PARLEMENT BRUXELLOIS
BRUSSELS PARLEMENT

**A-769/1** – 2023/2024

GEWONE ZITTING 2023-2024

2 OKTOBER 2023

# BRUSSELS HOOFDSTEDELIJK PARLEMENT

## VOORSTEL VAN RESOLUTIE

## betreffende het verbod op het gebruik van gezichtsherkenningssoftware en -algoritmen in vaste of mobiele bewakingscamera's in openbare ruimten in het Brussels Hoofdstedelijk Gewest

(ingediend door mevrouw Leïla LAHSSAINI (FR), de heren Petya OBOLENSKY (FR), Francis DAGRIN (FR), Jan BUSSELEN (NL) en mevrouw Françoise DE SMEDT (FR))

### Toelichting

Machines en robots nemen steeds meer taken over, met name door middel van artificiële intelligentie (AI). Een van deze ontwikkelingen is het gebruik van gezichtsherkenningssoftware en -algoritmen in bewakingscamera's.

In België bestaat er geen wetgeving over deze technologie. Nochtans werd die al meermaals ingezet:

– in 2017 en 2019 heeft de federale politie gezichtsherkenning uitgetest op de luchthaven van Zaventem. Volgens de commissaris-generaal van de federale politie Marc De Mesmaeker, was een wetswijziging niet nodig. Het Controleorgaan op de Politionele Informatie heeft na onderzoek echter geconcludeerd dat het project in strijd was met de wet op het politieambt en met de wet betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens: camerabewaking is toegestaan maar gezichtsherkenning niet. Er is bijvoorbeeld geen enkele voorafgaande impactanalyse uitgevoerd, wat nochtans een wettelijke verplichting is. De federale politie heeft

SESSION ORDINAIRE 2023-2024

2 OCTOBRE 2023

# PARLEMENT DE LA RÉGION DE BRUXELLES-CAPITALE

## PROPOSITION DE RÉSOLUTION

## relative à l'interdiction de l'utilisation de logiciels et d'algorithmes de reconnaissance faciale sur les caméras de surveillance, fixes ou mobiles, dans les endroits publics de la Région de Bruxelles-Capitale

(déposée par Mme Leïla LAHSSAINI (FR), MM. Petya OBOLENSKY (FR), Francis DAGRIN (FR), Jan BUSSELEN (NL) et Mme Françoise DE SMEDT (FR))

### Développements

Aujourd'hui, de plus en plus de tâches sont confiées à des machines et des robots, notamment par le biais de l'intelligence artificielle (IA). L'un de ces développements consiste en l'usage de logiciels et d'algorithmes de reconnaissance faciale sur les caméras de surveillance.

En Belgique, aucune loi n'encadre l'usage de cette technologie. Pour autant, celle-ci a été utilisée à diverses reprises:

– en 2017 et 2019, la reconnaissance faciale a été testée par la police fédérale à l'aéroport de Zaventem. Selon le commissaire général de la police fédérale, Marc De Mesmaeker, une modification législative n'était pas nécessaire. Suite à une enquête de l'Organe de contrôle de l'information policière, ce dernier a néanmoins conclu que le projet contrevenait à la loi sur la fonction de police ainsi qu'à celle sur la protection des données: «La surveillance par caméra reste possible, mais la reconnaissance faciale ne l'est pas». L'une des illégalités consiste dans le fait qu'aucune analyse d'impact préalable n'avait été réalisée, alors que celle-ci est obligatoire. La police

evenwel opnieuw herhaald dat zij in de toekomst gezichtsherkenning zou gebruiken[1];

– in 2019 hebben twee speurders van de Belgische federale politie deelgenomen aan een test van Clearview. Deze software herkent na enkele kliks een persoon met behulp van een databank van meer dan 30 miljard foto's die onder andere op sociale media verzameld werden. Volgens het Controleorgaan op de Politionele Informatie[2], zouden er in het kader van deze test 78 illegale onderzoeken uitgevoerd zijn[3];

– volgens een onderzoek van de KU Leuven in 2021 in de politiezones van het Vlaams Gewest en het Brussels Gewest zouden ten minste 5 zones op de 86 die geantwoord hebben over gezichtsherkenning beschikken. Een zone verklaart die technologie zelfs zeer vaak te gebruiken[4].

Het gebruik van gezichtsherkenning stuit op hevige kritiek van burgers en het maatschappelijke middenveld, zowel in België als in het buitenland.

In maart 2023 heeft de campagne #Protect my face[5] van verschillende verenigingen, waaronder de Liga voor Mensenrechten, la Ligue des droits humains, de MRAX en Genre Pluriel, geleid tot de indiening van een petitie in het Brussels Parlement met het verzoek deze technologie te verbieden[6]. De petitie heeft tot op vandaag 1.131 handtekeningen verzameld en uit sterke kritiek op het gebruik door het Brussels Gewest van de BriefCamsoftware waarmee elke bewegend voorwerp gedetecteerd, gevolgd en geëxtraheerd kan worden. Het Israëlische bedrijf dat de software verkoopt, biedt ook gezichtsherkenningstechnologie aan.

Deze mensenrechtenbewegingen herinneren aan de gevaren van deze technologie: het gebruik ervan in onze straten zou leiden tot een grootschalige controle die de overheid de mogelijkheid zou geven de hele bevolking in de openbare ruimte te identificeren. De gevolgen zouden nog groter zijn voor de privacy van mensen in bestaansonzekerheid of minderheden. De veiligheid van de gegevens (hacking) kan in het gedrang komen en er bestaan risico's op discriminatie en afglijden naar een maatschappij met massacontrole.

1. https://www.lavenir.net/regions/bruxelles/2019/09/20/la-police-federale-doit-mettre-un-terme-a-son-projet-de-reconnaissance-faciale-a-zaventem-JVOSXZSRDNA45NUXTSGNINSV4U/.
2. https://www.controleorgaan.be/files/DIO21006_Toezichtrapport_Clearview_N_00050443.pdf.
3. https://www.rtbf.be/article/investigation-clearview-ai-quand-la-reconnaissance-faciale-porte-atteinte-a-la-vie-privee-11212380.
4. https://www.researchgate.net/publication/355585410_Digitalisering_in_de_lokale_politie_in_Vlaanderen_en_Brussel_Waar_staan_we.
5. https://www.protectmyface.be/.
6. https://democratie.brussels/initiatives/i-155.

fédérale a néanmoins réitéré son intention d'utiliser la reconnaissance faciale à l'avenir[1];

– en 2019, deux enquêteurs de la police judiciaire fédérale belge ont été impliqués dans un test du logiciel *Clearview*. Ce logiciel est capable, en seulement quelques clics, de reconnaître une personne sur la base d'une banque de données de plus de 30 milliards de photos notamment obtenues illégalement sur les réseaux sociaux. Selon l'Organe de contrôle de l'information policière[2], 78 recherches illégales auraient été menées dans le cadre de ce test[3];

– selon une recherche réalisée en 2021 par la KULeuven auprès des zones de police des régions flamande et bruxelloise, au moins 5 zones sur les 86 ayant répondu disposaient de la reconnaissance faciale, l'une d'elle affirmant même l'utiliser souvent à très souvent[4].

L'utilisation de la reconnaissance faciale est fortement décriée par les citoyens ainsi que par la société civile, tant en Belgique qu'à l'étranger.

En mars 2023, la campagne «#Protect my face»[5], lancée par plusieurs associations, dont la Ligue des droits humains, la *Liga voor mensenrechten*, le MRAX, et Genre Pluriel, a abouti au dépôt d'une pétition au Parlement bruxellois demandant l'interdiction de cette technologie[6]. La pétition, qui rassemble à ce jour 1.131 signatures, dénonce notamment l'utilisation par la Région bruxelloise du logiciel *BriefCam* qui permet de détecter, suivre et extraire tout objet en mouvement, fourni par une entreprise israélienne qui propose également des technologies de reconnaissance faciale.

Ces associations de défense des droits fondamentaux rappellent les dangers posés par cette technologie: son usage dans nos rues engendrerait une surveillance généralisée, donnant aux autorités le pouvoir d'identifier l'intégralité de la population dans l'espace public, avec un impact plus important sur la vie privée de personnes précarisées ou de minorités. À cela s'ajoutent les risques liés à la sécurité des données (piratages), les risques de discrimination et les risques de glissement vers une société de surveillance de masse.

1. https://www.lavenir.net/regions/bruxelles/2019/09/20/la-police-federale-doit-mettre-un-terme-a-son-projet-de-reconnaissance-faciale-a-zaventem-JVOSXZSRDNA45NUXTSGNINSV4U/.
2. https://www.organedecontrole.be/files/DIO21006_Rapport_Contr%C3%B4le_Clearview_F_00050441.pdf.
3. https://www.rtbf.be/article/investigation-clearview-ai-quand-la-reconnaissance-faciale-porte-atteinte-a-la-vie-privee-11212380
4. https://www.researchgate.net/publication/355585410_Digitalisering_in_de_lokale_politie_in_Vlaanderen_en_Brussel_Waar_staan_we
5. https://www.protectmyface.be/
6. https://democratie.brussels/initiatives/i-155

Deze verenigingen onderstrepen dat de technologie de grondrechten en de vrijheden van burgers sterk aantast, met name het recht op privacy, betogen en vrije meningsuiting. Zij waarschuwen ervoor dat minderheden bijzonder kwetsbaar worden door de uitrol van deze technologie die geracialiseerde personen en migranten discrimineert. Een van de gevaren van gezichtsherkenning is dat personen uit seksuele minderheden gedetecteerd en geïdentificeerd kunnen worden, bijvoorbeeld door camera's in de buurt van plaatsen van bijeenkomsten.

Ook elders in Europa en wereldwijd wijzen diverse instellingen op de talrijke gevaren van de schending van de grondrechten. Verschillende steden hebben het gebruik van gezichtsherkenning verboden.

In juli 2021 heeft de Franse Défenseur des droits een rapport over biometrie gepubliceerd en gewaarschuwd voor het ongeziene potentieel van uitgebreide en geautomatiseerde discriminatie door het gebruik van dit soort technologie. De Défenseur des droits wijst op het gevaar van vergissingen en onderstreept dat in het geval van gezichtsherkenning de gevolgen van dergelijke vergissingen kunnen gaan van het ontzeggen van de toegang tot een bepaalde plaats tot een onterechte aanhouding door de politie. Zij vreest dat deze technologie discriminatie zal verergeren, zelfs als de technologie 100% betrouwbaar zou zijn. De technologie zou uitgerold kunnen worden in buurten en gebieden waar de bevolking al meer dan elders identiteitscontroles moet ondergaan, bijvoorbeeld op plaatsen waar jonge mannen als behorend tot een minderheid gepercipieerd worden. De vrees om herkend te worden zou sommigen ertoe kunnen aanzetten om af te zien van bepaalde rechten, zoals het recht op betogen[7].

Op 26 januari 2021 heeft Amnesty International 'Ban the Scan' gestart, een mondiale campagne om het gebruik van systemen van gezichtsherkenning te verbieden. Amnesty International stelt een vorm van massacontrole aan de kaak die het risico op racisme bij politieacties sterk vergroot en het recht op betogen bedreigt[8].

De speciale rapporteur van de Verenigde Naties voor de bevordering en bescherming van de rechten op vrijheid van mening en meningsuiting, David Kaye, merkt het volgende op: "surveillance tools can interfere with human rights, from the right to privacy and freedom of expression to rights of association and assembly, religious belief, non-discrimination, and public participation. And yet they are not subject to any effective global or national control."[9].

7. https://www.lesechos.fr/tech-medias/intelligence-artificielle/reconnaissance-faciale-la-defenseure-des-droits-craint-un-potentiel-inegale-de-discrimination-1333247.
8. https://www.amnesty.org/fr/latest/news/2021/01/ban-dangerous-facial-recognition-technology-that-amplifies-racist-policing/.
9. UN expert calls for immediate moratorium on the sale, transfer and use of surveillance tools", website van de Verenigde Naties Mensenrechten, 25 juni 2019.

Ces associations soulignent le fait que cette technologie entrave gravement les droits fondamentaux et libertés des citoyens, notamment le droit à la vie privée, le droit de manifester, de s'exprimer librement. Elles alertent sur le fait que les minorités sont particulièrement vulnérables face à ces technologies qui discriminent les personnes racisées et les personnes migrantes. L'un des risques liés à la reconnaissance faciale réside dans la possibilité de cibler et d'identifier les personnes issues de minorités sexuelles, par exemple dans le cas où des caméras seraient placées à proximité de lieux de rassemblement.

Ailleurs en Europe et dans le monde, les nombreux risques d'atteinte aux droits fondamentaux sont pointés par diverses institutions, et plusieurs villes ont par ailleurs banni l'utilisation de la technologie de reconnaissance faciale.

Ainsi, en juillet 2021 déjà, la Défenseure des droits française a publié un rapport consacré à la biométrie, alertant face au «potentiel inégalé d'amplification et d'automatisation des discriminations» lié à ce type de technologie. Si la Défenseure des droits pointe le risque d'erreurs, soulignant que «Dans le cas de la reconnaissance faciale, les conséquences de ces erreurs peuvent aller du refus d'accéder à un lieu, à une arrestation policière non justifiée», elle craint que cette technologie ne renforce les discriminations, même si elle était fiable à 100 %. L'institution craint notamment un déploiement de ces systèmes dans les zones géographiques où les populations font déjà beaucoup plus qu'ailleurs l'objet de contrôles d'identité, notamment là où sont surreprésentés les «jeunes hommes perçus comme issus des minorités». La peur d'être reconnu pourrait également pousser certaines personnes à renoncer à des droits, par exemple en renonçant à participer à une manifestation[7].

Le 26 janvier 2021, Amnesty international a lancé «Ban the Scan», une campagne mondiale en vue d'interdire l'utilisation des systèmes de reconnaissance faciale, dénonçant «une forme de surveillance de masse qui décuple le risque de racisme lors des opérations policières et menace le droit de manifester»[8].

Comme le fait remarquer le rapporteur spécial de l'ONU sur la liberté d'opinion et d'expression David Kaye, «Les outils de surveillance peuvent interférer avec les droits humains, du droit à la vie privée et de la liberté d'expression jusqu'aux droits d'association et de rassemblement, de liberté religieuse, du droit à la non-discrimination et à la participation publique. Et pourtant ils ne sont soumis à aucun contrôle global ou national effectif."[9].

7. https://www.lesechos.fr/tech-medias/intelligence-artificielle/reconnaissance-faciale-la-defenseure-des-droits-craint-un-potentiel-inegale-de-discrimination-1333247.
8. https://www.amnesty.org/fr/latest/news/2021/01/ban-dangerous-facial-recognition-technology-that-amplifies-racist-policing/
9. "UN expert calls for immediate moratorium on the sale, transfer and use of surveillance tools", site internet des Nations Unies Droits de l'Homme, le 25 juin 2019.

Uit een rapport van 2021 van het Government Accountability Office (GAO) van de Verenigde Staten blijkt dat niet minder dan zes overheidsagentschappen (FBI, US Park Police, US Postal Inspection service, US Marshals, ATF en US Capitol Police) gebruik hebben gemaakt van technologie voor de gezichtsherkenning van personen die betoogden voor "Black Lives Matter"[10].

In 2023 heeft de federale minister van Justitie Vincent Van Quickenborne (Open VLD) een wetsontwerp ingediend om justitie menselijker, sneller en straffer te maken (III).

Een van de bepalingen van het ontwerp voert een betogingsverbod in dat kan worden opgelegd voor een zeer ruime waaier van misdrijven. Het maatschappelijke middenveld heeft een breed front opgezet om de intrekking van deze nieuwe straf te vragen. Het Federaal Instituut voor de Rechten van de Mens stelt de vraag naar controle: "Hoe zal men bij, bijvoorbeeld, grote betogingen weten wie wel en wie niet aanwezig mag zijn? Zal men bij protestbijeenkomsten systematisch identiteitscontroles uitvoeren? Zal men in de verleiding komen camera's met gezichtsherkenning in te zetten om deze maatregel te doen naleven? (in zoverre dat zelfs effectief zou zijn, bv. in het geval van gezichtsbedekking)?"[11]. In het geval van een algemene invoering van gezichtsherkenning in ons land, bestaat het gevaar dat de technologie gebruikt wordt om personen te identificeren die deelnemen aan manifestaties en maatschappelijke bewegingen.

Deze risico's voor de grondrechten zijn des te meer onverantwoord omdat gezichtsherkenningstechnologie niet aantoonbaar efficiënt is in de strijd tegen criminaliteit. In Groot-Brittannië, waar gezichtsherkenning sinds 2016 gebruikt wordt, heeft een studie van de universiteit van Essex uit 2019 aangetoond dat 80 % van de met gezichtsherkenning geïdentificeerde personen eigenlijk onschuldig waren. De technologie identificeerde regelmatig personen ten onrechte, met alle sociale en wettelijke gevolgen van dien[12]. Volgens cijfers van de krant The Independent in 2018, zou gezichtsherkenningssoftware in niet minder dan 98 % van de gevallen de bal misslaan[13].

Voor een dergelijk pover resultaat heeft gezichtsherkenning een hoge kostprijs van ongeveer 50.000 euro per camera.

Deze voorbeelden en gevaren hebben geleid tot een verbod op gezichtsherkenning in verschillende delen van de wereld.

10. https://www.vice.com/en/article/3aqpmj/six-federal-agencies-used-facial-recognition-on-george-floyd-protestors.
11. Advies van het FIRM, Advies 2023-04 - Gerechtelijk betogingsverbod (1).pdf, blz. 12.
12. https://abcnews.go.com/International/80-facial-recognition-suspects-flagged-londons-met-police/story?id=64129255.
13. https://www.independent.co.uk/news/uk/home-news/met-police-facial-recognition-success-south-wales-trial-home-office-false-positive-a8345036.html.

Un rapport de 2021 du *Government Accountability Office* (GAO) des États-Unis révèle que pas moins de six agences gouvernementales (le FBI, la US Park Police, l'US Postal Inspection service, l'US Marshals, l'ATF et l'US Capitol Police) ont utilisé des technologies de reconnaissance faciale sur les manifestants «Black Lives Matter»[10].

En 2023, le ministre fédéral de la justice Vincent Van Quickenborne (Open VLD) a introduit un projet de loi «visant à rendre la justice plus humaine, plus rapide et plus ferme – III».

Parmi d'autres dispositions, ce projet introduit une peine d'interdiction de manifester pouvant être prononcée dans le cadre d'un panel très large d'infractions. Un large front de la société civile s'est uni pour demander le retrait de cette nouvelle peine. L'une des questions soulevées par l'Institut fédéral des droits humains est celle du contrôle: «Comment saura-t-on par exemple qui peut être présent ou non lors de manifestations à grande échelle? Va-t-on systématiquement procéder à des contrôles d'identité lors de rassemblements revendicatifs? Sera-t-on tenté de recourir à des caméras équipées de la technologie de reconnaissance faciale pour faire respecter cette mesure (pour autant que ce système soit efficace, par exemple dans l'hypothèse où les manifestants se couvrent le visage)?»[11]. En cas d'introduction généralisée de la reconnaissance faciale dans notre pays, le risque existe que celle-ci soit utilisée pour identifier les personnes participant à des manifestations ainsi qu'à des mouvements sociaux.

Ces risques pour les droits fondamentaux sont d'autant moins justifiés que la technologie de reconnaissance faciale n'a pas fait la preuve de son efficacité pour lutter contre la criminalité. En Grande-Bretagne, où la reconnaissance faciale est utilisée depuis 2016, une étude réalisée par l'université d'Essex en 2019 a démontré que 80 % des personnes identifiées par ce biais à Londres étaient en fait innocentes. Le système identifiait régulièrement des personnes à tort, avec toutes les conséquences sociales et légales que cela peut induire[12]. Selon des chiffres révélés par *The Independent* en 2018, les logiciels de reconnaissance faciale se tromperaient dans pas moins de 98 % des cas[13].

Pour un résultat aussi discutable, la reconnaissance faciale présente pourtant un coût important, autour de 50.000 euros par caméra.

Ces exemples et risques ont entraîné une interdiction de la reconnaissance faciale dans diverses régions du monde.

10. https://www.vice.com/en/article/3aqpmj/six-federal-agencies-used-facial-recognition-on-george-floyd-protestors.
11. Avis de l'IFDH, https://institutfederaldroitshumains.be/fr/publications/interdiction-judiciaire-de-manifester, p. 12.
12. https://abcnews.go.com/International/80-facial-recognition-suspects-flagged-londons-met-police/story?id=64129255.
13. https://www.independent.co.uk/news/uk/home-news/met-police-facial-recognition-success-south-wales-trial-home-office-false-positive-a8345036.html.

In de VS is gezichtsherkenning verboden in Portland, San Francisco, Oakland, Minneapolis, Jackson, Pittsburgh, Baltimore, Portland, en overal in de staat Vermont.

In Frankrijk heeft de stad Montpellier eind 2022 als eerste gezichtsherkenning verboden[14].

In Zwitserland is gezichtsherkenning verboden in Lausanne, Sankt Gallen en Zurich[15].

Op 14 juni 2023 heeft het Europees Parlement zijn onderhandelingspositie over de wet op de AI bepaald[16]. De tekst is aangenomen met 499 stemmen tegen 28, bij 93 onthoudingen en voert een verbod in op:

– AI-systemen die door het ongericht verzamelen van gezichtsbeelden op het internet of via videobewaking, databanken voor gezichtsherkenning aanleggen;

– systemen voor de herkenning van emoties in ordediensten, bij grensbeheer, op de werkvloer en in scholen;

– systemen voor de biometrische identificatie op afstand *a posteriori*, met als enige uitzondering de ordediensten met het oog op de vervolging van zware misdaden, en enkel na rechterlijke machtiging.

Deze beslissing van het Europees Parlement is op applaus onthaald door Amnesty International[17], dat evenwel betreurde dat de beslissing op bepaalde punten niet ver genoeg ging.

De ngo heeft het parlement en de lidstaten van de Europese Unie opgeroepen tot een verbod:

– op ontwikkeling, verkoop, gebruik en uitvoer van technologieën voor gezichtsherkenning en andere technologieën voor massacontrole;

– op systemen voor discriminerende profilering en risicobeheer en voorspellende systemen die gebruikt worden om bewegingen aan de grenzen te beperken, verbieden en voorkomen.

Er bestaat in ons land geen specifieke wetgeving over gezichtsherkenning.

14. https://www.nextinpact.com/article/70661/ia-contre-ia-montpellier-interdit-reconnaissance-faciale-a-aide-chatgpt.
15. https://www.humanrights.ch/fr/nouvelles/reconnaissance-biometrique-lieux-publics-une-menace-droits-humains.
16. https://oeil.secure.europarl.europa.eu/oeil/popups/printsummary.pdf?id=1747977&l=fr&t=E.
17. https://www.amnesty.org/fr/latest/news/2023/06/eu-european-parliament-adopts-ban-on-facial-recognition-but-leaves-migrants-refugees-and-asylum-seekers-at-risk/.

Ainsi, aux USA, la reconnaissance faciale est notamment interdite à Portland, San Francisco, Oakland, Minneapolis, Jackson, Pittsburgh, Baltimore, Portland, ainsi que dans la totalité de l'État du Vermont.

En France, la ville de Montpellier a été la première à interdire la reconnaissance faciale fin 2022[14].

En Suisse, la reconnaissance faciale est interdite dans les villes de Lausanne, Saint-Gall et Zurich[15].

Le 14 juin 2023, le Parlement européen a adopté sa position de négociation sur la loi sur l'IA[16]. Adopté à 499 voix pour, 28 contre et 93 abstentions, le texte prévoit l'interdiction:

– des systèmes d'IA qui créent ou développent, par le moissonnage non ciblé d'images faciales provenant de l'internet ou de la vidéosurveillance, des bases de données de reconnaissance faciale;

– des systèmes reconnaissance des émotions utilisés dans les services répressifs, la gestion des frontières, le lieu de travail et les établissements d'enseignement;

– les systèmes d'identification biométrique à distance «*a posteriori*», à la seule exception des forces de l'ordre pour la poursuite de crimes graves, et seulement après autorisation judiciaire.

Cette décision du Parlement européen a été saluée par Amnesty international [17], tout en regrettant qu'il n'aille pas assez loin sur certains points.

L'ONG a ainsi appelé le Parlement et les États membres de l'Union européenne:

– à interdire le développement, la vente, l'utilisation et l'exportation des technologies de reconnaissance faciale et autres technologies de reconnaissance de masse;

– à interdire les systèmes de profilage discriminatoire et d'évaluation des risques, de même que les systèmes de prédiction utilisés pour restreindre, interdire et prévenir les mouvements aux frontières.

La reconnaissance faciale ne fait pas l'objet d'un cadre législatif spécifique dans notre pays.

14. https://www.nextinpact.com/article/70661/ia-contre-ia-montpellier-interdit-reconnaissance-faciale-a-aide-chatgpt.
15. https://www.humanrights.ch/fr/nouvelles/reconnaissance-biometrique-lieux-publics-une-menace-droits-humains.
16. https://oeil.secure.europarl.europa.eu/oeil/popups/printsummary.pdf?id=1747977&l=fr&t=E.
17. https://www.amnesty.org/fr/latest/news/2023/06/eu-european-parliament-adopts-ban-on-facial-recognition-but-leaves-migrants-refugees-and-asylum-seekers-at-risk/.

Er is enkel de camerawet die de plaatsing en het gebruik van bewakingscamera's regelt. De camerawet en de wet op het politieambt staan het gebruik van gezichtsherkenningscamera's niet toe, waaruit afgeleid mag worden dat deze technologie niet door particulieren of overheidsdiensten mag worden gebruikt.

Op een vraag van federaal volksvertegenwoordiger Nabil Boukili (PVDA-PTB) in de commissie voor Binnenlandse Zaken van de Kamer van Volksvertegenwoordigers op 6 oktober 2021, heeft federaal minister van Binnenlandse Zaken Annelies Verlinden het volgende geantwoord: "Aangezien het Belgisch wettelijk kader de exploitatie van deze software [Clearview] niet toelaat, zal ze niet door de federale politie worden gebruikt, conform mijn eerdere antwoorden met betrekking tot dit thema. Clearview AI meldt dat het momenteel geen zaken doet in België of elders in de Europese Unie. Gezichtsherkenning is zeker een interessante piste om op termijn te gebruiken ter ondersteuning van de werking van de politie in uitvoering van de opdrachten van de bestuurlijke en gerechtelijke politie. Dat kan uiteraard enkel met een correcte wettelijke basis zodat de verkregen informatie rechtsgeldig bestuurlijk en gerechtelijk aangewend kan worden."[18].

Dit antwoord voldoet niet gelet op de bovenvermelde risico's. Mher Hakobyan, Advocacy Advisor on AI Regulation bij Amnesty International, verklaart daarover: "There is no human rights compliant way to use remote biometric identification (RBI). No fixes, technical or otherwise, can make it compatible with human rights law. The only safeguard against RBI is an outright ban. If these systems are legalized, it will set an alarming and far-reaching precedent, leading to the proliferation of AI technologies that don't comply with human rights in the future."[19].

De bereidheid van de federale minister van Binnenlandse Zaken om in de toekomst een wettelijk kader te creëren voor gezichtsherkenning, is voldoende reden om een debat binnen dit parlement te starten, een duidelijk standpunt over deze kwestie in te nemen en deze technologie gewoonweg te verbieden, zoals veel Amerikaanse en Europese steden hebben gedaan.

18. https://www.lachambre.be/doc/CCRI/pdf/55/ic597.pdf, blz. 15.
19. https://www.amnesty.org/fr/latest/news/2023/06/eu-european-parliament-adopts-ban-on-facial-recognition-but-leaves-migrants-refugees-and-asylum-seekers-at-risk/.

Seule existe la «loi caméras» qui régit l'installation et l'utilisation de caméras de surveillance. Cette loi «caméras» ainsi que la loi sur la fonction de police n'autorisant pas l'utilisation de caméras à reconnaissance faciale, il faut en déduire que cette technologie est interdite tant pour les particuliers que pour les pouvoirs publics.

Interrogée par le député fédéral Nabil Boukili (PTB-PVDA) en commission de l'Intérieur de la Chambre des représentants le 6 octobre 2021, la ministre de l'Intérieur Annelies Verlinden a indiqué que: «Vu que le cadre légal belge n'autorise pas l'exploitation de ce logiciel [Clearview], la police fédérale ne l'utilisera pas. La reconnaissance faciale constitue une application intéressante qui pourrait être utilisée à terme mais elle devra être assortie d'une base légale correcte, afin que les informations récoltées puissent être juridiquement utilisables.»[18].

Cette réponse n'est pas satisfaisante au regard des risques cités ci-dessus. Ainsi que l'indique Mher Hakobyan, conseiller en matière de plaidoyer sur la réglementation de l'intelligence artificielle à Amnesty International, «Il n'existe pas de moyen d'utiliser l'identification biométrique à distance tout en respectant les droits humains. Aucune correction, technique ou autre, ne saurait la rendre compatible avec le droit relatif aux droits humains. La seule garantie contre l'identification biométrique à distance est une interdiction pure et simple. Si ces systèmes sont légalisés, cela créera un précédent inquiétant et de grande portée, susceptible de conduire à l'avenir à la prolifération de technologies d'IA qui ne respectent pas les droits humains.»[19].

L'ouverture laissée par la ministre de l'Intérieur quant à la possibilité, à l'avenir, de créer un cadre légal pour l'utilisation de la reconnaissance faciale justifie d'ouvrir un débat au sein de ce parlement afin de prendre une position claire à ce sujet et d'exclure purement et simplement cette technologie, comme l'ont fait de nombreuses villes américaines et européennes.

Leïla LAHSSAINI (FR)
Petya OBOLENSKY (FR)
Francis DAGRIN (FR)
Jan BUSSELEN (NL)
Françoise DE SMEDT (FR)

18. https://www.lachambre.be/doc/CCRI/pdf/55/ic597.pdf, p. 15.
19. https://www.amnesty.org/fr/latest/news/2023/06/eu-european-parliament-adopts-ban-on-facial-recognition-but-leaves-migrants-refugees-and-asylum-seekers-at-risk/.

## VOORSTEL VAN RESOLUTIE

### betreffende het verbod op het gebruik van gezichtsherkenningssoftware en -algoritmen in vaste of mobiele bewakingscamera's in openbare ruimten in het Brussels Hoofdstedelijk Gewest

Het Brussels Hoofdstedelijk Parlement,

Overwegende dat de uitrol van gezichtsherkenning een bedreiging kan vormen voor de grondrechten, waaronder het recht op privacy, de bescherming van persoonsgegevens en de vrijheid van vergadering;

Overwegende artikel 12 van de Universele Verklaring van de Rechten van de Mens luidende: "Niemand zal onderworpen worden aan willekeurige inmenging in zijn persoonlijke aangelegenheden, in zijn gezin, zijn tehuis of zijn briefwisseling, noch aan enige aantasting van zijn eer of goede naam. Tegen een dergelijke inmenging of aantasting heeft een ieder recht op bescherming door de wet";

Overwegende artikel 8 van het Europees Verdrag voor de Rechten van de Mens met betrekking tot het respect voor het privéleven en het gezinsleven luidende: "Eenieder heeft recht op respect voor zijn privéleven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie. Geen inmenging van enig openbaar gezag is toegestaan in de uitoefening van dit recht, dan voor zover bij de wet is voorzien en in een democratische samenleving noodzakelijk is in het belang van de nationale veiligheid, de openbare veiligheid of het economisch welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden of voor de bescherming van de rechten en vrijheden van anderen.";

Overwegende artikel 7 van het Handvest van de Grondrechten van de Europese Unie met betrekking tot het privéleven en het gezinsleven luidende: "Eenieder heeft recht op eerbiediging van zijn privéleven, zijn familie- en gezinsleven, zijn woning en zijn communicatie";

Overwegende artikel 22 van de Belgische Grondwet luidende: "Ieder heeft recht op eerbiediging van zijn privéleven en zijn gezinsleven, behoudens in de gevallen en onder de voorwaarden door de wet bepaald";

Overwegende de gevaren van deze technologie die op niet-exhaustieve wijze aan de kaak gesteld werden in de campagne Protect my face, door de Franse Défenseur des droits, Amnesty International en de speciale rapporteur van de Verenigde Naties voor de bevordering en bescherming van de rechten op vrijheid van mening en meningsuiting, David Kaye, die een onmiddellijk moratorium op de verkoop, overdracht en het gebruik van surveillancetechnologie vroeg;

Overwegende dat de precieze impact van dit belangrijke probleem van gezichtsherkenning op de rechten van de mensen nog niet bekend is en het dus aangewezen is om de

## PROPOSITION DE RÉSOLUTION

### relative à l'interdiction de l'utilisation de logiciels et d'algorithmes de reconnaissance faciale sur les caméras de surveillance, fixes ou mobiles, dans les endroits publics de la Région de Bruxelles-Capitale

Le Parlement de la Région de Bruxelles-Capitale,

Considérant que des droits fondamentaux pourraient être menacés par la mise en place de la reconnaissance faciale, dont le droit au respect de la vie privée, la protection des données personnelles ou la liberté de réunion;

Considérant l'article 12 de la Déclaration universelle des droits de l'homme qui stipule: «Nul ne sera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes à son honneur et à sa réputation. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes»;

Considérant l'article 8 de la Convention européenne des droits de l'homme concernant le droit au respect de la vie privée et familiale qui stipule: «Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance. Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui.»;

Considérant l'article 7 de la Charte des droits fondamentaux de l'Union européenne qui concerne le respect de la vie privée et familiale et qui stipule que «Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de ses communications»;

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

Considérant les dangers de cette technologie dénoncés, de façon non exhaustive, par la Campagne *Protect my face*, par la Défenseure des droits française, par Amnesty international, et par le rapporteur spécial de l'ONU sur la liberté d'opinion et d'expression David Kaye, demandant un moratoire immédiat sur la vente, le transfert et l'utilisation des technologies de surveillance;

Considérant qu'on ne connaît pas encore l'impact précis qu'aura la technologie de reconnaissance faciale sur les droits humains, alors qu'il s'agit d'une question

technologie niet te implementeren alvorens alle gevolgen bekend zijn;

Overwegende dat het mediabedrijf BuzzFeed begin 2020 dankzij een datalek een lijst kon onthullen van gebruikers van gezichtsherkenningstechnologie ontwikkeld door het zeer controversiële bedrijf Clearview AI, waaronder Belgische politiediensten;

Overwegende dat het COC, het federale Controleorgaan belast met het toezicht op de politionele informatiehuishouding in België, daar niet op de hoogte van was en beslist heeft om een onderzoek te openen waaruit gebleken is dat "de centrale directie van de bestrijding van de zware en georganiseerde criminaliteit (DJSOC) onmiddellijk na afloop van de taskforce mondeling en minstens op 7 november 2019 formeel schriftelijk op de hoogte was van het gebruik van de Clearviewapplicatie. Dit betekent dat de hiërarchie van de federale gerechtelijke politie onmiddellijk na de taskforce bij Europol […] op de hoogte was van het gebruik van de Clearview-gezichtsherkenningstechnologie en dit ook heeft toegestaan." Dit onderzoek heeft aangetoond dat Clearview AI voor de eerste maal gebruikt is door een lid van de federale gerechtelijke politie in oktober 2019 in het kader van de taskforce van Europol en het NCMEC-dossier dat "foto's en beelden van potentiële daders en slachtoffers van seksueel geweld op minderjarigen" verzamelt. De leden van de DJSOC hebben de software 78 maal gebruikt tot 10 februari 2020 waarna de accounts werden afgesloten. De verplichting om een impactanalyse met betrekking tot de gegevensbescherming te maken is ook niet door de DJSOC nageleefd. In oktober 2021 heeft federaal minister van Binnenlandse Zaken Annelies Verlinden uiteindelijk in het parlement toegegeven dat deze software wel degelijk getest werd;

Overwegende dat volgens een onderzoek van de KU Leuven in het Vlaams Gewest en het Brussels Gewest, ten minste 5 lokale politiezones op 86 respondenten, over gezichtsherkenning beschikten in 2021, en dat een van hen bevestigde die "vaak tot zeer vaak" te gebruiken";

Overwegende dat in het Brussels Gewest politiezones gebruikmaken van de software voor analyse van videocontent BriefCam van het Israëlische bedrijf van dezelfde naam, om door middel van algoritmen een analyse te maken van de beelden van camera's die de Brusselse openbare ruimte filmen en alle objecten (mensen, dieren, auto's enz.) extraheren die in beweging zijn tegenover een vaste achtergrond. BriefCam stelt ook gezichts-herkenningstechnologie voor die compatibel is met een deel van het cameranetwerk in Brussel;

Overwegende dat in een casestudy van het bedrijf Genetec, toenmalig gewestelijk coördinator voor de veiligheid bij het CIBG – Centrum voor Informatica van het Brussels Gewest – Christian Banken, met betrekking tot BriefCam verklaarde dat de volgende stap de integratie zou worden van gezichtsherkenning en herkenning van nummerplaten;

Overwegende dat andere politiezones zoals Moeskroen en

essentielle, et qu'il est par conséquent important de ne pas implémenter la technologie avant qu'on n'en connaisse toutes les implications;

Considérant que début 2020, une fuite de données a permis au media *Buzzfeed* de révéler une liste d'utilisateurs des technologies de reconnaissance faciale développées par la très controversée entreprise *Clearview AI*, parmi lesquels figurent des services de police belges;

Considérant que le COC, l'Organe de contrôle fédéral chargé de surveiller l'usage de l'information policière en Belgique, qui n'était nullement informé de cela, décida d'ouvrir une enquête qui indiqua que «la Direction centrale de la lutte contre la criminalité grave et organisée (DJSOC) a été informée de l'utilisation de l'application *Clearview* immédiatement après la *taskforce* (verbalement), et au moins le 7 novembre 2019 de manière formelle par écrit. Cela signifie que la hiérarchie de la police judiciaire fédérale était au courant de l'utilisation de la technologie de reconnaissance faciale de *Clearview* immédiatement après la *taskforce* d'Europol [...], et a également toléré cette utilisation.». Cette enquête a révélé que *Clearview AI* a été utilisé pour la première fois par un membre de la police judiciaire belge en octobre 2019 dans le cadre de la *taskforce* d'Europol et du dossier NCMEC qui rassemble «des photos et images d'auteurs et victimes potentiels de violences sexuelles à l'encontre de mineurs d'âge». Les membres de la DJSOC ont utilisé le logiciel à 78 reprises jusqu'au 10 février 2020, date à laquelle les comptes furent clôturés. L'obligation de réaliser une analyse d'impact relative à la protection des données (AIPD) n'a pas non plus été respectée par la DJSOC. En octobre 2021, la ministre de l'Intérieur Verlinden admettra finalement au parlement que ce logiciel a bien été testé;

Considérant que selon une recherche menée par la KU Leuven en Flandre et en Région bruxelloise, au moins 5 zones de police locale sur 86 répondantes, disposaient de la reconnaissance faciale en 2021, l'une d'elle affirmant même l'utiliser «souvent à très souvent»;

Considérant qu'en Région bruxelloise, des zones de police utilisent notamment le logiciel d'analyse de contenu vidéo *BriefCam*, de la société israélienne du même nom, pour analyser, au moyen d'algorithmes, les images des caméras qui filment l'espace public bruxellois et extraire tous les objets (humains, animaux, voitures, etc.) en mouvement d'un arrière-plan fixe. *Briefcam* propose également des technologies de reconnaissance faciale compatibles avec une partie du réseau de caméras à Bruxelles;

Considérant que dans une étude de cas rédigée par l'entreprise Genetec, Christian Banken qui était alors coordinateur régional pour la sécurité au CIRB – Centre d'informatique de la Région bruxelloise – disait à propos de *Briefcam*: «Notre prochaine étape sera l'intégration de la reconnaissance faciale et des plaques minéralogiques»;

Considérant que d'autres zones de police telles que

Kortrijk, Kuurne en Lendelede ook de technologie van BriefCam gebruiken. In het kader van een onderzoek naar cameratoezicht in Kortrijk schreef de krant Médor dat het bedrijf RTS, dat een invoerlicentie heeft voor BriefCam en het systeem in Kortrijk ingevoerd heeft, in die tijd de gebruikersrechten voor gezichtsherkenning heeft moeten desactiveren. De optie is automatisch beschikbaar. RTS voert aan dat hun leveranciers ervan uitgaan dat iedereen gebruik wil maken van gezichtsherkenning;

Overwegende dat federaal minister van Binnenlandse Zaken Annelies Verlinden op 6 oktober 2021 in de commissie voor Binnenlandse Zaken van het federaal parlement het volgende verklaard heeft: "Gezichtsherkenning is zeker een interessante piste om op termijn te gebruiken ter ondersteuning van de werking van de politie in uitvoering van de opdrachten van de bestuurlijke en gerechtelijke politie. Dat kan uiteraard enkel met een correcte wettelijke basis zodat de verkregen informatie rechtsgeldig bestuurlijk en gerechtelijk kan worden aangewend.";

Overwegende de onderhandelingspositie van het Europees Parlement dat zich uitspreekt voor een verbod op deze technologieën;

Verzoekt de federale regering:

– om de aankoop en het gebruik van software en algoritmen voor gezichtsherkenning voor vaste of mobiele bewakingscamera's in openbare ruimten te verbieden;

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

– om te werken aan een verbod op de aankoop en het gebruik van software en algoritmen voor gezichtsherkenning voor vaste of mobiele bewakingscamera's in openbare ruimten op het volledige grondgebied van het Brussels Hoofdstedelijk Gewest;

– om na te gaan of deze technologie al gebruikt wordt in de Brusselse politiezones, met name voor ordehandhaving, en of er daartoe biometrische data verzameld werden;

– om controle uit te oefenen op het platform voor gedeelde camerabewakingsbeelden en na te gaan of er geen matching (overeenstemming van beelden via software voor gezichtsherkenning) a posteriori gebeurt door middel van de beelden die via het platform gebruikt worden;

– om naar een totale transparantie te streven voor:

  – de precieze praktijken en gebruiken, de gebruikte software, de monitoring;

celles de Mouscron et de Kortrijk, Kuurne et Lendelde utilisent également la technologie de *Briefcam*. Dans une enquête sur la vidéosurveillance à Courtrai, le journal *Médor* écrivait: «La société RTS, qui détient une licence d'importateur pour *Briefcam* et l'a installée à Courtrai, a dû, à l'époque, désactiver les droits d'utilisateur pour la reconnaissance faciale. L'option est automatiquement disponible. RTS se justifie: leurs fournisseurs «supposent que tout le monde veut faire usage de la reconnaissance faciale»;

Considérant que la ministre de l'Intérieur Annelies Verlinden déclarait le 6 octobre 2021 en commission de l'Intérieur du Parlement fédéral: «La reconnaissance faciale est une piste intéressante à utiliser à l'avenir en appui du fonctionnement de la police dans le cadre de la réalisation des missions de police administrative et judiciaire. Ce n'est évidemment possible que moyennant une base légale correcte, de manière à ce que les informations obtenues puissent être utilisées valablement sur le plan administratif et judiciaire.»;

Considérant la position de négociation adoptée par le Parlement européen se prononçant pour une interdiction de ces technologies;

Demande au Gouvernement fédéral:

– de mettre en place une interdiction d'achat et d'utilisation de logiciels et d'algorithmes de reconnaissance faciale sur les caméras de surveillance, fixes ou mobiles, dans les endroits publics;

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

– de s'engager en faveur d'une interdiction d'achat et d'utilisation de logiciels et d'algorithmes de reconnaissance faciale sur les caméras de surveillance, fixes ou mobiles, dans les endroits publics sur l'ensemble du territoire de la Région de Bruxelles-Capitale;

– de clarifier si cette technologie est déjà utilisée au sein des zones de police bruxelloises, notamment à des fins de maintien de l'ordre, et si des fichiers biométriques ont été constitués dans ce but;

– de réaliser un contrôle de la plateforme de mutualisation des images de vidéosurveillance et de vérifier qu'aucun «matching» (correspondance d'images à l'aide d'un logiciel de reconnaissance faciale) *a posteriori* n'est effectué grâce aux images utilisées via la plateforme de mutualisation;

– de faire toute la transparence sur:

  – les pratiques et usage précis, les logiciels utilisés, le monitoring effectué;

– de overheidsopdrachten om te voorkomen dat er financiële middelen gaan naar de aanleg van bestanden met biometrische kenmerken of de ontwikkeling van technologieën die biometrische surveillance op het grondgebied van het Brussels Hoofdstedelijk Gewest mogelijk maken;

– de onderaannemers, dienstverleners en bedrijven op gewestelijk en federaal niveau, die betrokken zijn bij (gedeelde) camerabewaking op het Brusselse grondgebied.

– les marchés publics afin de s'assurer qu'aucun financement ne soit alloué au développement de fichiers biométriques ou de technologies permettant la surveillance biométrique sur le territoire de la Région de Bruxelles-Capitale;

– la liste des différents sous-traitants, prestataires et entreprises, au niveau régional et fédéral, impliqués dans la vidéosurveillance (mutualisée) utilisée sur le sol bruxellois.

Leïla LAHSSAINI (FR)
Petya OBOLENSKY (FR)
Francis DAGRIN (FR)
Jan BUSSELEN (NL)
Françoise DE SMEDT (FR)