



GEWONE ZITTING 2023-2024

26 FEBRUARI 2024

**BRUSSELS
HOOFDSTEDELIJK PARLEMENT****VOORSTEL VAN RESOLUTIE**

houdende een verbod op de aanschaf en het gebruik van gezichtsherkenningsoftware op vaste en mobiele bewakingscamera's in het Brussels Hoofdstedelijk Gewest

(ingediend door de heer Hicham TALHI (FR))

Toelichting*Context*

Op initiatief van verschillende verenigingen, zoals de Ligue des droits humains, de Liga voor Mensenrechten, Genres Pluriels, Ciré, Mémoire coloniale et lutte contre les discriminations, Tactic vzw en Technopolice.be, werd onlangs een petitie voor een verbod op het gebruik van gezichtsherkenning ingediend bij het Brussels Parlement. De petitie maakt deel uit van een bewustmakingscampagne die in 2023 werd gevoerd onder de naam #ProtectMyFace, met als doel mensen te informeren over en te waarschuwen voor de gevolgen en gevaren van het gebruik van dergelijke software voor onze samenleving.

Veel burgers zijn ook verontwaardigd over het gebruik van deze software in België. Dit geldt des te meer in een tijd waarin artificiële intelligentie een steeds belangrijker onderdeel van ons dagelijkse leven wordt.

Op dit moment is het gebruik van gezichtsherkenningstechnologie in België niet vastgelegd in enig regelgevend of juridisch kader. Desondanks werd gezichtsherkenning al meermaals gebruikt tijdens onderzoeken door de Belgische federale politie via de gezichtsherkenningsoftware *Clearview AI*, onder andere op de luchthaven van Zaventem in 2017 en 2019, en tijdens Europol-vergaderingen in 2019 en 2020.

SESSION ORDINAIRE 2023-2024

26 FÉVRIER 2024

**PARLEMENT DE LA RÉGION
DE BRUXELLES-CAPITALE****PROPOSITION DE RÉOLUTION**

visant l'interdiction de l'achat et de l'usage de logiciels de reconnaissance faciale sur les caméras de surveillance, fixes et mobiles, en Région de Bruxelles-Capitale

(déposée par M. Hicham TALHI (FR))

Développements*Contexte*

À l'initiative de plusieurs associations telles que la Ligue des droits humains, la *Liga voor Mensenrechten*, Genres Pluriels, Ciré, Mémoire coloniale et lutte contre les discriminations, Tactic ASBL et Technopolice.be, une pétition ayant pour objectif l'interdiction de l'usage de la reconnaissance faciale a récemment été déposée au Parlement bruxellois. Celle-ci s'inscrit dans le cadre d'une campagne de sensibilisation menée en 2023, appelée #ProtectMyFace, visant à informer et alerter des conséquences et des dangers de l'utilisation de tels logiciels pour notre société.

Par ailleurs, de nombreux citoyens et citoyennes s'indignent face à l'utilisation de ces logiciels en Belgique. Cela est d'autant plus vrai dans un contexte où l'intelligence artificielle prend chaque jour davantage d'ampleur dans notre quotidien.

À l'heure actuelle, l'usage des technologies relatives à la reconnaissance faciale en Belgique n'est encadré par aucun cadre réglementaire ou juridique. Malgré cela, la reconnaissance faciale a été utilisée, via le logiciel de reconnaissance faciale *Clearview AI*, à de nombreuses reprises lors d'enquêtes par la police fédérale belge, notamment à l'aéroport de Zaventem, en 2017 et en 2019, ainsi que dans le cadre des réunions Europol en 2019 et 2020.

Aangezien deze experimenten illegaal werden uitgevoerd, werden ze beëindigd na een advies van het Controleorgaan op de Politie-informatie.

De controverse rond laatstgenoemde zaak kwam niet alleen voort uit het feit dat deze politie-testen volledig verborgen en illegaal werden uitgevoerd, maar ook uit het feit dat *Clearview AI* een uiterst controversieel bedrijf is. Zijn algoritmen worden gevoed met behulp van miljarden foto's van aangezichten die zonder toestemming van de betrokkenen van websites en sociale netwerken worden gehaald. Tot slot blijkt uit een onderzoek van de KU Leuven uit 2021 dat in het Brussels en Vlaams Gewest "minstens 5 politiezones over gezichtsherkenningssystemen beschikten, waarvan er een zone zelfs beweerde deze vaak tot zeer vaak te gebruiken".^[1]

In een advies van 16 juni 2020 betreffende een voorstel van resolutie over een driejarig moratorium op het gebruik van gezichtsherkenningssystemen en – algoritmen in vaste of mobiele beveiligingscamera's op openbare en private plekken legde het Controleorgaan over de politie-informatie heel duidelijk uit dat er geen gebruik mag worden gemaakt van gezichtsherkenning door politiediensten of magistraten: "Voor wat politie-gegevensverwerkingen betreft en dus voor handhavingdoeleinden (of meer algemeen doeleinden van bestuurlijke en gerechtelijke politie of voor zgn. *law enforcement*-doeleinden) is het voorstel van resolutie evenwel juridisch gezien in zekere zin overbodig vermits het huidige wettelijk kader sowieso geen (afdoende) rechtsgrond biedt voor de geïntegreerde politie (hierna 'GPI') - en dus ook voor parket en onderzoeksrechter - om dergelijke gezichtsherkenningstechnologie in te zetten. Inderdaad, noch de Wet op het Politieambt, noch het Wetboek van Strafvordering of enig andere bijzondere (straf)wet biedt de lege lata een (afdoende) rechtsgrond voor de inzet van FRT voor opdrachten van bestuurlijke of gerechtelijke politie."

Definities

De bovengenoemde verenigingen definiëren gezichtsherkenning als volgt:

"Gezichtsherkenning is een van de biometrische technologieën waarmee mensen kunnen worden geïdentificeerd op basis van de analyse van unieke kenmerken van hun aangezicht (oogafstand, neusbrug, mondhoeken enz.). Door de verwerking van beelden van menselijke gezichten, identificeren of bevestigen de algoritmen van gezichtsherkenningssystemen de identiteit van personen die op een plaats of in een groep aanwezig zijn op basis van de raadpleging van een databank."^[2]

[1] <https://www.gegevensbeschermingsautoriteit.be/professioneel/thema-s/recht-op-afbeelding/gezichts-herkenning-en-recht-op-afbeelding>

[2] *Petitie tegen het gebruik van gezichtsherkenning in het Brussels Hoofdstedelijk Gewest*, blz. ¼.

Ces expérimentations ayant été réalisées illégalement, elles ont pris fin après un avis de l'Organe de contrôle de l'information policière.

La polémique que suscita cette dernière affaire tenait à la fois au fait que ces essais par la police étaient réalisés en toute opacité et illégalité, mais aussi parce que l'entreprise *Clearview AI* est extrêmement controversée. En effet, ses algorithmes sont entraînés grâce à des milliards de photos de visages récupérés sans le consentement des personnes sur des sites internet et sur des réseaux sociaux. Enfin, il est primordial de noter qu'une recherche de la KU Leuven menée en 2021 en Région bruxelloise et flamande a affirmé «qu'au moins 5 zones de police disposaient de la reconnaissance faciale, l'une d'elle affirmant même l'utiliser souvent à très souvent».^[1]

Dans un avis du 16 juin 2020 relatif à la proposition de résolution pour la mise en place d'un moratoire de trois ans sur l'utilisation de logiciels et d'algorithmes de reconnaissance faciale sur les caméras de sécurité, fixes ou mobiles, dans les endroits publics et privés, l'Organe de contrôle de l'information policière expliquait très clairement qu'aucun usage de la reconnaissance faciale ne pouvait être fait par les services de police ou les magistrats: «En ce qui concerne par contre les traitements policiers et donc les finalités de maintien de l'ordre ou répressives (ou, plus généralement, les finalités de police administrative et judiciaire ou de *law enforcement*), la proposition de résolution est d'une certaine manière superflue d'un point de vue juridique étant donné que le cadre légal actuel n'offre de toute manière aucun fondement juridique (suffisant) permettant à la police intégrée (ci-après 'la GPI') – et donc également au parquet et au juge d'instruction – de recourir à une telle technologie de reconnaissance faciale. De fait, ni la loi sur la fonction de police, ni le Code d'instruction criminelle ni une quelconque autre loi (pénale) spéciale n'offre *de lege lata* un fondement juridique (suffisant) pour l'utilisation de la FRT dans le cadre de missions de police administrative ou judiciaire.».

Définitions

Les associations précitées définissent la reconnaissance faciale comme suit:

«La reconnaissance faciale est l'une des technologies biométriques qui permet l'identification des personnes sur la base de l'analyse de caractéristiques propres et uniques des traits de leurs visages (écartement des yeux, arêtes du nez, commissures des lèvres, etc...). Par le traitement d'images de visages humains, les algorithmes des systèmes de reconnaissance faciale identifient ou confirment l'identité de personnes présentes au sein d'un lieu, d'un groupe sur la base de la consultation d'une base de données.».^[2]

[1] <https://www.autoriteprotectiondonnees.be/professionnel/themes/le-droit-a-l-image/reconnaissance-faciale-et-droit-a-l-image>

[2] *Pétition contre l'usage de la reconnaissance faciale en Région de Bruxelles-Capitale*, p.1/4.

De Gegevensbeschermingsautoriteit specificeert de twee hoofddoelen van gezichtsherkenning: authenticatie en identificatie.

Het eerste bestaat erin "een persoon te authenticeren: dat wil zeggen, verifiëren of een persoon is wie hij of zij beweert te zijn (in het kader van de toegangscontrole). Het systeem vergelijkt of de identiteit die als gevolg van de identificatie wordt verkregen, overeenkomt met de identiteit die eerder in de bestanden is opgeslagen."

Het tweede is "een persoon te identificeren: dat wil zeggen, om een persoon te vinden binnen een groep van individuen, een plaats, een afbeelding of een database. Het systeem analyseert of het voorgelegde aangezicht overeenkomt met de modellen die zijn geregistreerd in de database op basis van "gelijksoortigheidscriteria". Een voorbeeld van een biometrisch identificatiesysteem is het gezichtsherkenningssysteem van Interpol."^[3]

Een schending van de mensenrechten en fundamentele vrijheden

Gezichtsherkenning zou dus een gebruikelijke manier kunnen worden om burgers te identificeren. Zo vormt het een instrument voor massasurveillance, dat de fundamentele vrijheden van eenieder kan belemmeren. Aangezien elke burger die zich in de openbare ruimte bevindt op elk moment kan worden geïdentificeerd en mogelijk kan worden verdacht, roept het regelen van deze technologie voor de hand liggende juridische en ethische bezwaren op.

Deze voortdurende identificatie belemmert ieders recht op privacy en individuele vrijheid. In de context van bijeenkomsten bijvoorbeeld, zou het uiten van bepaalde politieke meningen onmiddellijk aan banden kunnen worden gelegd. Dit is een rechtstreekse belemmering van de vrijheid van meningsuiting van burgers. In 2021 is Amnesty International een bewustmakings- en informatiecampagne gestart, waarin deze belemmeringen van eenieders grondrechten aan de kaak worden gesteld.

Bovendien zou dit gebruik sociale minderheidsgroepen, zoals mensen met een immigratieachtergrond, de LGBTQIA+-gemeenschap, migranten en daklozen nog meer stigmatiseren. Deze sociale minderheidsgroepen, die al onderhevig zijn aan discriminatie en stereotypering, zouden vaker kunnen worden verdacht.

Uit een onderzoek van MIT Media Lab bleek dat vanaf 2018 de software meer fouten maakt bij niet-blanke personen en dan vooral bij vrouwen. Dit kan met name worden verklaard door het bevooroordeelde ontwerp van de algoritmen en door hun invoergegevens, die voornamelijk bestaan uit de gezichten van blanke mannen. Naast deze algoritmische vooroordelen in de ontwerpfase, verklaart een

[3] <https://www.gegevensbeschermingsautoriteit.be/professioneel/thema-s/recht-op-afbeelding/gezichts-herkenning-en-recht-op-afbeelding>

L'Autorité de protection de données précise les deux missions principales de la reconnaissance faciale: l'authentification et l'identification.

La première étant «d'authentifier une personne: c'est-à-dire, vérifier qu'une personne est bien celle qu'elle prétend être (dans le cadre d'un contrôle d'accès). Le système compare si l'identité obtenue suite à l'identification correspond avec celle préalablement enregistrée dans les fichiers.»

La seconde étant «d'identifier une personne: c'est-à-dire, de retrouver une personne au sein d'un groupe d'individus, dans un lieu, une image ou une base de données. Le système analyse si le visage présenté correspond aux modèles enregistrés dans sa base de données sur la base de critères de «similarité». Le système de reconnaissance faciale d'INTERPOL est un exemple de système d'identification biométrique.»^[3]

Une atteinte aux droits humains et libertés fondamentales

L'usage de la reconnaissance faciale pourrait donc devenir un dispositif usuel d'identification des citoyens. Ce faisant, il représente un outil de surveillance de masse pouvant entraver les libertés fondamentales de chacun et chacune. Chaque citoyen et citoyenne se trouvant dans l'espace public pouvant être identifiable et potentiellement suspecté en permanence, la réglementation de cette technologie suscite des difficultés juridiques et éthiques évidentes.

Cette identification constante entrave le droit à la vie privée et à la liberté individuelle de toutes et tous. Comme par exemple dans le cadre de rassemblements, la manifestation de certaines opinions politiques serait vouée à être limitée instantanément. Il s'agit là d'une entrave directe à la liberté d'expression des citoyens et citoyennes. À ce sujet, en 2021, Amnesty international a mis en place une campagne de sensibilisation et d'information dénonçant ces entraves aux droits fondamentaux de toutes et tous.

De plus, cette utilisation stigmatiserait davantage des groupes sociaux minoritaires comme les personnes issues de l'immigration, de la communauté LGBTQIA+, des personnes migrantes, sans abri. Ces groupes sociaux minoritaires, subissant déjà des discriminations et stéréotypes, pourraient davantage être suspectés.

Comme le démontrait une recherche du MIT Media Lab dès 2018, les logiciels font plus d'erreurs pour les personnes non blanches et particulièrement les femmes. Cela s'explique notamment par la conception biaisée des algorithmes et par leurs données d'entraînement qui sont majoritairement composées de visages d'hommes blancs. Outre ces biais algorithmiques dès la conception, plusieurs

[3] <https://www.autoriteprotectiondonnees.be/professionnel/themes/le-droit-a-l-image/reconnaissance-faciale-et-droit-a-l-image>

aantal organisaties en komt er ook uit onderzoeksprojecten voort dat gezichtsherkenning rassendiscriminatie versterkt door historisch gecriminaliseerde groepen in politiedatabases te oververtegenwoordigen.

De doeltreffendheid van deze software in het bestrijden van criminaliteit blijkt gering te zijn. Uit een onderzoek dat in 2019 werd uitgevoerd door de universiteit van Essex in Groot-Brittannië blijkt dat 80% van de geïdentificeerde personen onschuldig was. Gezichtsherkenning werd daar al gedurende drie opeenvolgende jaren gebruikt.^[4]

Bijgevolg is gezichtsherkenning, door de manier waarop de databases waar zij op gebaseerd is ontworpen zijn, bevooroordeeld en ondoeltreffend.

Daarom is het natuurlijk van essentieel belang om een regelgevend en juridisch kader op te stellen specifiek voor gezichtsherkenningssystemen. Vanuit dat oogpunt dient er ook een principieel verbod op te komen.

Tot slot, dienen we hier nog aan toe te voegen dat deze gegevensopslag extreme beveiliging en voorzorgsmaatregelen vereist, maar dat geen enkel beveiligingssysteem onfeilbaar is. De risico's om gehackt te worden zijn zeer groot voor gegevens die door de Gegevensbeschermingsautoriteit als "bijzonder gevoelig" worden beschouwd. Het hacken van deze gegevens kan bijzonder ernstige en onherroepelijke gevolgen met zich meebrengen. Met andere woorden, het is gemakkelijk om een wachtwoord te wijzigen, maar niet een gezicht.

Zo onthulde de pers in november 2022 dat een hacker via een inbraak in het systeem van de lokale politiezone van Zwijndrecht (provincie Antwerpen) politiegegevens had kunnen stelen die dateerden van 2006 tot 2022, waaronder processen-verbaal en nummerplaten, maar ook foto's van personen.

organisations et recherches expliquent que la reconnaissance faciale entraîne un renforcement des discriminations raciales du fait d'une surreprésentation, dans les bases de données policières, des groupes de personnes historiquement criminalisées.

L'efficacité de ces logiciels s'avère minime dans la lutte contre la criminalité. Une étude réalisée en 2019 par l'Université d'Essex, en Grande-Bretagne, démontre que 80 % des personnes identifiées étaient innocentes. La reconnaissance faciale y était utilisée depuis trois années consécutives.^[4]

Par conséquent, la reconnaissance faciale, du fait même de la manière dont sont conçues les bases de données sur lesquelles elles s'appuient, s'avère biaisée et inefficace.

C'est pourquoi il est bien sûr primordial d'instaurer un cadre réglementaire et juridique portant spécifiquement sur les dispositifs de reconnaissance faciale. Et dans cette optique, d'établir une interdiction de principe à leur égard.

Enfin, ajoutons également que ce stockage de données requiert une sécurité et une précaution extrême, mais qu'aucun système de protection n'est infaillible. Les risques de piratage informatique sont très élevés pour ces données qui sont considérées comme «particulièrement sensibles» par l'Autorité de protection des données. En effet, le piratage de ces données peut avoir des effets particulièrement graves et irrémédiables. Autrement dit, on peut aisément changer un mot de passe, mais pas son visage.

À titre d'exemple, la presse révélait en novembre 2022 qu'une intrusion dans le système de la zone de police locale de Zwijndrecht (province d'Anvers) avait permis au pirate de voler des données policières datant de 2006 à 2022, dont des procès-verbaux et des plaques d'immatriculation, mais aussi des photos de personnes.

Hicham TALHI (FR)

[4] <https://www.independent.co.uk/news/uk/home-news/met-police-facial-recognition-success-south-wales-trial-home-office-false-positive-a8345036.html>

[4] <https://www.independent.co.uk/news/uk/home-news/met-police-facial-recognition-success-south-wales-trial-home-office-false-positive-a8345036.html>

VOORSTEL VAN RESOLUTIE

houdende een verbod op de aanschaf en het gebruik van gezichtsherkenningsoftware op vaste en mobiele bewakingscamera's in het Brussels Hoofdstedelijk Gewest

Het Brussels Hoofdstedelijk Parlement,

Gelet op de bevoegdheden van het Brussels Hoofdstedelijk Gewest inzake veiligheid en preventie;

Gelet op de taken van safe.brussels op het gebied van veiligheid en preventie;

Gelet op de Universele Verklaring van de Rechten van de Mens, die op 10 september 1948 werd aangenomen door de Algemene Vergadering van de Verenigde Naties;

Gelet op het Internationaal Verdrag inzake burgerrechten en politieke rechten, waaronder het recht op non-discriminatie, het recht op gelijkheid van mannen en vrouwen, het recht op vrij verkeer, het recht op privacy, het recht op vrijheid van meningsuiting, het recht op vrijheid van vereniging en het recht van minderheden;

Gelet op artikel 7 van het Handvest van de grondrechten van de Europese Unie betreffende de eerbiediging van het privéleven en van het familie- en gezinsleven: "Eenieder heeft recht op eerbiediging van zijn privéleven, zijn familie- en gezinsleven, zijn woning en zijn communicatie.";

Gelet op artikel 11 van de Belgische Grondwet, dat het volgende bepaalt: "Het genot van de rechten en vrijheden aan de Belgen toegekend moet zonder discriminatie verzekerd worden. Te dien einde waarborgen de wet en het decreet inzonderheid de rechten en vrijheden van de ideologische en filosofische minderheden.";

Gelet op artikel 12 inzake het recht op persoonlijke vrijheid in de Belgische Grondwet: "De vrijheid van de persoon is gewaarborgd.";

Gelet op artikel 22 van de Belgische Grondwet over het recht op privacy: "Ieder heeft recht op eerbiediging van zijn privéleven en zijn gezinsleven, behoudens in de gevallen en onder de voorwaarden door de wet bepaald.";

Gelet op artikel 27 van de Belgische Grondwet: "De Belgen hebben het recht van vereniging; dit recht kan niet aan enige preventieve maatregel worden onderworpen.";

Gelet op de wet van 30 juli 1981 tot bestraffing van bepaalde door racisme of xenofobie ingegeven daden en de wet van 10 mei 2007 ter bestrijding van bepaalde vormen van discriminatie;

Gelet op het feit dat, volgens algemene beleidsaanbeveling nr. 11 die de Commissaris voor de Mensenrechten van de Raad van Europa aan België heeft gedaan na zijn bezoek aan België in september 2015, het gebruik door de politie van gronden zoals ras, huidskleur,

PROPOSITION DE RÉSOLUTION

visant l'interdiction de l'achat et de l'usage de logiciels de reconnaissance faciale sur les caméras de surveillance, fixes et mobiles, en Région de Bruxelles-Capitale

Le Parlement de la Région de Bruxelles-Capitale,

Vu les compétences de la Région de Bruxelles-Capitale en matière de sécurité et de prévention;

Vu les missions de safe.brussels relatives à la sécurité et la prévention;

Vu la Déclaration universelle des droits humains, adoptée par l'Assemblée générale des Nations unies, le 10 septembre 1948;

Vu le Pacte international relatif aux droits civils et politiques dont le droit à la non-discrimination, le droit à l'égalité entre les hommes et les femmes, le droit de circuler librement, le droit à la vie privée, le droit à la liberté d'expression, le droit à la liberté d'association, le droit des minorités;

Vu l'article 7 de la Charte des droits fondamentaux de l'Union européenne concernant le respect de la vie privée et familiale: «Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de ses communications.»;

Vu l'article 11 de la Constitution belge qui dispose que «La jouissance des droits et libertés reconnus aux Belges doit être assurée sans discrimination. À cette fin, la loi et le décret garantissent notamment les droits et libertés des minorités idéologiques et philosophiques.»;

Vu l'article 12 relatif au droit à la liberté individuelle figurant dans la Constitution belge, «La liberté individuelle est garantie.»;

Vu l'article 22 de la Constitution belge relatif au droit à la vie privée, «Chacun a droit au respect de sa vie privée et familiale, sauf dans les cas et conditions fixés par la loi.»;

Vu l'article 27 figurant dans la Constitution belge, «Les Belges ont le droit de s'associer; ce droit ne peut être soumis à aucune mesure préventive.»;

Vu la loi du 30 juillet 1981 tendant à réprimer certains actes inspirés par le racisme et la xénophobie et la loi du 10 mai 2007 tendant à lutter contre certaines formes de discrimination;

Vu que, selon la recommandation de politique générale n° 11 faite à la Belgique par le Commissaire aux Droits de l'Homme du Conseil de l'Europe suite à sa visite en Belgique en septembre 2015, l'utilisation par la police de motifs comme la race, la couleur, la langue, la religion, la

taal, godsdienst, nationaliteit of nationale of etnische afkomst bij observatie-, controle- of onderzoeksactiviteiten bijna nooit kan worden gerechtvaardigd, buiten het geval waarin de politie optreedt op basis van een beschrijving van een verdachte met in de tijd beperkte gevolgen;

Gelet op de goedkeuring door het Europees Parlement van zijn onderhandelingspositie inzake artificiële intelligentie op 14 juni 2023, die een "volledig verbod op artificiële intelligentie (AI) voor biometrische surveillance, emotieherkenning en voorspellend politiewerk" bevat;

Overwegende de algemene onzekerheden in verband met de voorwaarden voor opslag, overdracht en classificatie van gegevens en het gebrek aan onafhankelijke democratische controle daarover;

Overwegende de risico's op targeting en discriminatie van bepaalde categorieën van de bevolking die rechtstreeks of onrechtstreeks worden gevisieerd door de verwerking van de verzamelde gegevens;

Overwegende de petitie "tegen het gebruik van gezichtsherkenning in het Brussels Hoofdstedelijk Gewest", ingediend door Ciré, Genres Pluriels, de Liga voor Mensenrechten, de Ligue des droits humains, Mémoire coloniale et lutte contre les discriminations, Tactic vzw en Technopolice.be;

Overwegende de informatie- en bewustmakingscampagne #Protectmyface, die de coalitie van deze acht Brusselse verenigingen heeft gevoerd;

Overwegende de hoorzittingen van de coalitie #Protectmyface op 13 juni 2023 in de commissie voor de Binnenlandse Zaken van het Brussels Parlement;

Overwegende de bewustmakingscampagne "Ban The Scan" van Amnesty International in 2021 en haar wens om verder te gaan in de verboden die zijn opgenomen in de Europese wetgeving die op 14 juni 2023 werd aangenomen;

Overwegende het ontbreken van een Belgisch wetgevend en juridisch kader voor het gebruik van gezichtsherkenning;

Overwegende dat elke vorm van etnische profilering onwettig is volgens het internationaal recht, omdat het in strijd is met de waarborgen die zijn vastgelegd in het Internationaal Verdrag inzake de uitbanning van alle vormen van rassendiscriminatie, dat bindend is voor alle lidstaten van de Europese Unie;

Overwegende de ethische uitdagingen in verband met technologische vooruitgang zoals gezichtsherkenning, in termen van individuele vrijheden;

nationalité ou l'origine nationale ou ethnique dans des activités de surveillance, de contrôle ou d'investigation ne peut quasiment jamais se justifier en dehors du cas où la police intervient sur la base d'une description d'un suspect avec des effets limités dans le temps;

Vu l'adoption le 14 juin 2023, par le Parlement européen, de sa position de négociation sur l'intelligence artificielle stipulant: «Le recours à l'intelligence artificielle (IA) est interdit pour la surveillance biométrique, la reconnaissance des émotions et la police prédictive»;

Considérant les incertitudes générales liées aux conditions de conservation, de transmission et de classement des données, ainsi que le manque de contrôle démocratique indépendant vis-à-vis de celles-ci;

Considérant les risques de ciblage et de discrimination de catégories particulières de la population directement ou indirectement ciblées par le traitement des données recueillies;

Considérant la pétition «contre l'usage de la reconnaissance faciale en Région de Bruxelles-Capitale» déposée par Ciré, Genres Pluriels, la Liga voor Mensenrechten, la Ligue des droits humains, Mémoire coloniale et lutte contre les discriminations, Tactic ASBL et Technopolice.be;

Considérant la campagne d'information et de sensibilisation #Protectmyface menée par la coalition de ces huit associations bruxelloises;

Considérant les auditions de la coalition #Protectmyface le 13 juin 2023 en commission des Affaires intérieures du Parlement bruxellois;

Considérant la campagne de sensibilisation menée en 2021 par Amnesty International, «Ban The Scan», ainsi que leur volonté d'aller plus loin dans les interdictions prévues par la législation européenne, adoptée en date du 14 juin 2023;

Considérant l'absence de cadre juridique et réglementaire belge au sujet de l'utilisation de la reconnaissance faciale;

Considérant que toute forme de profilage ethnique est illégale au regard du droit international en ce qu'elle contrevient aux garanties établies par la Convention internationale sur l'élimination de toute forme de discrimination raciale qui lie tous les États membres de l'Union européenne;

Considérant les enjeux éthiques propres aux avancées technologiques telles que la reconnaissance faciale en termes de libertés individuelles;

Overwegende de oprichting van het Strategisch Comité I, ook bekend als het "Comité Informatie en ICT", dat tot doel heeft beleidsadvies te verstrekken voor het beheer en de bescherming van politionele informatie teneinde de ministers van Binnenlandse Zaken en Justitie bij te staan;

Verzoekt de Brusselse Hoofdstedelijke Regering, in samenwerking met de federale regering:

- de invoering en het gebruik van gezichtsherkenningstechnologieën binnen het kader van haar bevoegdheden, te verbieden op vaste en mobiele camera's die opgesteld zijn in de openbare ruimte binnen het Brussels Hoofdstedelijk Gewest;
- ervoor te zorgen dat, binnen het kader van haar bevoegdheden, geen overheidsmiddelen worden toegewezen aan particuliere of openbare instanties voor de ontwikkeling, de aankoop en het gebruik van gezichtsherkenningstechnologieën;
- te zorgen voor de invoering van een onafhankelijke controle van het platform voor het delen van videobewakingsbeelden en te verifiëren dat geen enkele beeldvergelijking met behulp van gezichtsherkenningsoftware wordt uitgevoerd achteraf met beelden die via het platform worden gebruikt;
- de aankoop en het gebruik van gezichtsherkenning in de zes Brusselse politiezones te verbieden.

Verzoekt de federale regering:

- een openbaar verslag voor te leggen aan het maatschappelijke middenveld over de lopende werkzaamheden van de "ethische adviescommissie veiligheid opgericht om "het ethisch en doeltreffend gebruik van technologieën en onderzoeks- en interventiemethoden" te evalueren";

Verzoekt federale overheid:

- een juridisch kader uit te werken dat het gebruik van gezichtsherkenninginstrumenten principieel verbiedt.

Considérant la mise en place du Comité stratégique I, autrement appelé «Comité Information et ICT» ayant pour objectif de fournir des avis en termes de politique de gestion et de protection de l'information policière afin d'assister les ministres de l'Intérieur et de la Justice;

Demande au Gouvernement de la Région de Bruxelles-Capitale, en concertation avec le Gouvernement fédéral:

- d'interdire, dans le cadre de ses compétences, le déploiement et l'utilisation des technologies de reconnaissance faciale sur les caméras fixes et mobiles mises en place dans l'espace public au sein de la Région de Bruxelles-Capitale;
- de s'assurer, dans le cadre de ses compétences, qu'aucun financement public ne soit alloué à des organismes, tant privés que publics, visant le développement, l'achat et l'usage de technologies relatives à la reconnaissance faciale;
- d'assurer la mise en place d'un contrôle indépendant de la plateforme de mutualisation des images de vidéosurveillance et de vérifier qu'aucune correspondance d'images à l'aide d'un logiciel de reconnaissance faciale n'est effectuée *a posteriori* grâce aux images utilisées via la plateforme de mutualisation;
- d'interdire l'achat et l'usage de la reconnaissance faciale au sein des six zones de polices bruxelloises;

Demande au Gouvernement fédéral:

- d'assurer un rapport public auprès de la société civile sur les travaux en cours au sujet de la «Commission consultative éthique et sécurité chargée d'évaluer l'utilisation éthique et efficace des technologies et des méthodes d'enquête et d'intervention»;

Demande à l'autorité fédérale:

- de déterminer un cadre juridique imposant une interdiction de principe des dispositifs de reconnaissance faciale.

Hicham TALHI (FR)