pieņēmēji ir apmācīti par iespējamo neobjektivitāti, jo datu kopas var būt balstītas uz diskriminējošiem un aizspriedumainiem datiem; atbalsta izpratnes veicināšanas un izglītojošu iniciatīvu izveidi nolūkā nodrošināt, ka cilvēki, kas strādā tiesībaizsardzības un tiesu iestādēs, apzinās un saprot MI sistēmu izmantošanas ierobežojumus, iespējas un riskus, tostarp automatizācijas neobjektivitātes risku; atgādina, ka tas, ka MI apmācības datu kopās iekļauj gadījumus, kad policijas spēki, pildot savus pienākumus, rīkojušies rasistiski, neizbēgami novedīs pie rasistiskas neobjektivitātes MI ģenerētajos konstatējumos, rezultātos un ieteikumos; tādēļ vēlreiz aicina dalībvalstis veicināt diskriminācijas novēršanas rīcībpolitiku un izstrādāt valsts rīcības plānus cīņai pret rasismu policijas un tiesu sistēmas jomā;

24. atzīmē, ka kriminoloģiskā prognozēšana ir viens no MI lietojumiem tiesībaizsardzības jomā, taču brīdina, ka, lai gan kriminoloģiskajā prognozēšanā var analizēt datu kopas modeļu un korelāciju identificēšanai, tā nevar atbildēt uz cēloņsakarības jautājumu un nevar sniegt uzticamas prognozes par individuālo uzvedību, tāpēc tā nevar būt vienīgais intervences pamats; norāda, ka vairākas ASV pilsētas pēc revīzijām ir beigušas izmantot kriminoloģiskās prognozēšanas sistēmas; atgādina, ka LIBE komitejas darba brauciena laikā uz ASV 2020. gada februārī Ņujorkas un Kembridžas (Masačūsetsā) policijas departamenti informēja deputātus, ka rezultativitātes trūkuma, diskriminējošas ietekmes un praktiskā nederīguma dēļ viņi ir pakāpeniski izbeiguši savas kriminoloģiskās prognozēšanas programmas un tā vietā ir pievērsušies uz sabiedrību vērstam policijas darbam; atzīmē, ka tas ir novedis pie noziedzības līmeņa samazināšanās; tādēļ ir pret to, ka tiesībaizsardzības iestādes izmanto MI, lai prognozētu indivīdu vai grupu uzvedību, balstoties uz vēsturiskiem datiem un iepriekšēju uzvedību, piederību pie grupas, atrašanās vietu vai jebkādām citām šādām pazīmēm, tādējādi mēģinot identificēt cilvēkus, kuri, ļoti iespējams, varētu izdarīt noziegumu;

25. atzīmē, ka sejas atpazīšanu izmanto dažādi, cita starpā verifikācijai/autentifikācijai (t. i., sejas sastatīšanai ar fotogrāfiju ID dokumentā klātienē, piemēram, uz viedrobežas), identifikācijai (t. i., fotogrāfijas sastatīšanai ar fotogrāfijām datubāzē) un atklāšanai (t. i., seju detektēšanai reāllaikā no tādiem avotiem kā videonovērošanas sistēmas un to sastatīšanai ar datubāzēm, piemēram, novērošanai reāllaikā), un katram izmantošanas veidam ir citāda ietekme uz pamattiesību aizsardzību; ir stingri pārliecināts, ka sejas atpazīšanas sistēmu ieviešana, ko veic tiesībaizsardzības iestādes, būtu jāierobežo, to ļaujot izmantot tikai skaidri pamatotiem mērķiem, pilnībā ievērojot proporcionalitātes un nepieciešamības principus un piemērojamos tiesību aktus; vēlreiz apstiprina, ka sejas atpazīšanas tehnoloģijas izmantošanai ir jāatbilst vismaz datu minimizēšanas, datu precizitātes, glabāšanas ierobežošanas, datu drošības un pārskatatbildības prasībām, kā arī jābūt likumīgai, taisnīgai, pārredzamai un ar konkrētu, skaidru un leģitīmu mērķi, kas ir skaidri noteikts dalībvalsts vai Savienības tiesību aktos; uzskata, ka verifikācijas un autentifikācijas sistēmas var turpināt ieviest un sekmīgi izmantot tikai tad, ja to negatīvo ietekmi var mazināt un var izpildīt minētos kritērijus;

26. turklāt aicina uz visiem laikiem aizliegt izmantot citu cilvēka īpašību, piemēram, gaitas, pirkstu nospiedumu, DNS, balss un citu biometrisko un uzvedības signālu, automatizētu analīzi un/vai atpazīšanu publiski pieejamās vietās;

27. tomēr aicina noteikt moratoriju tādu sejas atpazīšanas sistēmu ieviešanai tiesībaizsardzības nolūkos, kurām ir identifikācijas funkcija, ja vien tās netiek izmantotas strikti tikai noziedzīgos nodarījumos cietušo identificēšanai, kamēr tehniskos standartus nevar uzskatīt par pilnībā atbilstīgiem pamattiesībām, iegūtie rezultāti nav objektīvi un nediskriminējoši, tiesiskais regulējums nenodrošina stingrus aizsardzības pasākumus pret nepareizu izmantošanu un stingru demokrātisko kontroli un uzraudzību un nav empīrisku pierādījumu par šādu tehnoloģiju ieviešanas nepieciešamību un proporcionalitāti; atzīmē, ka tad, ja minētie kritēriji nav izpildīti, sistēmas nevajadzētu izmantot vai ieviest;

28. pauž nopietnas bažas par to, ka tiesībaizsardzības aktori un izlūkdienesti izmanto privātas sejas atpazīšanas datubāzes, piemēram, *Clearview AI* — datubāzi, kurā ir vairāk nekā trīs miljardi attēlu, kas nelikumīgi savākti no sociālajiem tīkliem un citām interneta daļām, tostarp ES iedzīvotāju attēli; aicina dalībvalstis noteikt tiesībaizsardzības aktoriem pienākumu atklāt informāciju, vai tie izmanto *Clearview AI* tehnoloģiju vai līdzvērtīgas citu pakalpojumu sniedzēju tehnoloģijas; atgādina par Eiropas Datu aizsardzības kolēģijas (EDAK) atzinumu, ka tādu pakalpojumu kā *Clearview AI* izmantošana, ko veic tiesībaizsardzības iestādes Eiropas Savienībā, "ļoti iespējams, neatbilst ES datu aizsardzības režīmam"; aicina aizliegt privātu sejas atpazīšanas datubāzu izmantošanu tiesībaizsardzības iestādēs;

29. ņem vērā Komisijas priekšizpēti par iespējamām izmaiņām Prīmes lēmumā ([8]), arī attiecībā uz sejas attēliem; pieņem zināšanai iepriekšējos pētījumus, kas rāda, ka nekādi potenciāli jauni identifikatori, piemēram, varavīksnenes vai sejas atpazīšana, tiesu ekspertīzes kontekstā nebūs tikpat uzticami kā DNS vai pirkstu nospiedumi; atgādina Komisijai, ka jebkuram tiesību akta priekšlikumam jābūt balstītam pierādījumos un jāatbilst proporcionalitātes principam; mudina Komisiju nepagarināt Prīmes lēmuma sistēmu, ja vien nav pārliecinošu zinātnisku pierādījumu par sejas atpazīšanas uzticamību tiesu ekspertīzes kontekstā salīdzinājumā ar DNS vai pirkstu nospiedumiem, pēc tam, kad tā būs veikusi pilnīgu ietekmes novērtējumu, un ņemot vērā Eiropas Datu aizsardzības uzraudzītāja (EDAU) un EDAK ieteikumus;

30. uzsver, ka biometrisko datu izmantošana plašākā skatījumā ir saistīta ar cilvēka cieņas principu, kas ir visu Hartas garantēto pamattiesību pamatā; uzskata, ka jebkādu biometrisko datu izmantošana un vākšana attālinātas identifikācijas nolūkos, piemēram, veicot sejas atpazīšanu sabiedriskās vietās, kā arī automātiskos robežkontroles vārtos, ko izmanto robežpārbaudēm lidostās, var radīt īpašus riskus pamattiesībām, kuru sekas var ievērojami atšķirties atkarībā no izmantošanas mērķa, konteksta un tvēruma; turklāt uzsver, ka afektīva stāvokļa atpazīšanas tehnoloģiju, piemēram, kameras, kas detektē acu kustības un zīlītes lieluma izmaiņas, zinātniskais derīgums tiesībaizsardzības kontekstā ir apšaubīts; uzskata, ka biometriskās identifikācijas izmantošana tiesībaizsardzības un tiesu kontekstā vienmēr būtu jāuzskata par lielu risku un tādēļ tai būtu jāpiemēro papildu prasības, kā ieteikusi Komisijas Mākslīgā intelekta augsta līmeņa ekspertu grupa;

31. ir ļoti nobažījies par pamatprogrammā "Apvārsnis 2020" finansētiem pētniecības projektiem, kas ievieš mākslīgo intelektu uz ārējām robežām, piemēram, projektu *iBorderCtrl*, "viedas melu detektēšanas sistēmu", kas profilē ceļotājus, balstoties uz datorautomatizētu interviju, kura ar ceļotāju veikta pa tīmekļa kameru pirms ceļojuma, un mākslīgajā intelektā balstītu 38 mikrožestu analīzi, kas testēta Ungārijā, Latvijā un Grieķijā; tādēļ aicina Komisiju, izmantojot leģislatīvus un neleģislatīvus līdzekļus un vajadzības gadījumā pārkāpumu procedūras, aizliegt jebkādu biometrisko datu, tostarp sejas attēlu, apstrādi tiesībaizsardzības nolūkos, kura noved pie masveida novērošanas publiski pieejamās vietās; turklāt aicina Komisiju vairs nefinansēt biometriskos pētījumus vai biometrisko sistēmu ieviešanu vai programmas, kas, ļoti iespējams, var izraisīt neselektīvu masveida novērošanu sabiedriskās vietās; šajā kontekstā uzsver, ka īpaša uzmanība būtu jāpievērš dronu izmantošanai policijas operācijās un tai būtu jāpiemēro stingrs regulējums;

32. atbalsta Komisijas Mākslīgā intelekta augsta līmeņa ekspertu grupas ieteikumus, kuros aicināts aizliegt cilvēku masveida vērtēšanu ar MI palīdzību; uzskata, ka jebkāda veida normatīva, iedzīvotāju vērtēšana plašā mērogā, ko veic valsts iestādes, īpaši tiesībaizsardzības un tiesu jomā, noved pie autonomijas zaudēšanas, apdraud nediskriminēšanas principu un to nevar uzskatīt par atbilstošu pamattiesībām, it sevišķi cilvēka cieņai, kas kodificētas ES tiesību aktos;

33. aicina panākt lielāku vispārējo pārredzamību, lai izveidotos vispusīga izpratne par MI lietotņu izmantošanu Savienībā; prasa, lai dalībvalstis sniedz visaptverošu informāciju par to tiesībaizsardzības un tiesu iestāžu izmantotajiem rīkiem, izmantoto rīku veidiem, mērķiem, kādiem tie tiek izmantoti, noziegumu veidiem, kuriem tie tiek piemēroti, un to uzņēmumu vai organizāciju nosaukumiem, kuri ir izstrādājuši šos rīkus; aicina tiesībaizsardzības un tiesu iestādes arī informēt sabiedrību un nodrošināt pietiekamu pārredzamību attiecībā uz to, kā tās, īstenojot savas pilnvaras, izmanto MI un saistītās tehnoloģijas, un cita starpā publiskot attiecīgās tehnoloģijas pseidopozitīvo un pseidonegatīvo rezultātu līmeņus; prasa, lai Komisija apkopo un atjaunina informāciju vienā vietā; aicina Komisiju arī publicēt un atjaunināt informāciju par to, kā MI izmanto Savienības aģentūras, kurām uzticēti tiesībaizsardzības un tiesu iestāžu uzdevumi; aicina EDAK novērtēt tiesībaizsardzības un tiesu iestāžu izmantoto MI tehnoloģiju un lietotņu likumību;

34. atgādina, ka MI lietotnes, tostarp tās, ko izmanto tiesībaizsardzības un tiesu kontekstā, pasaulē tiek izstrādātas strauji; mudina visas Eiropas ieinteresētās personas, tostarp dalībvalstis un Komisiju, starptautiskās sadarbības ceļā nodrošināt ārpussavienības partneru iesaisti, lai starptautiskā līmenī paaugstinātu standartus un izveidotu kopīgu un komplementāru tiesisko un ētisko MI izmantošanas satvaru — īpaši tiesībaizsardzības un tiesu iestādēm —, kas pilnībā atbilstu Hartai, Eiropas datu aizsardzības *acquis* un cilvēktiesībām plašākā mērogā;

([8]) Padomes Lēmums 2008/615/TI (2008. gada 23. jūnijs) par pārrobežu sadarbības pastiprināšanu, jo īpaši apkarojot terorismu un pārrobežu noziedzību (OV L 210, 6.8.2008., 1. lpp.).

35. aicina ES Pamattiesību aģentūru sadarbībā ar EDAK un EDAU izstrādāt visaptverošas vadlīnijas, ieteikumus un paraugprakses, lai precizētu kritērijus un nosacījumus MI lietotņu un risinājumu izstrādei, izmantošanai un ieviešanai tiesībaizsardzības un tiesu iestādēs; apņemas veikt pētījumu par Tiesībaizsardzības direktīvas ([9]) īstenošanu, lai apzinātu, kā tiesībaizsardzības un tiesu iestāžu veiktajās apstrādes darbībās ir nodrošināta persondatu aizsardzība, īpaši tad, kad tiek izstrādātas vai ieviestas jaunas tehnoloģijas; turklāt aicina Komisiju izsvērt, vai ir nepieciešams ar īpašu likumdošanas darbību precizēt kritērijus un nosacījumus MI lietotņu un risinājumu izstrādei, izmantošanai un ieviešanai tiesībaizsardzības un tiesu iestādēs;

36. uzdod priekšsēdētājam šo rezolūciju nosūtīt Padomei un Komisijai.

([9]) Eiropas Parlamenta un Padomes Direktīva (ES) 2016/680 (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi, ko veic kompetentās iestādes, lai novērstu, izmeklētu, atklātu noziedzīgus nodarījumus vai sauktu pie atbildības par tiem vai izpildītu krimināsodus, un par šādu datu brīvu apriti, ar ko atceļ Padomes Pamatlēmumu 2008/977/TI (OV L 119, 4.5.2016., 89. lpp.).