

Woensdag, 6 oktober 2021

P9_TA(2021)0405

Artificiële intelligentie in het strafrecht en het gebruik ervan door politieke en gerechtelijke instanties in strafzaken**Resolutie van het Europees Parlement van 6 oktober 2021 over artificiële intelligentie in het strafrecht en het gebruik ervan door politieke en gerechtelijke instanties in strafzaken (2020/2016(INI))**

(2022/C 132/02)

Het Europees Parlement,

- gezien het Verdrag betreffende de Europese Unie, en met name de artikelen 2 en 6, en het Verdrag betreffende de werking van de Europese Unie, en met name artikel 16,
- gezien het Handvest van de grondrechten van de Europese Unie (het “Handvest”), en met name de artikelen 6, 7, 8, 11, 12, 13, 20, 21, 24 en 47,
- gezien het Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden,
- gezien het Verdrag van de Raad van Europa tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens (ETS 108), en het protocol tot wijziging van dat verdrag (“Verdrag 108+”),
- gezien het Europees Ethisch Handvest over het gebruik van artificiële intelligentie in gerechtelijke systemen en hun omgeving van de Europese Commissie voor Efficiëntie in Justitie (Cepej) van de Raad van Europa,
- gezien de mededeling van de Commissie van 8 april 2019 getiteld “Vertrouwen kweken in mensgerichte kunstmatige intelligentie” (COM(2019)0168),
- gezien de ethische richtsnoeren voor betrouwbare AI, die de deskundigengroep op hoog niveau inzake artificiële intelligentie van de Commissie op 8 april 2019 heeft gepubliceerd,
- gezien het witboek van de Commissie van 19 februari 2020, getiteld “Kunstmatige intelligentie — Een Europese benadering op basis van excellentie en vertrouwen” (COM(2020)0065),
- gezien de mededeling van de Commissie van 19 februari 2020, getiteld “Een Europese datastrategie” (COM(2020)0066),
- gezien Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens, en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) ⁽¹⁾,
- gezien Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad ⁽²⁾,
- gezien Verordening (EU) 2018/1725 van het Europees Parlement en de Raad van 23 oktober 2018 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door instellingen, organen en instanties van de Unie en betreffende het vrije verkeer van die gegevens, en tot intrekking van Verordening (EG) nr. 45/2001 en Besluit nr. 1247/2002/EG ⁽³⁾,
- gezien Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie) ⁽⁴⁾,

⁽¹⁾ PB L 119 van 4.5.2016, blz. 1.

⁽²⁾ PB L 119 van 4.5.2016, blz. 89.

⁽³⁾ PB L 295 van 21.11.2018, blz. 39.

⁽⁴⁾ PB L 201 van 31.7.2002, blz. 37.

Woensdag, 6 oktober 2021

- gezien Verordening (EU) 2016/794 van het Europees Parlement en de Raad van 11 mei 2016 betreffende het Agentschap van de Europese Unie voor samenwerking op het gebied van rechtshandhaving (Europol) en tot vervanging en intrekking van de Besluiten 2009/371/JBZ, 2009/934/JBZ, 2009/935/JBZ, 2009/936/JBZ en 2009/968/JBZ van de Raad ⁽⁵⁾,
 - gezien zijn resolutie van 19 juni 2020 over de antiracismedemonstraties na de dood van George Floyd ⁽⁶⁾,
 - gezien zijn resolutie van 14 maart 2017 over de gevolgen van big data voor de grondrechten: persoonlijke levenssfeer, gegevensbescherming, non-discriminatie, veiligheid en rechtshandhaving ⁽⁷⁾,
 - gezien de hoorzitting van de Commissie burgerlijke vrijheden, justitie en binnenlandse zaken (LIBE) van 20 februari 2020 over artificiële intelligentie in het strafrecht en het gebruik ervan door politieke en gerechtelijke instanties in strafzaken,
 - gezien het verslag van het werkbezoek van de commissie LIBE aan de Verenigde Staten in februari 2020,
 - gezien artikel 54 van zijn Reglement,
 - gezien de adviezen van de Commissie interne markt en consumentenbescherming en de Commissie juridische zaken,
 - gezien het verslag van de Commissie burgerlijke vrijheden, justitie en binnenlandse zaken (A9-0232/2021),
- A. overwegende dat digitale technologieën in het algemeen en de proliferatie van door artificiële intelligentie (AI) mogelijk gemaakte dataverwerking en -analyse in het bijzonder buitengewoon veelbelovend zijn, én grote risico's met zich meebrengen; overwegende dat de afgelopen jaren op het vlak van de ontwikkeling van AI enorm veel progressie is geboekt, waardoor deze nu een van de strategische technologieën van de 21e eeuw is, met het potentieel aanzienlijke voordelen op het gebied van efficiëntie, nauwkeurigheid en comfort op te leveren, en bijgevolg een positieve verandering van de Europese economie en samenleving teweeg te brengen, hetgeen echter gepaard gaat met grote risico's voor grondrechten en voor op de rechtsstaat gebaseerde democratieën; overwegende dat AI geen doel op zich moet zijn, maar een instrument dat ten dienste staat van mensen, met als uiteindelijke doel het vergroten van het welzijn, de capaciteiten en de veiligheid van mensen;
- B. overwegende dat ondanks de voortdurend toenemende snelheid waarmee computers gegevens kunnen verwerken en de steeds groter wordende geheugencapaciteit van computers, er nog geen programma's bestaan die zich kunnen meten met de menselijke flexibiliteit op meerdere terreinen of bij de uitvoering van taken die begrip van de context of kritische analyse vereisen; overwegende dat bepaalde AI-toepassingen inmiddels menselijke deskundigen en professionals evenaren bij de uitvoering van bepaalde specifieke taken (bijv. "legal tech"), en veel sneller en op bredere schaal resultaten kunnen produceren;
- C. overwegende dat politieke en gerechtelijke instanties in sommige landen, waaronder een aantal lidstaten, op grotere schaal AI-toepassingen, of geïntegreerde AI-systemen, gebruiken dan in andere, hetgeen deels te wijten is aan een gebrek aan regelgeving en verschillen in regelgeving die het gebruik van AI voor bepaalde doeleinden mogelijk maken of juist verbieden; overwegende dat het toegenomen gebruik van AI in het strafrecht in het bijzonder gebaseerd is op de belofte dat dit zal leiden tot vermindering van bepaalde vormen van criminaliteit en tot een meer objectieve besluitvorming; overwegende dat dit evenwel niet altijd het geval is;
- D. overwegende dat de in het Handvest verankerde grondrechten en vrijheden gedurende de hele levenscyclus van AI en aanverwante technologieën, met name bij het ontwerp, de ontwikkeling, de invoering en het gebruik, gewaarborgd moeten zijn, en onder alle omstandigheden van toepassing moeten zijn bij wetshandhaving;
- E. overwegende dat AI-technologie op een manier moet worden ontwikkeld die de mens centraal stelt, het vertrouwen van het publiek geniet, en altijd ten dienste van de mens staat; overwegende dat AI-systemen zo ontworpen moeten zijn dat gewaarborgd is dat ze altijd door een mens kunnen worden uitgeschakeld;
- F. overwegende dat AI-systemen ontworpen moeten zijn met het oog op de bescherming en ten bate van alle leden van de samenleving (waarbij in het ontwerpstadium onder andere rekening moet worden gehouden met kwetsbare, gemarginaliseerde groepen), niet-discriminerend en veilig moeten zijn, over uitlegbare en transparante besluitvormingsprocessen moeten beschikken, en de autonomie en de grondrechten van de mens moeten eerbiedigen, teneinde betrouwbaar te zijn, zoals beschreven in de ethische richtsnoeren van de deskundigengroep op hoog niveau inzake kunstmatige intelligentie;

⁽⁵⁾ PB L 135 van 24.5.2016, blz. 53.

⁽⁶⁾ PB C 362 van 8.9.2021, blz. 63.

⁽⁷⁾ PB C 263 van 25.7.2018, blz. 82.

Woensdag, 6 oktober 2021

- G. overwegende dat de Unie samen met de lidstaten een cruciale verantwoordelijkheid draagt om te waarborgen dat besluiten in verband met de levenscyclus en het gebruik van AI-applicaties door politieke en gerechtelijke instanties op transparante wijze worden genomen, de grondrechten ten volle eerbiedigen, en met name discriminatie, vooringenomenheid of vooroordelen, daar waar deze bestaan, niet bestendigen; overwegende dat bij de desbetreffende beleidsbeslissingen de beginselen van noodzakelijkheid en evenredigheid moeten worden gerespecteerd, teneinde voor grondwettelijkheid en een billijk en humaan justitieel systeem te zorgen;
- H. overwegende dat AI-toepassingen grote mogelijkheden kunnen bieden op het gebied van wetshandhaving, met name door bij te dragen aan verbetering van de werkmethoden van politieke en gerechtelijke instanties, alsook aan een doeltreffendere bestrijding van bepaalde vormen van criminaliteit, met name financiële criminaliteit, het witwassen van geld en terrorismefinanciering, seksueel misbruik en de uitbuiting van kinderen online, alsook bepaalde soorten cybercriminaliteit, en daarmee aan de veiligheid en beveiliging van EU-burgers, maar óók aanzienlijke risico's voor de grondrechten van mensen in zich kunnen dragen; overwegende dat de algemene toepassing van AI met het oog op grootschalige bewaking onevenredig zou zijn;
- I. overwegende dat bij de ontwikkeling en het gebruik van AI-systemen voor respectievelijk door politieke of gerechtelijke instanties meerdere personen, organisaties, machinecomponenten, softwarealgoritmen en menselijke gebruikers betrokken zijn in vaak complexe en uitdagende omgevingen; overwegende dat AI-toepassingen voor politieke of gerechtelijke instanties zich in verschillende fasen van ontwikkeling bevinden, van de conceptualiserings-, de prototyping- en de evaluatiefase tot de fase van gebruik na goedkeuring; overwegende dat er in de toekomst nieuwe gebruiksmogelijkheden kunnen ontstaan naarmate de technologieën volwassen worden als gevolg van lopend wereldwijd wetenschappelijk onderzoek;
- J. overwegende dat het een absolute "must" is een duidelijk model voor het toeschrijven van de juridische verantwoordelijkheid voor de potentiële schadelijke gevolgen van AI-systemen op het gebied van het strafrecht te ontwikkelen; overwegende dat regelgeving op dit vlak er nooit toe mag leiden dat de eindverantwoordelijkheid elders komt te liggen dan bij de mens, én er eerst en vooral op gericht moet zijn schadelijke effecten überhaupt te vermijden;
- K. overwegende dat het uiteindelijk de verantwoordelijkheid van de lidstaten is om te waarborgen dat bij het gebruik van AI-systemen door politieke of gerechtelijke instanties de grondrechten volledig worden gerespecteerd;
- L. overwegende dat het verband tussen bescherming van grondrechten en doeltreffend politiewerk altijd een essentieel element moet zijn in de discussies over het gebruik (of überhaupt, en hoe) van AI door politieke instanties, waar beslissingen blijvende gevolgen voor het leven en de vrijheden van personen kunnen hebben; overwegende dat dit van bijzonder groot belang is omdat AI het potentieel heeft om in de vorm van analyse en bijstand in het kader van onderzoeken een vast onderdeel van ons strafrechtelijk ecosysteem te worden;
- M. overwegende dat in het kader van wetshandhaving gebruik wordt gemaakt van AI, onder meer bestaand uit gezichtsherkenningstechnologie om bijvoorbeeld verdachte databanken te doorzoeken en slachtoffers van mensenhandel of seksuele uitbuiting van kinderen op te sporen, automatische nummerplaat herkenning, identificatie van de spreker, spraakidentificatie, spraakafzienttechnologieën, fonetisch toezicht (d.w.z. algoritmen voor gewerschotdetectie), autonoom onderzoek en analyse van geïdentificeerde databanken, prognoses (voorspellend politiewerk en analyse van misdaadhotspots), instrumenten voor het opsporen van gedrag, geavanceerde virtuele autopsie-instrumenten voor het vaststellen van de doodsoorzaak, autonome instrumenten voor het opsporen van financiële fraude en terrorismefinanciering, monitoring van de sociale media (scraping en harvesting voor dataminingconnecties), en geautomatiseerde bewakingssystemen waarin verschillende detectiemogelijkheden zijn verwerkt (zoals camera's voor hartslagdetectie en thermische camera's); overwegende dat de betrouwbaarheid en nauwkeurigheid van de bovengenoemde toepassingen, alsook hun impact op de bescherming van grondrechten en op de dynamiek van strafrechtssystemen, en die van andere potentiële of toekomstige AI-toepassingen op het gebied van wetshandhaving, sterk kunnen uiteenlopen; overwegende dat veel van deze instrumenten in derde landen worden gebruikt, maar in de Unie illegaal zijn krachtens het wetgevingskader en de rechtspraak van de Unie inzake gegevensbescherming; overwegende dat het routinematige gebruik van algoritmen, zelfs met een laag percentage aan valse positieven, ertoe kan leiden dat het aantal valse waarschuwingen het aantal correcte waarschuwingen ruim overtreft;
- N. overwegende dat AI-instrumenten en -toepassingen ook wereldwijd in meerdere landen door gerechtelijke instanties worden gebruikt, onder meer ter ondersteuning van besluiten inzake voorlopige hechtenis, bij veroordeling, de berekening van de kans op recidive en de vaststelling van de proeftijd, onlinegeschillenbeslechting, beheer van de jurisprudentie en het toegankelijker maken van het recht; overwegende dat dit heeft geleid tot verstoorde en kleinere kansen voor kleurlingen en andere minderheden; overwegende dat het gebruik ervan in de EU, op een paar lidstaten na, op dit moment hoofdzakelijk beperkt blijft tot het civiel gebied;
- O. overwegende dat het gebruik van AI bij wetshandhaving een aantal potentieel grote, en in sommige gevallen onaanvaardbare, risico's voor de bescherming van grondrechten van personen met zich meebrengt, zoals ondoorzichtige besluitvorming, verschillende vormen van discriminatie en fouten die inherent zijn aan het onderliggende algoritme, en die kunnen worden versterkt door feedbackloops, evenals risico's voor de bescherming

Woensdag, 6 oktober 2021

van de persoonlijke levenssfeer en persoonsgegevens, de bescherming van de vrijheid van meningsuiting en informatie, het vermoeden van onschuld, het recht op doeltreffende rechtsmiddelen en een eerlijk proces, alsook risico's voor de vrijheid en veiligheid van personen;

- P. overwegende dat AI-systemen die door politieke en gerechtelijke instanties worden gebruikt, ook kwetsbaar zijn voor door AI aangedreven aanvallen op informatiesystemen of gegevensvergiftiging, waarbij opzettelijk verkeerde gegevensreeksen worden ingevoerd om vertekende resultaten te produceren; overwegende dat de daaruit voortvloeiende schade in deze situaties potentieel nog aanzienlijker is en kan leiden tot een exponentiële toename van de schade voor zowel individuen als groepen;
- Q. overwegende dat het gebruik van AI door politieke en gerechtelijke instanties niet moet worden gezien als uitsluitend een technische mogelijkheid, maar veeleer als een politiek besluit over het ontwerp en de doelstellingen van wetshandhaving en strafrechtssystemen; overwegende dat het moderne strafrecht gebaseerd is op het idee dat autoriteiten pas op een strafbaar feit reageren nadat het is gepleegd, zonder ervan uit te gaan dat alle mensen gevaarlijk zijn en permanent in de gaten moeten worden gehouden om mogelijke wetsovertredingen te voorkomen; overwegende dat op AI gebaseerde surveillancetechnologieën deze benadering in sterke mate ondermijnen en wetgevers overal ter wereld dwingen tot een grondige analyse van de gevolgen van het gebruik van technologieën die de rol van de mens bij wetshandhaving en in de rechtspleging verkleinen;
1. herhaalt dat, aangezien de verwerking van grote hoeveelheden persoonsgegevens de kern vormt van AI, het recht op bescherming van de persoonlijke levenssfeer en persoonsgegevens van toepassing is op alle gebieden van AI, en dat het rechtskader van de Unie voor gegevensbescherming en privacy volledig moet worden nageleefd; herinnert er derhalve aan dat de EU reeds gegevensbeschermingsnormen voor de wetshandhaving heeft vastgesteld, die de grondslag vormen voor de toekomstige regelgeving inzake het gebruik van AI door politieke en gerechtelijke instanties; herinnert eraan dat de verwerking van persoonsgegevens wettig en billijk moet zijn, het ermee beoogde doel gespecificeerd, expliciet en legitiem moet zijn, adequaat, relevant en evenredig moet zijn met het nagestreefde doel, accuraat moet zijn en up-to-date moet worden gehouden, dat inaccurate gegevens, behoudens in gevallen waarin beperkingen van toepassing zijn, gecorrigeerd of gewist moeten worden, gegevens niet langer dan noodzakelijk moeten worden bewaard, duidelijke en passende termijnen moeten worden vastgesteld voor het wissen of periodiek toetsen van de noodzaak om dergelijke gegevens op te slaan, en de verwerking op beveiligde wijze moet plaatsvinden; onderstreept daarnaast dat de mogelijke identificatie van personen middels een AI-toepassing die gebruik maakt van gegevens die eerder geanonimiseerd waren, moet worden voorkomen;
 2. bevestigt nogmaals dat alle AI-oplossingen voor politieke en gerechtelijke instanties ook de beginselen van menselijke waardigheid, non-discriminatie, vrij verkeer, het vermoeden van onschuld en de rechten van de verdediging, met inbegrip van het zwijgrecht, de vrijheid van meningsuiting en informatie, de vrijheid van vergadering en vereniging, gelijkheid voor de wet, het beginsel van wapengelijkheid en het recht op een effectief rechtsmiddel en een eerlijk proces volledig in acht moeten nemen, in overeenstemming met het Handvest en het Europees Verdrag inzake de rechten van de mens; benadrukt dat het gebruik van AI-toepassingen moet worden verboden wanneer dit onverenigbaar is met de grondrechten;
 3. onderkent dat de ontwikkeling van AI-toepassingen wereldwijd zo snel gaat dat het onmogelijk is een uitputtende lijst daarvan op te stellen en er derhalve een helder en samenhangend governance-model nodig is met zowel waarborgen voor de grondrechten van personen als rechtszekerheid voor ontwikkelaars, gezien de niet-aflatende technologische evolutie; is, gezien de rol en de verantwoordelijkheid van politie en justitie, alsmede gezien de impact van de beslissingen die zij nemen met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, evenwel van oordeel dat het gebruik van AI-toepassingen in gevallen met mogelijkerwijs grote gevolgen voor het leven van afzonderlijke personen als zeer risicovol moet worden aangemerkt;
 4. is in dit verband van mening dat elk AI-instrument dat door politieke of gerechtelijke instanties ontwikkeld of gebruikt wordt, ten minste veilig, robuust, beveiligd en geschikt voor het beoogde doel moet zijn en de beginselen van billijkheid, gegevensminimalisering, verantwoordingsplicht, transparantie, non-discriminatie en verklaarbaarheid in acht moet nemen, en dat de ontwikkeling, de invoering en het gebruik ervan moeten worden onderworpen aan een effectbeoordeling en een strikte noodzakelijkheids- en evenredigheidstoets, met waarborgen die evenredig zijn aan de geïdentificeerde risico's; wijst erop dat het vertrouwen van burgers in AI die in de EU ontwikkeld, ingevoerd en gebruikt wordt, zal afhangen van de volledige vervulling van deze criteria;
 5. erkent de positieve bijdrage van bepaalde soorten AI-toepassingen voor het werk van politieke en gerechtelijke instanties in de Unie; wijst daarbij bijvoorbeeld op het verbeterde beheer van jurisprudentie met behulp van instrumenten die extra zoekopties bieden; is van oordeel dat er nog meer potentiële toepassingen van AI voor politieke en gerechtelijke

Woensdag, 6 oktober 2021

instanties zijn die het onderzoeken waard zijn, rekening houdend met de vijf beginselen van het Ethisch Handvest over het gebruik van artificiële intelligentie in gerechtelijke systemen en hun omgeving van het Cepej, en met bijzondere aandacht voor de door het Cepej geïdentificeerde “gebruikstoepassingen die met uiterste terughoudendheid dienen te worden overwogen”;

6. benadrukt dat elke technologie kan worden herbestemd, en dringt derhalve aan op strikte democratische controle en onafhankelijk toezicht op alle door politieke en gerechtelijke instanties gebruikte AI-technologieën, met name die welke kunnen worden herbestemd voor grootschalige surveillance of grootschalige profilering; maakt zich derhalve grote zorgen over het potentieel van bepaalde AI-technologieën om in het kader van wetshandhaving voor grootschalige surveillancedoeleinden te worden gebruikt; onderstreept het wettelijk vereiste om te voorkomen dat AI-technologieën voor grootschalige surveillance worden gebruikt, die per definitie niet in overeenstemming is met de beginselen van noodzakelijkheid en evenredigheid, en dringt aan op een verbod op toepassingen die hierin resulteren;

7. beklemtoont dat de wijze waarop sommige derde landen de ontwikkeling, de invoering en het gebruik van technologieën voor grootschalige surveillance benaderen, waarbij in concreto het evenredigheidsbeginsel niet in acht wordt genomen, de grondrechten schendt en derhalve door de EU niet moet worden gekopieerd; beklemtoont dan ook dat uniforme, Uniebrede regels nodig zijn met waarborgen tegen misbruik van AI-technologieën door politieke en gerechtelijke instanties;

8. wijst op het potentieel voor vooringenomenheid en discriminatie van het gebruik van AI-toepassingen, zoals instrumenten voor machinaal leren, met inbegrip van de algoritmes waar dergelijke toepassingen op gebaseerd zijn; merkt op dat vooringenomenheid inherent kan zijn aan de onderliggende gegevensreeksen, met name wanneer historische gegevens worden gebruikt, ingevoerd door de ontwikkelaars van de algoritmen of gegenereerd wanneer de systemen in reële omgevingen worden toegepast; geeft aan dat de resultaten die met AI-toepassingen worden verkregen per definitie beïnvloed zijn door de kwaliteit van de gebruikte gegevens en dat de desbetreffende inherente vooringenomenheid waarschijnlijk geleidelijk groter zal worden en daarmee bestaande discriminatie zal bestendigen en vergroten, met name voor personen die tot bepaalde etnische groepen of door raciale scheidslijnen gekenmerkte gemeenschappen behoren;

9. benadrukt dat veel van de momenteel gebruikte, op grond van algoritmen gestuurde identificatietechnologieën personen uit door raciale scheidslijnen gekenmerkte gemeenschappen, leden van bepaalde etnische minderheden, lhbtbi-personen, kinderen, ouderen en vrouwen onevenredig vaak verkeerd identificeren en classificeren, en derhalve schade berokkenen; herinnert eraan dat personen niet alleen het recht hebben om correct te worden geïdentificeerd, maar ook om helemaal niet te worden geïdentificeerd, tenzij dat wettelijk verplicht is om dwingende en legitieme redenen van algemeen belang; beklemtoont dat AI-voorspellingen die gebaseerd zijn op de kenmerken van een specifieke groep personen, uiteindelijk resulteren in vergroting en bestendiging van bestaande vormen van discriminatie; is van oordeel dat serieuze inspanningen moeten worden ondernomen om geautomatiseerde discriminatie en vooringenomenheid te voorkomen; vraagt om robuuste aanvullende waarborgen voor gevallen waarin AI-systemen door politieke of gerechtelijke instanties worden toegepast ten aanzien van of met betrekking tot minderjarigen;

10. wijst op de machtsasymmetrie tussen degenen die AI-technologieën gebruiken en degenen op wie deze worden toegepast; benadrukt dat absoluut voorkomen moet worden dat het gebruik van AI door politieke of gerechtelijke instanties een factor voor ongelijkheid, sociale breuken of uitsluiting wordt; onderstreept de gevolgen van het gebruik van AI-instrumenten voor de rechten van verdediging van verdachten, het probleem om betekenisvolle informatie over de werking daarvan te verkrijgen, en het daaruit voortvloeiende probleem om de resultaten daarvan voor de rechtbank aan te vechten, met name door personen tegen wie een onderzoek loopt;

11. neemt kennis van de risico's die zijn verbonden aan met name datalekken, inbreuken op de gegevensbeveiliging en onbevoegde toegang tot persoonsgegevens en andere gegevens die verband houden met bijvoorbeeld strafrechtelijk onderzoeken of rechtszaken en die worden verwerkt door AI-systemen; onderstreept dat de beveiligings- en veiligheidsaspecten van AI-systemen die door politieke of gerechtelijke instanties worden gebruikt zorgvuldig moeten worden overwogen en voldoende robuust en veerkrachtig moeten zijn om de mogelijk catastrofale gevolgen van kwaadaardige aanvallen op AI-systemen te voorkomen; benadrukt het belang van beveiliging door ontwerp, alsook van specifiek menselijk toezicht, voorafgaand aan de ingebruikname van bepaalde kritieke toepassingen, en dringt er derhalve op aan dat politieke en gerechtelijke instanties alleen gebruikmaken van AI-toepassingen die de privacy waarborgen en het beginsel van beveiliging door ontwerp respecteren, teneinde functievoerschuiving te vermijden;

12. benadrukt dat geen enkel AI-systeem dat door politieke of gerechtelijke instanties wordt gebruikt zodanig ontworpen mag zijn dat het de fysieke integriteit van mensen kan aantasten, rechten kan toewijzen of wettelijke verplichtingen kan opleggen aan mensen;

13. erkent dat het, gezien de complexiteit van de ontwikkeling en het beheer van AI-systemen, een uitdaging is om vast te stellen waar de juridische verantwoordelijkheid en aansprakelijkheid voor potentiële schade ligt; acht het noodzakelijk om duidelijke en billijke regels vast te stellen voor het toeschrijven van de juridische verantwoordelijkheid en aansprakelijkheid voor de potentiële negatieve gevolgen van deze geavanceerde digitale technologieën; onderstreept evenwel dat het doel in de

Woensdag, 6 oktober 2021

eerste plaats moet zijn te voorkomen dat die schadelijke effecten überhaupt ontstaan; dringt er dan ook op aan bij het gebruik van AI-toepassingen in het kader van wetshandhaving stelselmatig het voorzorgsbeginsel toe te passen; onderstreept dat de juridische verantwoordelijkheid en aansprakelijkheid altijd bij een natuurlijke of een rechtspersoon moet liggen, die altijd moet worden geïdentificeerd voor beslissingen die met behulp van AI worden genomen; wijst dan ook met klem op de noodzaak van het waarborgen van de transparantie van de bedrijfsstructuren die AI-systemen produceren en beheren;

14. acht het voor zowel de effectiviteit van de uitoefening van verdedigingsrechten als voor de transparantie van nationale strafrechtstelsels van essentieel belang dat een specifiek, duidelijk en precies wettelijk kader voorziet in de voorwaarden, modaliteiten en consequenties van het gebruik van AI door politieke of gerechtelijke instanties, evenals in de rechten van de betrokkenen, en in doeltreffende en laagdrempelige klachten- en verhaalprocedures, met inbegrip van verhaalmogelijkheden voor de rechter; onderstreept dat de partijen in een strafrechtzaak recht hebben op toegang tot het gegevensverzamelingsproces en de daaraan gerelateerde beoordelingen die middels het gebruik van AI-toepassingen gemaakt of verkregen worden; onderstreept dat uitvoerende autoriteiten die in het kader van justitiële samenwerking besluiten over uitleverings- of overleveringsverzoeken van andere lidstaten of derde landen nemen, moeten beoordelen of het gebruik van AI-instrumenten in het verzoekende land klaarblijkelijk afbreuk kan doen aan het grondrecht op een eerlijk proces; verzoekt de Commissie richtsnoeren op te stellen voor het doorvoeren van een dergelijke beoordeling in het kader van justitiële samenwerking in strafrechtzaken; is van oordeel dat de lidstaten, in overeenstemming met toepasselijke wetgeving, erop toe moeten zien dat de betrokken personen ervan in kennis worden gesteld indien politieke of gerechtelijke instanties AI-toepassingen gebruiken;

15. wijst erop dat als mensen zich uitsluitend op door machines gegenereerde gegevens, profielen en aanbevelingen baseren, zij geen onafhankelijke beoordeling kunnen maken; wijst op de mogelijkerwijs ernstige nadelige gevolgen, met name op het gebied van wetshandhaving en justitie, wanneer personen een te groot vertrouwen hebben in de klaarblijkelijk objectieve en wetenschappelijke aard van AI-instrumenten en niet denken aan de mogelijkheid dat hun resultaten onjuist, onvolledig, irrelevant of discriminerend kunnen zijn; benadrukt dat niet te veel moet worden gesteund op de resultaten van AI-systemen, en beklemtoont dat autoriteiten vertrouwen en kennis moeten opbouwen om een algoritmische aanbeveling in twijfel te trekken of hiervan af te wijken; acht het belangrijk realistische verwachtingen van dergelijke technologische oplossingen te hebben en geen perfecte wetshandavingsoplossingen te verwachten of te beloven dat alle gepleegde strafbare feiten aan het licht zullen worden gebracht;

16. benadrukt dat in politieke en gerechtelijke contexten elke beslissing met een rechts- of een vergelijkbaar gevolg altijd moet worden genomen door een mens, die verantwoordelijk kan worden gehouden voor de genomen beslissingen; is van oordeel dat indien AI-systemen worden gebruikt, de betrokken personen de mogelijkheid van een rechtsmiddel moet worden geboden; herinnert eraan dat personen krachtens het EU-recht het recht hebben dat ten aanzien van hen geen beslissingen worden genomen met een rechtsgevolg of die een significante invloed op hen hebben indien deze beslissingen uitsluitend gebaseerd zijn op geautomatiseerde gegevensverwerking; onderstreept daarnaast dat geautomatiseerde individuele besluiten niet gebaseerd mogen zijn op bijzondere categorieën van persoonsgegevens, tenzij er passende maatregelen ter bescherming van de rechten en vrijheden en van de gerechtvaardigde belangen van de betrokkene zijn getroffen; Benadrukt dat het EU-recht profilering die tot discriminatie van natuurlijke personen op basis van bijzondere categorieën van persoonsgegevens leidt, verbiedt; onderstreept dat, als gevolg van de uitvoerende functie van wetshandavingsinstanties en hun acties, besluiten op het gebied van wetshandhaving bijna altijd rechtsgevolgen voor de betrokken persoon hebben; stelt vast dat het gebruik van AI menselijke beslissingen kan beïnvloeden en gevolgen kan hebben voor alle fasen van strafrechtelijke procedures; is derhalve van oordeel dat autoriteiten die AI-systemen gebruiken zeer hoge wettelijke normen in acht moeten nemen en menselijk ingrijpen moeten garanderen, met name bij de analyse van met dergelijke systemen gegenereerde gegevens; verlangt derhalve dat geen afbreuk wordt gedaan aan de soevereine oordeelkundigheid van rechters, noch aan het beginsel van besluitvorming per geval; dringt aan op een verbod op het gebruik van AI en aanverwante technologieën bij het formuleren van ontwerpen van rechterlijke beslissingen;

17. roept op tot verklaarbaarheid, transparantie, traceerbaarheid en verificatie van algoritmen als een onmisbaar onderdeel van toezicht, teneinde ervoor te zorgen dat de ontwikkeling, de invoering en het gebruik van AI-systemen voor respectievelijk door politieke of gerechtelijke instanties in overeenstemming zijn met de grondrechten en vertrouwen genieten van de burgers, alsook om ervoor te zorgen dat door AI-algoritmen gegenereerde resultaten begrijpelijk zijn voor de gebruikers en degenen die aan deze systemen worden onderworpen, en dat er transparantie is ten aanzien van de brongegevens en de wijze waarop het systeem tot een bepaalde conclusie is gekomen; geeft aan dat om technische transparantie, robuustheid en nauwkeurigheid te waarborgen politieke en gerechtelijke instanties in de Unie alleen instrumenten en systemen mogen gebruiken waarvan de algoritmen en logica gecontroleerd kunnen worden door en toegankelijk zijn voor in ieder geval politie en justitie, alsmede onafhankelijke toezichthouders, met het oog op beoordeling, controle en doorlichting, en die door de verkopers niet zijn afgesloten en auteursrechtelijk zijn beschermd; wijst er verder op dat in duidelijke en begrijpelijke taal gestelde documenten moeten worden verstrekt over de aard van de dienst, de ontwikkelde instrumenten, de prestaties en de voorwaarden waaronder ze geacht kunnen worden te werken en de risico's die er mogelijkerwijs aan verbonden zijn; dringt er derhalve bij politieke en gerechtelijke instanties op aan voor proactieve en

Woensdag, 6 oktober 2021

volledige transparantie te zorgen met betrekking tot particuliere bedrijven van wie zij AI-systemen kopen voor politieke- en gerechtelijke doeleinden; beveelt dan ook aan daar waar mogelijk gebruik te maken van opensourcesoftware;

18. moedigt politieke en gerechtelijke instanties aan de gebieden waar op maat gesneden AI-oplossingen van nut zouden kunnen zijn, in kaart te brengen en te beoordelen, en goede praktijken op het gebied van de invoering van AI uit te wisselen; verzoekt de lidstaten en de EU-agentschappen voor passende aanbestedingsprocedures voor AI-systemen voor politieke- en gerechtelijke doeleinden te zorgen, om te waarborgen dat deze de grondrechten respecteren en aan de toepasselijke wetgeving voldoen, en erop toe te zien dat softwaredocumentatie en -algoritmes met het oog op toetsing beschikbaar en toegankelijk zijn voor de bevoegde en toezichthoudende autoriteiten; dringt in het bijzonder aan op bindende regels inzake openbaarmaking van publiek-private partnerschappen, contracten en aankopen, alsook van de doeleinden daarvan; benadrukt dat instanties de nodige financiële middelen moeten krijgen en over de nodige deskundigheid moeten beschikken om volledige naleving van de ethische, wettelijke en technische vereisten in verband met het gebruik van alle AI-toepassingen te waarborgen;

19. roept op tot tracerbaarheid van de AI-systemen en van het besluitvormingsproces waarmee de functies, de capaciteiten en de beperkingen ervan worden vastgelegd en de bepalende kenmerken van een beslissing worden geregistreerd, middels verplichte documentatie; onderstreept dat het belangrijk is volledige documentatie bij te houden van trainingsgegevens, de context daarvan, het doel, de nauwkeurigheid en de bijwerkingen, alsook van de verwerking daarvan door de bouwers en ontwikkelaars van de algoritmes en de naleving van de grondrechten; onderstreept dat het altijd mogelijk moet zijn de berekeningen van een AI-systeem terug te brengen tot een vorm die voor mensen begrijpelijk is;

20. verzoekt om een verplichte beoordeling van het effect op grondrechten, die moet worden verricht voorafgaand aan de invoering of het gebruik van elk AI-systeem door politieke of gerechtelijke instanties, om elk potentieel risico voor de grondrechten te beoordelen; herinnert eraan dat elk type verwerking met een hoog risico voor de rechten en vrijheden van natuurlijke personen, met name wanneer bij die verwerking nieuwe technologieën worden gebruikt, voorafgaand verplicht aan een beoordeling van de effecten op de gegevensbescherming moet worden onderworpen, en is van mening dat dit geldt voor de meeste AI-technologieën die door politieke of gerechtelijke instanties worden gebruikt; onderstreept de deskundigheid van gegevensbeschermingsautoriteiten en grondrechtenagentschappen voor het beoordelen van deze systemen; benadrukt dat deze beoordelingen van de effecten op de grondrechten zo transparant mogelijk moeten plaatsvinden en met de actieve betrokkenheid van het maatschappelijk middenveld; verlangt dat in het kader van de effectbeoordelingen ook duidelijk wordt aangegeven welke maatregelen moeten worden getroffen om de geïdentificeerde risico's aan te pakken, en dat de desbetreffende beoordelingen in principe altijd voorafgaand aan de invoering van AI-systemen openbaar moeten worden gemaakt;

21. benadrukt dat alleen een robuuste Europese governance van AI met onafhankelijke evaluatie kan waarborgen dat de beginselen van de grondrechten operationeel worden gemaakt; dringt aan op verplichte periodieke controles, door een onafhankelijke instantie, van alle door politieke of gerechtelijke instanties gebruikte AI-systemen wanneer de kans bestaat dat zij het leven van personen sterk beïnvloeden, teneinde algoritmische systemen, hun context, doel, nauwkeurigheid, prestaties en schaal te testen en te evalueren, en om, nadat deze operationeel zijn geworden, ongewenste en negatieve effecten op te sporen, te onderzoeken, te diagnosticeren en te corrigeren, en ervoor te zorgen dat AI-systemen werken zoals beoogd; dringt er derhalve op aan hiervoor een helder institutioneel kader vast te stellen, inclusief passende regelgeving en toezicht om volledige tenuitvoerlegging daarvan te waarborgen, en een volledig geïnformeerd democratisch debat te voeren over de noodzaak en evenredigheid van AI op strafrechtgebied; onderstreept dat de resultaten van deze controles in openbare registers moeten worden vastgelegd, zodat burgers weten welke AI-systemen worden gebruikt en welke maatregelen worden getroffen om eventuele schendingen van de grondrechten te verhelpen;

22. benadrukt dat de gegevensreeksen en de algoritmische systemen die voor het produceren van classificaties, beoordelingen en voorspellingen in de verschillende fasen van de gegevensverwerking voor de ontwikkeling van AI en aanverwante technologieën worden gebruikt, ook kunnen resulteren in een gedifferentieerde behandeling en in zowel directe als indirecte discriminatie van groepen personen, met name aangezien de gegevens die gebruikt worden om voorspellende politiaalgoritmes te trainen, een weerspiegeling vormen van bestaande surveillanceprioriteiten en derhalve uiteindelijk kunnen leiden tot de uitbreiding en reproductie van bestaande vooringenomenheid; beklemtoont dan ook dat AI-technologieën, met name wanneer deze door politieke of gerechtelijke instanties worden gebruikt, onderzoek door en input van meerdere disciplines vereisen, waaronder wetenschap en technologie, "critical race studies", "disability studies", en andere disciplines die zich bezighouden met de sociale context, onder meer de manier waarop verschillen worden geconstrueerd, classificeringswerkzaamheden en de gevolgen ervan; benadrukt dat er daarom systematisch onderzoek moet worden gedaan naar de integratie van deze disciplines in AI-studies en -onderzoek op alle niveaus; benadrukt verder dat het belangrijk is dat de teams die deze AI-systemen voor politieke of gerechtelijke instanties ontwerpen, ontwikkelen, testen, onderhouden, invoeren en inkopen, waar mogelijk, een afspiegeling vormen van de verscheidenheid van de samenleving als geheel, als een niet-technisch middel om de risico's van discriminatie te verkleinen;

Woensdag, 6 oktober 2021

23. wijst er daarnaast op dat, om adequate verantwoording, verantwoordelijkheid en aansprakelijkheid te waarborgen, een gespecialiseerde opleiding over ethische normen, potentiële gevaren, beperkingen en correct gebruik van AI-technologie onontbeerlijk is, met name voor personeel van politie en justitie; benadrukt dat passende beroepsopleiding en kwalificaties ervoor moeten zorgen dat besluitvormers geschoold zijn ten aanzien van de mogelijkheid van vooringenomenheid, aangezien de gegevensreeksen gebaseerd kunnen zijn op discriminerende en bevooroordeelde gegevens; steunt bewustmakings- en educatieve initiatieven om ervoor te zorgen dat personeel van politie en justitie zich bewust is van en inzicht heeft in de beperkingen, capaciteiten en risico's die het gebruik van AI met zich meebrengt, waaronder het risico van vooringenomenheid in geautomatiseerde processen; geeft aan dat indien in de gegevensreeksen die bij AI-opleidingen worden gebruikt gevallen van racisme door de politie bij de uitoefening van hun taken worden opgenomen, dit ongetwijfeld tot racistische vooringenomenheid bij middels AI gegenereerde resultaten, scores en aanbevelingen zal leiden; herhaalt daarom zijn oproep aan de lidstaten om antidiscriminatiebeleid te bevorderen en nationale actieplannen tegen racisme op het gebied van politie en justitie te ontwikkelen;

24. erkent dat voorspellend politiewerk tot de AI-toepassingen behoort die op het vlak van wetshandhaving worden gebruikt, maar waarschuwt dat met voorspellend politiewerk wel gegevensreeksen kunnen worden geanalyseerd voor de identificatie van patronen en correlaties, maar de causaliteitsvraag niet kan worden beantwoord en geen betrouwbare voorspellingen over individueel gedrag kunnen worden gedaan, en dat dit daarom nooit de enige grond voor interventie kan vormen; geeft aan dat meerdere steden in de Verenigde Staten na controles gestopt zijn met het gebruik van systemen voor voorspellend politiewerk; herinnert eraan dat de leden van LIBE tijdens het werkbezoek van deze commissie aan de Verenigde Staten in februari 2020 van de politie van New York City en Cambridge, Massachusetts, te horen kregen dat die hun voorspellende politieprogramma's hadden afgebouwd wegens een gebrek aan effectiviteit, discriminerende impact en ontoepasbaarheid in de praktijk, en in plaats daarvan over waren gestapt op gemeenschapsgericht politiewerk; stelt vast dat dit tot een daling van de criminaliteitscijfers heeft geleid; is er derhalve tegen dat wetshandavingsinstanties AI gebruiken voor het doen van voorspellingen over het gedrag van personen of groepen op basis van historische gegevens en gedrag uit het verleden, lidmaatschap van een groep, locatie, of enig ander dergelijk kenmerk in een poging in kaart te brengen bij welke personen de kans het grootst is dat ze een strafbaar feit zullen begaan;

25. neemt kennis van de verschillende vormen van gebruik van gezichtsherkenning, zoals, maar niet beperkt tot, verificatie/authenticatie (d.w.z. het matchen van een levend gezicht met een foto in een identiteitsbewijs, denk aan slimme grenzen), identificatie (d.w.z. het matchen van een foto met een fotogegevensbank), en detectie (d.w.z. het in real time detecteren van gezichten van bronnen zoals camerabeelden, en het matchen daarvan met gegevensbanken, denk aan real time surveillance), elk met hun eigen implicaties voor de bescherming van grondrechten; is van mening dat de invoering van gezichtsherkenningssystemen door wetshandavingsinstanties te allen tijde beperkt moet zijn tot duidelijk gerechtvaardigde doeleinden, met volledige eerbiediging van de beginselen van noodzakelijkheid en evenredigheid, en van het toepasselijke recht; herbevestigt dat het gebruik van gezichtsherkenningstechnologie ten minste moet voldoen aan de vereisten van gegevensminimalisering, nauwkeurigheid van gegevens, opslagbeperking, gegevensbeveiliging en verantwoording en daarnaast rechtmatig, billijk en transparant moet zijn, en moet beantwoorden aan een specifiek, uitdrukkelijk en legitiem doel dat duidelijk gedefinieerd is in het nationale of het Unierecht; is van oordeel dat verificatie- en authenticatiesystemen alleen succesvol ingevoerd en gebruikt kunnen blijven worden indien de negatieve effecten ervan kunnen worden beperkt en aan de hierboven vermelde criteria wordt voldaan;

26. roept verder op tot een permanent verbod op het gebruik van geautomatiseerde analyse en/of herkenning in openbare ruimten van andere menselijke kenmerken, zoals tred, vingerafdrukken, DNA, stemgeluid, en andere biometrische en gedragsignalen;

27. dringt overigens aan op een moratorium op de invoering van gezichtsherkenningssystemen voor wetshandavingsdoeleinden met de identificatiefunctie, tenzij die functie uitsluitend wordt gebruikt voor de identificatie van slachtoffers van strafbare feiten, totdat de technische normen kunnen worden beschouwd als volledig in overeenstemming met de grondrechten, de afgeleide resultaten niet-discriminerend zijn, het rechtskader voorziet in strenge waarborgen en strikte democratische controle en supervisie, en er empirisch bewijs is van de noodzaak en de evenredigheid van de toepassing van dergelijke technologieën; is van oordeel dat indien niet aan de bovenstaande criteria wordt voldaan, deze systemen niet moeten worden gebruikt of ingevoerd;

28. geeft uiting aan zijn grote bezorgdheid over het gebruik van particuliere gezichtsherkenningsdatabanken door wetshandavingsactoren en inlichtingendiensten, zoals Clearview AI, een databank van meer dan drie miljard afbeeldingen, waaronder van EU-burgers, die onrechtmatig zijn verzameld op sociale media en andere delen van het internet; verzoekt de lidstaten wetshandavingsactoren te verplichten bekend te maken of ze Clearview AI-technologie, of equivalente technologieën van andere aanbieders, gebruiken; herinnert aan het advies van het Europees Comité voor gegevensbescherming (EDPB) dat het gebruik van een dienst als Clearview AI door wetshandavingsinstanties in de Europese Unie "waarschijnlijk niet in overeenstemming is met de gegevensbeschermingswetgeving van de EU"; dringt erop aan een verbod in te voeren op het gebruik van particuliere gezichtsherkenningsdatabanken in het kader van wetshandhaving;

Woensdag, 6 oktober 2021

29. neemt kennis van de studie van de Commissie naar de haalbaarheid van mogelijke wijzigingen van het Prüm-besluit⁽⁸⁾, waaronder met betrekking tot beelden van gezichten; neemt kennis van eerder onderzoek waaruit gebleken is dat geen enkele potentiële nieuwe identificatiemethode, zoals iris- of gezichtsherkenning, in de forensische context even betrouwbaar is als DNA of vingerafdrukken; herinnert de Commissie eraan dat elk nieuw wetgevingsvoorstel gebaseerd moet zijn op wetenschappelijk bewijs en eerbiediging van het evenredigheidsbeginsel; dringt er bij de Commissie op aan het kader van het Prüm-besluit niet te verlengen, tenzij er solide wetenschappelijk bewijs beschikbaar is dat gezichtsherkenning in een forensische context even betrouwbaar is als DNA of vingerafdrukken, na uitvoering van een volledige effectbeoordeling en met in inachtneming van de aanbevelingen van de Europese Toezichthouder voor gegevensbescherming (EDPS) en het EDPB;

30. benadrukt dat het gebruik van biometrische gegevens meer in het algemeen verband houdt met het beginsel van het recht op menselijke waardigheid als basis voor alle door het Handvest gegarandeerde grondrechten; is van mening dat het verzamelen en gebruiken van biometrische gegevens ten behoeve van identificatie op afstand, zoals door gezichtsherkenning in openbare ruimten en bij geautomatiseerde grenscontroles op luchthavens, specifieke risico's voor de grondrechten met zich mee kan brengen, met sterk uiteenlopende gevolgen afhankelijk van het doel, de context en de schaal waarop dit gebeurt; wijst daarnaast op de betwiste wetenschappelijke validiteit van affectherkenningstechnologie, zoals camera's die oogbewegingen en veranderingen in de pupilgrootte meten, in een wetshandhavingscontext; is van oordeel dat het gebruik van biometrische identificatie door politieke of gerechtelijke instanties altijd als "zeer risicovol" moet worden beschouwd en daarom onderworpen moet zijn aan aanvullende vereisten, overeenkomstig de aanbevelingen van de deskundigengroep op hoog niveau inzake AI van de Commissie;

31. maakt zich grote zorgen over door Horizon 2020 gefinancierde onderzoeksprojecten waarin gebruik wordt gemaakt van artificiële intelligentie aan de buitengrenzen, zoals het iBorderCtrl-project, een "slim leugendetectiesysteem" waarin reizigers worden geprofileerd op basis van een geautomatiseerd onderhoud via de webcam van de reiziger voorafgaand aan de reis en een op AI gebaseerde analyse van 38 microgezichtsuitdrukkingen, dat is getest in Hongarije, Letland en Griekenland; verzoekt de Commissie dan ook de biometrische verwerking van persoonsgegevens, met inbegrip van afbeeldingen van gezichten, voor wetshandhavingsdoeleinden die tot grootschalig toezicht in openbare ruimten leidt met behulp van wetgevende en niet-wetgevende middelen en, indien nodig, via inbreukprocedures, over de hele linie te verbieden; verzoekt de Commissie daarnaast te stoppen met het financieren van biometrisch onderzoek en biometrische toepassingen of programma's waarbij een aanzienlijk risico bestaat dat ze bijdragen tot grootschalige surveillance in openbare ruimten; beklemtoont in dit verband dat specifiek moet worden gekeken naar het gebruik van drones door de politie, en dat hiervoor een strikt kader moet worden ontwikkeld;

32. steunt de aanbevelingen van de deskundigengroep op hoog niveau inzake AI van de Commissie om de grootschalige toekenning van scores aan personen op basis van AI te verbieden; is van oordeel dat elke vorm van het op grote schaal toekennen van normatieve scores aan burgers door overheidsinstanties, met name door politieke of gerechtelijke instanties, tot verlies van autonomie leidt, een gevaar voor het non-discriminatiebeginsel vormt, en niet als in overeenstemming met de grondrechten, in het bijzonder de menselijke waardigheid, als vastgelegd in het EU-recht, kan worden beschouwd;

33. roept op tot meer algemene transparantie om tot een compleet inzicht in het gebruik van AI-toepassingen in de Unie te komen; verzoekt de lidstaten een volledig overzicht te geven van de door politieke of gerechtelijke instanties gebruikte instrumenten, de soorten gebruikte instrumenten, de doeleinden waarvoor ze worden gebruikt, de strafbare feiten waarvoor ze worden ingezet, en de namen van de ondernemingen of organisaties die deze instrumenten hebben ontwikkeld; dringt er bij politieke en gerechtelijke instanties op aan om ook het publiek te informeren en voor voldoende transparantie te zorgen over het gebruik dat zij maken van AI en aanverwante technologieën bij het uitoefenen van hun bevoegdheden, waaronder openbaarmaking van de percentages valse positieven en valse negatieven van de gebruikte technologie; verzoekt de Commissie de informatie op één plaats bijeen te brengen en regelmatig te actualiseren; verzoekt de Commissie verder informatie te publiceren over het gebruik van AI door Unie-agentschappen die met politieke- en justitiële taken belast zijn, en deze informatie regelmatig te actualiseren; verzoekt het EDPB de rechtmatigheid van deze door politieke of gerechtelijke instanties gebruikte AI-technologieën en -toepassingen te beoordelen;

34. herinnert eraan dat de ontwikkeling van AI-toepassingen, waaronder toepassingen die door politieke of gerechtelijke instanties worden gebruikt, wereldwijd zeer snel gaat; verzoekt alle Europese belanghebbende partijen, waaronder de lidstaten en de Commissie, met klem er middels internationale samenwerking aan te werken dat partners buiten de EU participeren in het aanscherpen van de normen op internationaal niveau, alsook in het vaststellen van een gemeenschappelijk en complementair wettelijk en ethisch kader voor het gebruik van AI, met name door politieke of gerechtelijke instanties, dat het Handvest, het Europees gegevensbeschermingsacquis en de mensenrechten meer in het algemeen volledig respecteert;

⁽⁸⁾ Besluit 2008/615/JBZ van de Raad van 23 juni 2008 inzake de intensivering van de grensoverschrijdende samenwerking, in het bijzonder ter bestrijding van terrorisme en grensoverschrijdende criminaliteit (PB L 210 van 6.8.2008, blz. 1).

Woensdag, 6 oktober 2021

35. verzoekt het Bureau voor de grondrechten van de EU om, in samenwerking met het EDPB en de EDPS, alomvattende richtsnoeren, aanbevelingen en goede praktijken te ontwerpen voor het nader specificeren van de criteria en condities voor de ontwikkeling, het gebruik en de invoering van AI-toepassingen en -oplossingen voor gebruik door politieke of gerechtelijke instanties; zegt toe een studie te zullen verrichten naar de tenuitvoerlegging van de richtlijn wetshandhaving⁽⁹⁾, teneinde in kaart te brengen hoe er bij de verwerkingsactiviteiten van politieke of gerechtelijke instanties, en met name bij de ontwikkeling en invoering van nieuwe technologieën, voor wordt gezorgd dat de gegevensbeschermingsregels worden gerespecteerd; verzoekt de Commissie daarnaast te onderzoeken of er behoefte bestaat aan specifieke wetgeving voor het nader specificeren van de criteria en condities voor de ontwikkeling, het gebruik en de invoering van AI-toepassingen en -oplossingen voor gebruik door politieke of gerechtelijke instanties;
36. verzoekt zijn Voorzitter deze resolutie te doen toekomen aan de Raad en de Commissie.
-

⁽⁹⁾ Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad (PB L 119 van 4.5.2016, blz. 89).