PARLEMENT BRUXELLOIS
BRUSSELS PARLEMENT

**A-719/1** – 2022/2023

SESSION ORDINAIRE 2022-2023

13JUIN 2023

# PARLEMENT DE LA RÉGION DE BRUXELLES-CAPITALE

## Examen de la pétition contre l'usage de la reconnaissance faciale en Région de Bruxelles-Capitale

**RAPPORT**
fait au nom de la commission
des Affaires intérieures

par M. Hicham TALHI (F)

Ont participé aux travaux de la commission :

*Membres effectifs :* MM. Marc-Jean Ghyssels, Jamal Ikazban, Mme Fadila Laanan, MM. Ahmed Mouhssin, John Pitseys, Hicham Talhi, Mme Dominique Dufourny, M. Sadik Köksal, Mmes Leila Lahssaini, Els Rochette, MM. Mathias Vanden Borre, Guy Vanhengel.

*Autre membre :* M. Christophe De Beukelaer.

GEWONE ZITTING 2022-2023

13 JUNI 2023

# BRUSSELS HOOFDSTEDELIJK PARLEMENT

## Behandeling van de petitie tegen het gebruik van gezichtsherkenning in het Brussels Hoofdstedelijk Gewest

**VERSLAG**
uitgebracht namens de commissie
voor de Binnenlandse Zaken

door de heer Hicham TALHI (F)

Aan de werkzaamheden van de commissie hebben deelgenomen:

*Vaste leden:* De heren Marc-Jean Ghyssels, Jamal Ikazban, mevr. Fadila Laanan, de heren Ahmed Mouhssin, John Pitseys, Hicham Talhi, mevr. Dominique Dufourny, de heer Sadik Köksal, mevr. Leila Lahssaini, mevr. Els Rochette, de heren Mathias Vanden Borre, Guy Vanhengel.

*Ander lid:* De heer Christophe De Beukelaer.

## I. Introduction

Le président souhaite la bienvenue à Mme Joke Blockx, directrice de la « Liga voor Mensenrechten », à Mme Nicha Mbuli, juriste au MRAX (Mouvement contre le racisme, l'antisémitisme et la xénophobie) et à M. Rémy Farge, formateur à la Ligue des droits humains, coauteurs de la pétition contre l'usage de la reconnaissance faciale en Région de Bruxelles-Capitale.

Cette pétition répond à toutes les conditions de forme et est revêtue de plus de 1.000 signatures.

## II. Exposé introductif de Mme Joke Blockx, Mme Nicha Mbuli, et M. Rémy Farge, coauteurs de la pétition

Les coauteurs de la pétition ont tenu devant les commissaires, en s'appuyant pour ce faire sur une présentation Powerpoint, l'exposé suivant :

**Mme Joke Blockx** : « Je vous remercie de l'invitation à venir vous parler de la reconnaissance faciale aujourd'hui. Je m'appelle Joke Blockx et je suis directrice de la Liga voor Mensenrechten. Avec le MRAX et la Ligue des droits humains, nous représentons une coalition de huit organisations bruxelloises de défense des droits humains qui se sont fédérées dans le cadre la campagne *Protect My Face*. En mars de cette année, nous avons déposé sur la plateforme en ligne *democratie.brussels* une pétition dans laquelle nous demandons de préserver le droit au respect de la vie privée des Bruxellois. En moins de deux mois, plus de 1.000 citoyens ont soutenu l'interdiction de l'usage de la reconnaissance faciale dans l'espace public bruxellois. C'est grâce à eux que nous sommes ici aujourd'hui.

Avant d'expliquer pourquoi le Parlement bruxellois devrait se prononcer en faveur d'une interdiction de la reconnaissance faciale, examinons de plus près ce qu'implique cette technologie.

*Qu'est-ce que la reconnaissance faciale ?*

L'Autorité de protection des données définit la reconnaissance faciale comme une technique permettant d'authentifier ou d'identifier une personne sur la base des traits de son visage :

- Par "authentifier", on entend : vérifier qu'une personne est bien qui elle prétend être. Utilisé aux contrôles d'accès, par exemple, un tel système détermine si l'identité obtenue au moyen de la reconnaissance faciale correspond à l'identité précédemment stockée dans la base de données.

- Identifier permet de retrouver une personne au sein d'un groupe, dans un lieu, une image ou une base de données. Ce système analyse si le visage présenté correspond aux modèles

## I. Inleiding

De voorzitter verwelkomt mevrouw Joke Blockx, directrice van de Liga voor Mensenrechten, mevrouw Nicha Mbuli, juriste bij het MRAX (Mouvement contre le Racisme, l'Antisémitisme et la Xénophobie) en de heer Rémy Farge, opleider bij de « Ligue des droits humains », mede-indieners van de petitie tegen het gebruik van gezichtsherkenning in het Brussels Hoofdstedelijk Gewest.

Deze petitie voldoet aan alle vormvereisten en is ondertekend door meer dan 1.000 personen.

## II. Inleidende uiteenzetting van mevrouw Joke Blockx, mevrouw Nicha Mbuli en de heer Rémy Farge, mede-indieners van de petitie

De mede-indieners van de petitie hielden voor de commissieleden, met een PowerPointpresentatie, de volgende uiteenzetting:

**Mevrouw Joke Blockx**: "Bedankt voor de gelegenheid om het vandaag met u over gezichtsherkenning te hebben. Mijn naam is Joke Blockx, ik ben directeur van de Liga voor Mensenrechten. Samen met het MRAX en la Ligue des Droits Humains vertegenwoordigen wij een coalitie van acht Brusselse organisaties die opkomen voor de bescherming van de mensenrechten en die zich hebben verenigd in de campagne *Protect My Face*. In maart van dit jaar hebben wij een petitie ingediend op het onlineplatform *democratie.brussels*. In die petitie vragen wij om het recht op privacy van de Brusselaars te vrijwaren. In minder dan twee maanden tijd hebben meer dan 1.000 burgers het verbod op het gebruik van gezichtsherkenning in de publieke ruimte van Brussel gesteund. Het is dankzij hen dat wij hier vandaag zitten.

Vooraleer we uitleggen waarom het Brussels Parlement zich moet uitspreken voor een verbod op gezichtsherkenning, gaan we eerst dieper in op wat de technologie inhoudt.

*Wat is gezichtsherkenning?*

De Gegevensbeschermingsautoriteit definieert gezichtsherkenning als een techniek die het mogelijk maakt om aan de hand van gelaatstrekken een persoon te authenticeren of te identificeren:

- Authenticatie betekent verifiëren of iemand is wie hij beweert te zijn. Dat gebeurt bijvoorbeeld bij toegangscontroles. Zo'n systeem vergelijkt of de identiteit die door middel van gezichtsherkenning wordt vastgesteld, overeenkomt met de identiteit die eerder in de database werd opgeslagen.

- Identificatie maakt het mogelijk om iemand in een groep van individuen, een plaats, een afbeelding of een database op te sporen. Er wordt nagegaan of het gezicht

enregistrés dans la base de données sur la base de "critères de similarité".

La reconnaissance faciale effectue des analyses à partir des caractéristiques du visage, telles que la longueur du visage, l'écartement des yeux, l'arête du nez, la distance entre la bouche et le nez, etc. Le système convertit ces caractéristiques faciales en données biométriques et les compare aux données collectées et stockées dans une base de données. En principe, toute caméra peut être équipée d'un logiciel de reconnaissance faciale. Les analyses peuvent être effectuées en temps réel ou a posteriori, sur la base d'images stockées.

En principe, il faut donc trois éléments pour utiliser la reconnaissance faciale : une caméra, un logiciel de reconnaissance faciale et une ou plusieurs bases de données.

Il est important de souligner qu'il s'agit clairement de données biométriques – des données uniques, propres à une personne. Ces données sont donc considérées comme des données personnelles très sensibles en vertu des lois européennes et nationales sur la protection de la vie privée.

Sachant ce qu'implique la reconnaissance faciale, nous tenons à souligner que notre pétition porte sur l'utilisation, par les autorités et la police, de la reconnaissance faciale afin d'identifier une personne. Le Parlement bruxellois a la possibilité de jouer un rôle important dans ce dossier.

*Que dit la loi ?*

En Belgique, aucune loi ne réglemente l'usage de la technologie de reconnaissance faciale. Comme je viens de le dire, il s'agit pourtant de données biométriques, des données uniques, propres à chacun – notre visage, nos empreintes digitales, nos iris, par exemple. C'est ce qui rend ces données si intéressantes pour l'identification des personnes, mais également si dangereuses lorsqu'elles sont utilisées à mauvais escient. Le traitement des données biométriques a un impact majeur sur notre vie privée. C'est précisément pourquoi nous devons être prudents en la matière. En vertu de la législation sur la protection de la vie privée, les données biométriques ne peuvent, par définition, pas être traitées, sauf sous certaines conditions. Un dispositif légal est le minimum requis à cet égard.

En l'absence de législation, la reconnaissance faciale doit, à ce jour, être considérée comme une technique illégale et donc interdite.

Nous ne sommes pas les seuls à le dire. Le COC – l'Organe de contrôle de l'information policière – l'a lui aussi encore souligné récemment. En mai 2020, un projet de résolution déposé au parlement fédéral demandait un moratoire de trois ans sur l'utilisation de logiciels et d'algorithmes de reconnaissance faciale dans les caméras de sécurité fixes ou mobiles installées dans l'espace public et les lieux privés. Dans son avis sur cette résolution, le COC souligne que : « Ni la loi sur la fonction de police, ni le Code d'instruction criminelle ni une quelconque autre loi (pénale)

overeenkomt met de modellen die zijn geregistreerd in de database op basis van "gelijkaardigheidscriteria".

Gezichtsherkenning gebruikt de kenmerken van het gelaat om analyses op uit te voeren. Het gaat dan bijvoorbeeld om de lengte van het gezicht, de afstand tussen de ogen, de neusbrug, de afstand tussen de mond en de neus enz. Het systeem zet die gezichtskenmerken om in biometrische gegevens en vergelijkt ze met gegevens die verzameld en opgeslagen zijn in een database. In principe kan elke camera uitgerust worden met gezichtsherkenningssoftware. De analyses kunnen zowel in *real time* of achteraf, op basis van opgeslagen beelden, gebeuren.

Je hebt dus in principe drie dingen nodig voor gezichtsherkenning: een camera, gezichtsherkenningssoftware en één of meerdere databanken.

Belangrijk om mee te geven is dat het hier duidelijk om biometrische gegevens gaat - gegevens die uniek zijn bij elk individu -, en daarom als zeer gevoelige persoonsgegevens worden beschouwd onder de Europese en nationale privacywetten.

Nu we weten wat gezichtsherkenning inhoudt, willen we benadrukken dat onze petitie gaat over het gebruik van gezichtsherkenning door overheden en politie om iemand te identificeren. Het Brussels Parlement heeft de kans om in deze materie een belangrijke rol te spelen.

*Wat zegt de wet ?*

Er bestaat in België geen enkele wet die het gebruik van gezichtsherkenningstechnologie reguleert. Zoals ik net al zei, gaat het nochtans om biometrische gegevens. Dat zijn gegevens die uniek zijn bij elk individu – zoals ons gezicht, onze vingerafdrukken, onze irissen. Daardoor zijn ze zo interessant om mensen te identificeren en is het risico ook zo groot wanneer ze misbruikt worden. De verwerking van biometrische gegevens heeft een grote impact op onze privacy. Net daarom moeten we er voorzichtig mee omspringen. Op grond van de privacywetgeving mogen biometrische gegevens per definitie niet verwerkt worden, tenzij onder bepaalde voorwaarden. Een wettelijke regeling is daarbij het minimum.

Aangezien er geen wetgeving is, moet gezichtsherkenning voorlopig beschouwd worden als een illegale en dus verboden techniek.

Wij zijn niet de enigen die dat zeggen, ook het COC - het Controleorgaan op de Politionele Informatie - hamerde er recent nog op. In mei 2020 werd een ontwerp van resolutie ingediend in het Federaal Parlement waarin gevraagd werd om een driejarig moratorium in te stellen op het gebruik van gezichtsherkenningssoftware en algoritmen bij vaste of mobiele beveiligingscamera's in de openbare ruimte en privélocaties. In zijn advies over de resolutie wijst het COC erop dat: "Noch de Wet op het Politieambt, noch het Wetboek van Strafvordering, noch enige andere bijzondere

spéciale n'offre *de lege lata* un fondement juridique (suffisant) pour l'utilisation de la technologie de reconnaissance faciale dans le cadre de missions de police administrative ou judiciaire. » Une législation sur l'intelligence artificielle (loi IA) est en cours d'élaboration au niveau de l'Union européenne. Nous espérons qu'à l'issue du processus législatif en cours, la reconnaissance faciale sera strictement interdite en Europe, mais rien ne le garantit pour l'instant. Le vote au Parlement européen est prévu pour le 14 juin. Toutefois, ces règles risquent de ne pas entrer en vigueur avant plusieurs années. »

**M. Rémy Farge** : « Des tests ont déjà été réalisés par les services de police belges sans aucune transparence ni débat public. La police fédérale a en effet déjà mené plusieurs tests qui ont été pour la plupart interrompus par l'Organe de contrôle de l'information policière (COC), parce que jugés illégaux. Des expérimentations souvent lancées sans avoir sollicité l'avis du COC, alors que la loi l'y oblige.

*Rétroactes*

La reconnaissance faciale a été testée une première fois par la police fédérale à l'aéroport de Zaventem en 2017. De nombreuses erreurs causant des faux positifs avaient été constatées, notamment pour la reconnaissance de la couleur de peau, des lunettes et de la pilosité, ce qui avait mis fin à cette première tentative.

En 2019, le public apprenait en même temps que le COC qu'une nouvelle phase test était en route à l'aéroport. Ces tests visaient à repérer des suspects en matière de terrorisme et de criminalité organisée. "Nous allons comparer des photos d'auteurs (de crimes) connus, en des endroits spécifiques, sur place et en temps réel", expliquait à la RTBF la porte-parole de la police fédérale Sarah Frederickx.

Lors de sa visite, le COC a constaté que le système était encore partiellement actif : "des données biométriques sont encore collectées et conservées, mais sans être comparées aux photos de la (des) liste(s)." En juillet 2019, le COC a demandé dans un rapport de "mettre temporairement un terme à l'utilisation du système de reconnaissance faciale". Il a principalement pris cette décision parce que ce projet ne reposait sur aucun fondement juridique correct.

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.

Le COC, qui n'en était nullement informé, décidera d'ouvrir une enquête.[1]

Alors que le commissaire général de la police fédérale disait le 19 mai 2020 au COC qu'il n'avait "pas connaissance, au niveau organisationnel de la police fédérale, d'une utilisation de logiciels de reconnaissance faciale au sein des

(straf)wet *de lege lata* een (voldoende) wettelijke basis biedt voor het gebruik van gezichtsherkenningstechnologie in bestuurlijk of gerechtelijk politiewerk". De Europese Unie werkt momenteel aan wetgeving inzake artificiële intelligentie (AI-wet). We hopen dat aan het einde van het huidige wetgevingsproces gezichtsherkenning in Europa strikt verboden zal worden, maar momenteel is er geen garantie. De stemming in het Europees Parlement is gepland op 14 juni. Het risico bestaat echter dat de regels pas over enkele jaren van kracht worden.".

**M. Rémy Farge**: "De Belgische politie heeft al tests gedaan zonder enige vorm van transparantie of openbaar debat. De federale politie heeft meerdere proeven gedaan die het Controleorgaan van de politie (COC) grotendeels heeft stopgezet omdat ze als illegaal werden beschouwd. Vaak worden proeven opgezet zonder het advies van het COC te vragen, terwijl dat wettelijk verplicht is.

*Voorgeschiedenis*

Gezichtsherkenning werd voor het eerst getest door de federale politie op de luchthaven van Zaventem in 2017. De test gaf aanleiding tot talloze fouten bij de herkenning van de huidskleur, de bril en het haar, wat het einde van het eerste experiment inluidde.

In 2019 vernamen het publiek en het COC dat op de luchthaven een nieuwe testfase liep. Het doel was om verdachten van terrorisme en georganiseerde misdaad op te sporen. "We zullen foto's van bekende misdadigers, op specifieke locaties, ter plaatse en in real time vergelijken", legde federale politiewoordvoerster Sarah Frederickx uit aan de RTBF.

Tijdens haar bezoek stelde het COC vast dat het systeem nog gedeeltelijk werd gebruikt: "er worden nog steeds biometrische gegevens verzameld en opgeslagen, maar zonder ze te vergelijken met de foto's op de lijst(en)." In juli 2019 vroeg het COC in een rapport om "het gebruik van het gezichtsherkenningssysteem tijdelijk stop te zetten". Het nam dit besluit vooral omdat er geen goede wettelijke basis voor was.

Begin 2020 onthulde *Buzzfeed* na een datalek een lijst van gebruikers van gezichtsherkenningstechnologieën ontwikkeld door het controversiële bedrijf Clearview AI, waaronder Belgische politiediensten.

Het COC, dat daar geen weet van had, besloot een onderzoek in te stellen.[11]

Hoewel de commissaris-generaal van de federale politie het COC op 19 mei 2020 vertelde dat "hij niet op de hoogte was van het gebruik van gezichtsherkenningssoftware bij de federale politie", bleek uit het onderzoek het tegendeel.

[1] Rapport de contrôle de l'organe de contrôle de l'information policière relatif à l'utilisation de l'application Clearview AI par la police intégrée. https://www.organedecontrole.be/files/DIO21006_Rapport_Contr%C3%B4le_Clearview_F_00050441.pdf

[11] toezichtrapport van het controleorgaan op de politionele informatie met betrekking tot het gebruik van clearview AI door de geïntegreerde politie. https://www.controleorgaan.be/files/DIO21006_Toezichtrapport_Clearview_N_00050443.pdf

services de police", l'enquête révélera le contraire.

Le COC écrit : "La Direction centrale de la lutte contre la criminalité grave et organisée (DJSOC) a été informée de l'utilisation de l'application Clearview AI immédiatement après la task force (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 AI immédiatement après la task force d'Europol, et a également toléré cette utilisation."

L'enquête du COC révèle 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 task force 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.

Par ailleurs, selon une recherche menée par la KULeuven 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".[2]

En Région bruxelloise, des zones de police utilisent notamment le logiciel d'analyse de contenu vidéo BriefCam[3], 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.

Les zones de police telles que celles de Mouscron et de Courtrai, Kuurne et Lendelede utilisent également la technologie de Briefcam. Dans une enquête sur la vidéosurveillance à Courtrai, *Médor* écrivait : "La société RTS, qui détient une licence d'importateur pour Briefcam et l'a installé 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".[4]

Het COC schrijft: "De Centrale directie van de bestrijding van de zware en georganiseerde criminaliteit (DJSOC) werd meteen na de bijeenkomst van de werkgroep mondeling en op 7 november 2019 schriftelijk formeel op de hoogte gebracht van het gebruik van de Clearview AI-toepassing. Dat betekent dat de hiërarchie van de federale gerechtelijke politie onmiddellijk na de bijeenkomst van de Europolwerkgroep op de hoogte was van het gebruik van de gezichtsherkenningstechnologie van Clearview AI en dat gebruik ook toeliet."

Uit het onderzoek van het COC blijkt dat Clearview AI in oktober 2019 voor het eerst werd gebruikt door een lid van de Belgische gerechtelijke politie in het kader van de Europoltaskforce en het NCMEC-dossier, dat "foto's en beelden van mogelijke daders en slachtoffers van seksueel geweld tegen minderjarigen" bevat. Leden van de DJSOC gebruikten de software 78 keer tot 10 februari 2020, toen de accounts werden afgesloten. Ook de verplichte Data Protection Impact Assessment (DPIA) voerde de DJSOC niet uit. In oktober 2021 gaf federaal minister Verlinden van Binnenlandse Zaken in het federale parlement uiteindelijk toe dat de software wel degelijk was getest.

Voorts blijkt uit onderzoek van de KULeuven in Vlaanderen en het Brussels Gewest dat ten minste 5 van de 86 onderzochte lokale politiezones in 2021 over een gezichtsherkenningsprogramma beschikten, waarvan er een beweert het "vaak tot zeer vaak" te gebruiken.[12]

In het Brussels Gewest gebruiken de politiezones software van het Israëlische bedrijf BriefCam[13] om met behulp van algoritmes beelden te analyseren van camera's in de Brusselse openbare ruimte en alle bewegende objecten (mensen, dieren, auto's enz.) uit een statische achtergrond te halen. BriefCam biedt ook gezichtsherkenningstechnologieën die compatibel zijn met een deel van het Brusselse cameranetwerk.

Ook politiezones Moeskroen en Kortrijk, Kuurne en Lendelede maken gebruik van de BriefCamtechnologie. In een onderzoek naar de videobewaking in Kortrijk schreef *Médor*: "RTS, dat een invoerlicentie heeft voor BriefCam en de software in Kortrijk installeerde, heeft destijds de gebruikersrechten voor gezichtsherkenning moeten uitschakelen. Die optie is automatisch beschikbaar. Volgens RTS "gaan hun leveranciers ervan uit dat iedereen gezichtsherkenning wil gebruiken".[14]

[2] Lore Rooseleers, Jeroen Maesschalck, Digitalisering in de lokale politie in Vlaanderen en Brussel: Waar staan we? Panopticon, 42 (5), pp. 419-438 ; https://www.researchgate.net/publication/355585410_Digitalisering_in_de_lokale_politie_in_Vlaanderen_en_Brussel_Waar_staan_we

[3] Facial Recognition Face Recognition for Safety, Security & Operational Efficiency | BriefCam

[4] Courtrai, reconnaissance faciale dans le viseur ? - Médor (medor.coop)

[12] Lore Rooseleers, Jeroen Maesschalck, Digitalisering in de lokale politie in Vlaanderen en Brussel: Waar staan we? Panopticon, 42 (5), pp. 419-438; https://www.researchgate.net/publication/355585410_Digitalisering_in_de_lokale_politie_in_Vlaanderen_en_Brussel_Waar_staan_we

[13] Facial Recognition Face Recognition for Safety, Security & Operational Efficiency | BriefCam

[14] Courtrai, reconnaissance faciale dans le viseur ? - Médor (medor.coop)

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."

Dans une étude de cas rédigée par l'entreprise Genetec[5], Christian Banken qui était alors coordinateur régional pour la sécurité au CIRB – Centre d'informatique pour la Région bruxelloise – disait à propos de Briefcam : "Notre prochaine étape sera l'intégration de la reconnaissance faciale et des plaques minéralogiques."

En résumé, il n'y a donc pas de frein "technique" au déploiement de la reconnaissance faciale. De plus, la volonté politique est forte, au niveau fédéral en particulier, sans qu'aucun débat public ne soit réellement mené. »

**Mme Nicha Mbuli** : « Pourquoi nous demandons l'interdiction de la reconnaissance faciale ?

*Des menaces réelles sur le droit à l'anonymat, à la liberté d'expression et un effet d'autocensure des comportements*

Le simple fait de se savoir observés affecte notre comportement et notre liberté. Être filmés, enregistrés, surveillés dans l'espace public constitue une atteinte à la vie privée et à la liberté individuelle. Cela impacte notre manière de nous comporter, de nous exprimer, de nous déplacer, d'agir, aussi dans l'espace public. La menace et la peur induites par les conséquences de la surveillance peuvent inhiber les comportements et, dans certains cas, entraîner un éloignement de l'espace public, pour toute une partie de la population. C'est ce que les juristes et chercheurs nomment le "*chilling effect*", que l'on peut traduire par "effet dissuasif", "effet paralysant" ou "d'auto-censure".

L'identification par la reconnaissance faciale restreint considérablement l'anonymat auquel on s'attend à pouvoir jouir même en public. L'usage de cette technologie dans nos rues nous rendraient potentiellement tous identifiables en permanence, en tout cas tous surveillés, voire suspects. En effet, cela revient à donner à nos autorités le pouvoir d'identifier l'intégralité de sa population simplement parce qu'elle est dans l'espace public.

Lors de manifestations, la surveillance musèle la liberté d'expression et limite les possibilités de se rassembler. La mise en place de technologies de reconnaissance faciale pourrait, par ailleurs, être utilisée à l'encontre de toutes les personnes qui se rassembleraient, s'associeraient ou manifesteraient des opinions dissidentes dans l'espace public, qu'il s'agisse de journalistes, d'avocats, de syndicalistes, de militants ou de simples citoyens.

Op 6 oktober 2021 zei federaal minister van Binnenlandse Zaken Annelies Verlinden in de commissie Binnenlandse Zaken van het federale parlement dat gezichtsherkenning een interessante nieuwigheid is die in de toekomst de werking van de politie tijdens administratieve en gerechtelijke opdrachten kan ondersteunen. Dat kan natuurlijk alleen als er een correcte wettelijke basis is om de verkregen informatie administratief en gerechtelijk geldig te gebruiken.

In een casestudy van Genetec[15] zei Christian Banken, destijds de gewestelijke beveiligingscoördinator bij het Centrum voor Informatica voor het Brussels Gewest (CIBG), over BriefCam dat hun volgende stap de combinatie van gezichts- en nummerplaatherkenning zal zijn.

Kortom, er staat dus geen technische rem op het gebruik van gezichtsherkenning. Bovendien staan met name federale beleidsmakers er sterk voor open zonder dat er een reëel openbaar debat over wordt gevoerd".

**Mevrouw Nicha Mbuli:** "Waarom vragen wij een verbod op gezichtsherkenning?

*Reëel risico voor het recht op anonimiteit en de vrijheid van meningsuiting en zelfcensurerend gedrag*

Als we weten dat we worden geobserveerd, heeft dat gevolgen voor ons gedrag en onze vrijheid. Als we in de openbare ruimte worden gefilmd, geregistreerd en bewaakt, is dat een inbreuk op ons privéleven en op de individuele vrijheid. Het beïnvloedt hoe we ons gedragen, ons uitdrukken, ons verplaatsen, handelen, ook in de openbare ruimte. De dreiging en de angst die het gevolg zijn van dat toezicht, kunnen ons afremmen en er in bepaalde gevallen toe leiden dat een aanzienlijk deel van de bevolking de openbare ruimte vermijdt. Juristen en onderzoekers noemen dat het chilling effect, wat als ontradend effect, verlammend effect of zelfcensuureffect kan worden vertaald.

Identificatie door gezichtsherkenning zet een aanzienlijke domper op de anonimiteit die we ook in de openbare ruimte verwachten te genieten. Door het gebruik van de technologie worden we allemaal potentieel permanent identificeerbaar en in ieder geval in de gaten gehouden of zelfs verdacht. Het komt er immers op neer dat we de overheid machtigen om de hele bevolking te identificeren wanneer ze zich in de openbare ruimte bevindt.

Tijdens demonstraties muilkorft het toezicht de vrijheid van meningsuiting en beperkt het de mogelijkheden om samen te komen. Gezichtsherkenningstechnologie kan ook worden gebruikt tegen iedereen die in de openbare ruimte samenkomt, zich verenigt of een afwijkende mening uit, of dat nu journalisten, advocaten, vakbondsleden, activisten of gewone burgers zijn.

[5] https://www.genetec.com/binaries/content/assets/genetec-nl/case-studies/fr-genetec-city-of-brussels-case-study.pdf
[15] https://www.genetec.com/binaries/content/assets/genetec-fr/case-studies/fr-genetec-city-of-brussels-case-study.pdf

*Des risques renforcés de discriminations*

Comme toute technologie, la reconnaissance faciale n'est pas neutre. En effet, des exemples concrets, en plus de nombreuses études sur la question, ont mis en lumière que les décisions algorithmiques de cette technologie peuvent être biaisées et déboucher sur des cas de discriminations raciales. Les études montrent que cette technologie reproduit les préjugés et biais sexistes ou racistes de ses concepteurs ainsi que les discriminations sexistes ou racistes induites par les conceptions sociales dominantes et des institutions qui les vendent et qui les utilisent.[6]

Ces erreurs, dues notamment à une présence disproportionnée d'hommes blancs dans les bases de données utilisées pour "entraîner" les logiciels, peuvent entraîner des "faux positifs" et identifier erronément une personne. Les bases de données utilisées pour entraîner les logiciels de reconnaissance faciale constituent donc l'un des problèmes majeurs en matière de discrimination raciale.

Dans son avis relatif à une proposition de résolution pour la mise en place d'un moratoire[7], le COC mentionne notamment "les problèmes de qualité inhérents de la technologie de reconnaissance faciale".

On peut lire : "La littérature, les avis de l'EDPS (*European Data Protection Supervisor*) et de l'EDPB (*European Data Protection Board*) et les constatations propres du COC (dans le dossier de l'utilisation de la reconnaissance faciale à l'aéroport de Bruxelles-National p.ex.) nous apprennent que l'exactitude et la pertinence de la technologie de reconnaissance faciale posent encore de nombreux problèmes. L'absence d'évaluations indépendantes est une pierre d'achoppement connue. Les faux positifs et faux négatifs sont nombreux et des problèmes connus sont ceux qui se posent avec les personnes de couleur de peau foncée, portant une barbe et des lunettes, etc. Le COC ne constate que peu d'améliorations rassurantes sur ce plan."

Le recours à la reconnaissance faciale reproduit les discriminations raciales ayant cours dans notre société et contribue à les amplifier. Les préjugés et pratiques, comme le profilage ethnique, peuvent être intégrés dans le système, renforçant ainsi les discriminations tout en faisant perdurer lesdits préjugés.

Cette technologie induit aussi un renforcement des discriminations raciales du fait d'une surreprésentation, dans les bases de données policières, des groupes de personnes historiquement marginalisées et criminalisées. Elles subissent, de ce fait, des formes de violences et/ou de discrimination de la part des institutions, tels que des traitements policiers ou judiciaires injustifiés et

*Verhoogd risico op discriminatie*

Net als elke andere technologie is gezichtsherkenning niet neutraal. Uit concrete voorbeelden en talloze studies over de kwestie is naar voren gekomen dat de algoritmische beslissingen van de technologie bevooroordeeld kunnen zijn en tot rassendiscriminatie kunnen leiden. Studies tonen aan dat de technologie de seksistische of racistische vooroordelen van haar ontwerpers weerspiegelt, evenals de seksistische of racistische discriminatie die veroorzaakt wordt door dominante maatschappelijke opvattingen en de instellingen die ze verkopen en gebruiken.[16]

Die fouten, die vooral te wijten zijn aan de onevenredige aanwezigheid van blanke mannen in de databases die gebruikt worden om de software te "trainen", kunnen leiden tot "valse positieven" en een onjuiste identificatie van een persoon. De databases die gebruikt worden voor gezichtsherkenningssoftware zijn daarom een van de grootste problemen als het gaat om rassendiscriminatie.

In zijn advies over een voorstel van resolutie betreffende het instellen van een moratorium[17], noemt het COC "de inherente kwaliteitsproblemen van de gezichtsherkenningstechnologie (Facial recognition technology - FRT)".

Hierin staat: "Uit de literatuur, de adviezen van de EDPS (*European Data Protection Supervisor*) en EDPB (*European Data Protection Board*) en de eigen bevindingen van het COC (in de zaak van het gebruik van FRT op Brussels Airport bijvoorbeeld) weten we dat er nog heel wat problemen zijn met de juistheid en accuraatheid van FRT. Het gebrek aan onafhankelijke evaluaties is gekend probleem. Het aantal valse positieven en valse negatieven blijkt groot en er zijn problemen bij mensen met een donkere huidskleur, baarden en brillen, enz. Vooralsnog ziet het COC weinig geruststellende signalen."

Door het gebruik van gezichtsherkenning wordt de raciale discriminatie die in onze samenleving heerst, gereproduceerd en zelfs uitvergroot. Vooroordelen en praktijken, zoals etnische profilering, kunnen in het systeem worden ingevoerd, waardoor de discriminatie toeneemt en vooroordelen blijven bestaan.

De technologie zorgt ook voor meer rassendiscriminatie doordat historisch gemarginaliseerde en gecriminaliseerde groepen oververtegenwoordigd zijn in politiedatabases. Hierdoor worden ze het slachtoffer van vormen van geweld en/of discriminatie door de instellingen, zoals een ongerechtvaardigde en discriminerende behandeling door politie of justitie. Die vooroordelen, in combinatie met het

[6] Williams, P. and E. Kind, Data-driven policing: The hardwiring of discriminatory policing practices across Europe, ENAR, 2019.

[7] Avis relatif à une 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 (DOC 55 1349/001 du 16 juin 2020) https://www.organedecontrole.be/files/DA210029_Avis_F.pdf

[16] Williams, P. and E. Kind, Data-driven policing: The hardwiring of discriminatory policing practices across Europe, ENAR, 2019.

[17] Advies betreffende een voorstel van resolutie over een driejarig moratorium op het gebruik van gezichtsherkenningssoftware en – algoritmen in vaste of mobiele beveiligingscamera's in openbare en privéplaatsen (DOC 55 1349/001 van 16 juni 2020) https://www.controleorgaan.be/files/DA210029_Advies_N.pdf

discriminants. Ces biais, associés au pourcentage d'erreurs plus important commis par les technologies, dans le cas des femmes et des personnes de couleur, augmentent le risque d'arrestation et de détention d'innocents. »

**Mme Joke Blockx** : « Je vais m'arrêter sur deux risques liés à la reconnaissance faciale.

*Risque de glissement et de détournement des finalités*

On constate que souvent, une technologie introduite – par un parlement – dans un but précis en vient à être utilisée à d'autres fins par le pouvoir exécutif. Ce glissement de finalité - ou *function creep* – constitue un risque inhérent à l'introduction de toute nouvelle technologie. Il importe d'en tenir compte, car cela implique une perte du contrôle démocratique du pouvoir législatif et, par extension, de l'ensemble de la population.

On a déjà vu de nombreux exemples d'un tel glissement de finalité :

- Des caméras permettant de reconnaître les plaques d'immatriculation (caméras ANPR) ont été installées à l'appui de la zone de basses émissions (LEZ) ; elles sont à présent utilisées pour sanctionner automatiquement les contrevenants au code de la route.

- La pandémie a également accéléré l'utilisation de certaines technologies. Pendant la pandémie, divers dispositifs de surveillance ont été utilisés dans l'espace public bruxellois (par exemple, l'utilisation de drones par la police) afin de contrôler le comportement des personnes et de s'assurer que des mesures sanitaires étaient prises pour lutter contre le Covid-19, ce qui a donné lieu à des sanctions judiciaires et à des violences policières.

Pendant la pandémie, les caméras de sécurité utilisées pour protéger le quartier juif d'Anvers ont servi à contrôler le respect des mesures[8].

C'est extrêmement pertinent lorsqu'une technologie est testée dans le cadre d'un projet pilote. Les projets pilotes sont souvent mis sur pied dans les zones grises de la loi. Des technologies de surveillance sont installées à grande échelle dans notre espace public avant l'adoption des cadres légaux qui les régulariseront ultérieurement. À long terme, cela peut avoir pour effet de normaliser la surveillance de masse.

Là aussi, il y a déjà des exemples. Ainsi, en novembre, on a annoncé un projet pilote portant sur l'usage de caméras ANPR pour sanctionner l'utilisation du GSM au volant.

hogere percentage fouten dat door de technologieën wordt gemaakt in het geval van vrouwen en mensen van kleur, verhogen het risico dat onschuldigen worden gearresteerd en vastgehouden."

**Mevrouw Joke Blockx**: "Ik ga het over twee risico's van gezichtsherkenning hebben.

*Risico op doelverschuiving en misbruik*

We zien dat wanneer een parlement met een bepaald doel een technologie invoert, de uitvoerende macht die achteraf vaak voor andere doeleinden gebruikt. Dat heet doelverschuiving - of *function creep* - en is een inherent risico bij de invoer van elke nieuwe technologie. Het is belangrijk om daar rekening mee te houden omdat het een verlies van democratische controle door de wetgevende macht, en bij uitbreiding de gehele bevolking, inhoudt.

We hebben al heel wat voorbeelden van zo'n doelverschuiving gezien:

- Camera's voor nummerplaatherkenning (ANPR-camera's) om de lage-emissiezone (LEZ) te controleren, worden nu gebruikt om verkeersovertreders automatisch te straffen.

- De pandemie heeft het gebruik van bepaalde technologieën versneld. Tijdens de pandemie werden verschillende bewakingsapparaten gebruikt in de Brusselse openbare ruimte (bv. politiedrones) om het gedrag van mensen in de gaten te houden en ervoor te zorgen dat er gezondheidsgerelateerde maatregelen werden genomen om covid-19 te bestrijden, wat leidde tot gerechtelijke sancties en politiegeweld.

Beveiligingscamera's die werden gebruikt om de Joodse wijk in Antwerpen te beschermen, werden tijdens de pandemie gebruikt om de naleving van de maatregelen te controleren[18].

Dat is uitermate relevant wanneer een technologie wordt getest aan de hand van een proefproject. Proefprojecten worden vaak opgezet in de grijze zones van de wet. Op grote schaal worden bewakingstechnologieën in onze publieke ruimte geïnstalleerd, nog voor er een wettelijk kader. Dit kan er op lange termijn toe leiden dat massasurveillance wordt genormaliseerd.

Daar zijn ook al voorbeelden van. Zo werd in november een proefproject aangekondigd waarbij ANPR-camera's zouden worden ingezet om gsm-gebruik achter het stuur te bestraffen.

[8] Camera's in joodse wijk controleren nu synagogegangers", 13 mars 2021, https://www.standaard.be/cnt/dmf20210312_98151173

[18] Camera's in joodse wijk controleren nu synagogegangers", 13 mars 2021, https://www.standaard.be/cnt/dmf20210312_98151173

*Trop peu de contrôle indépendant*

Des organes de contrôle forts et indépendants protègent nos droits démocratiques contre les abus des pouvoirs publics. Mais le bât blesse, là aussi.

Des chercheurs comme Rosamunde Van Brakel[9], titulaire de la chaire d'études sur la surveillance à la VUB, soulignent les limites des organes de surveillance tels que le COC, qui s'expliquent notamment par le mandat restreint du COC : "Bien que le COC obtienne quelques résultats en ce qui concerne la cessation de pratiques illégales, la portée limitée de son mandat ouvre la porte à bon nombre des questions sociales et éthiques liées à la surveillance policière algorithmique.". Les pratiques manifestement illégales peuvent donc être stoppées. Mais il n'y a pas de débat sur l'impact social de ce type de technologies.

Mme Van Brakel qualifie les effets sociaux et éthiques de la surveillance policière algorithmique de "préjudice sociotechnique". "Le préjudice est sociotechnique dans le sens où il est dû à une conjonction de structures sociales existantes et de technologie. Il est de plus en plus prouvé que l'utilisation de la surveillance algorithmique par la police est discriminatoire à l'égard des groupes vulnérables de la société et qu'elle présente des risques pour les droits de l'homme en général."

Si les organes de surveillance ne sont pas à la hauteur, il est d'autant plus important que nos députés jouent leur rôle de contrôle. En outre, le parlement est le lieu par excellence pour débattre de l'impact sociétal des technologies de surveillance. On ne saurait dès lors sous-estimer l'importance d'une action du Parlement bruxellois. »

**Mme Nicha Mbuli** : « Le manque d'expertise des services de police est également une raison pour laquelle nous militons pour l'interdiction de la reconnaissance faciale.

À Bruxelles et en Belgique, où se trouvent les institutions européennes et le siège de l'OTAN et de nombreuses institutions, un aspect alarmant est le manque d'expertise des services de police.

Dans la pratique, le COC constate d'ailleurs trop souvent que les collaborateurs de terrain de la GPI ne sont pas suffisamment, voire pas du tout en mesure d'expliquer le fonctionnement des moyens technologiques qu'ils utilisent, voire ne le comprennent pas vraiment eux-mêmes. C'est déjà le cas pour les traitements actuels "ordinaires" des caméras, et ce problème ne fera que s'aggraver avec l'introduction de systèmes de reconnaissance faciale complexes recourant à des algorithmes.

*Te weinig onafhankelijk toezicht*

Sterke, onafhankelijke toezichtsorganen beschermen onze democratische rechten tegen misbruik door de overheid. Maar ook daar wringt het schoentje.

Onderzoekers zoals Rosamunde Van Brakel[19], die de leerstoel surveillancestudies aan de VUB bekleedt, wijzen op de beperkingen van toezichtsorganen zoals het COC, die het gevolg zijn van het beperkte mandaat van het COC: "Hoewel het COC erin slaagt om een aantal illegale praktijken stop te zetten, laat de beperkte reikwijdte van zijn mandaat ruimte voor tal van sociale en ethische kwesties die bij algoritmisch politiesurveillance komen kijken.". Wat flagrant illegaal is, kan dus worden gestopt, maar er worden geen debatten gevoerd over de maatschappelijke impact van dat soort technologieën.

Mevrouw Van Brakel noemt de sociale en ethische effecten van algoritmische politiesurveillance "sociaal-technische schade". "Ze is sociaal-technisch in de zin dat de schade wordt veroorzaakt door een samenspel van bestaande sociale structuren en technologie. Er is steeds meer bewijs dat het gebruik van algoritmische surveillance door de politie discriminerend is voor kwetsbare groepen in de samenleving en risico's met zich meebrengt voor de mensenrechten in het algemeen."

Wanneer toezichtsorganen tekortschieten, is het nog belangrijker dat onze volksvertegenwoordigers hun controlerol spelen. Daarenboven is het parlement bij uitstek de plek om over de maatschappelijke impact van surveillancetechnologie te debatteren. Het belang van actie door het Brussels Parlement kan dus niet onderschat worden.".

**Mevrouw Nicha Mbuli**: "Het gebrek aan expertise bij de politiediensten is nog een reden waarom we actie voeren voor een verbod op gezichtsherkenning.

In Brussel en België, waar de Europese instellingen, de hoofdzetel van de NAVO en vele andere instellingen gevestigd zijn, is het gebrek aan expertise bij de politie alarmerend.

Het COC merkt in de praktijk maar al te vaak dat de medewerkers van de GPI niet of onvoldoende in staat zijn om uit te leggen hoe de technologie die ze gebruiken werkt, of die zelfs niet eens begrijpen. Dit is al het geval bij de huidige "gewone" camerabewerking, en het probleem zal alleen maar ernstiger worden met de komst van complexe gezichtsherkenningssystemen gebaseerd op algoritmen.

[9] Van Brakel, R. (2021). How to watch the watchers? Democratic oversight of algorithmic police surveillance in Belgium. surveillance and society, 19(2), 228-240. https://doi.org/10.24908/ss.v19i2.14325

[19] Van Brakel, R. (2021). How to watch the watchers? Democratic oversight of algorithmic police surveillance in Belgium. surveillance and society, 19(2), 228-240. https://doi.org/10.24908/ss.v19i2.14325

Dans son avis relatif à une proposition de résolution pour la mise en place d'un moratoire de trois ans, le COC écrit : "Un autre aspect important réside dans les connaissances et le savoir-faire dont dispose la GPI elle-même. Le COC n'est à ce stade nullement rassuré à ce sujet. Il existe au sein de la GPI en général un réel problème d'expertise (connaissances juridiques élémentaires, expertise en technologies de l'information, aptitude numérique, etc.). [...] force est d'admettre que la formation qui est dispensée en Belgique est minimale et ne souffre souvent pas la comparaison avec ce qui se fait à l'étranger [...]."

*Des risques de fuites et de piratage informatiques*

L'usage de la reconnaissance faciale suppose la constitution et l'utilisation de banques de données biométriques collectant des "templates" ou "gabarits" propres à chaque visage. Or, la création de telles bases de données implique un risque réel de piratage dont les conséquences peuvent être irrémédiables pour les personnes concernées.

Au Royaume-Uni, 28 millions d'enregistrements représentant un total de plus de 23 gigaoctets ont été publiés sur internet après l'exploitation d'une faille d'une solution de l'entreprise Suprema, dont les clients sont notamment la Metropolitan Police, des entreprises de défense et des banques dans 83 pays. Outre des noms d'utilisateur et des mots de passe non cryptés, des registres d'accès aux installations, des niveaux de sécurité et des habilitations, les données exposées concernaient aussi les empreintes digitales et les enregistrements de reconnaissance faciale de millions de personnes. En plus du risque de manipulation des systèmes de contrôle d'accès de sites sécurisés, les observateurs ont souligné que le problème le plus grave résidait dans l'accès à des données biométriques qui ne peuvent par nature être modifiées.

En novembre 2022, les services de police belges aussi faisaient l'objet d'un piratage informatique, avec énormément de données sensibles divulguées et de graves conséquences. Un pirate visait la zone de police de Zwijndrecht en province d'Anvers et publiait des milliers de plaques d'immatriculation, des amendes pour excès de vitesse ainsi que des procès-verbaux, avec les photos de victimes de violences intrafamiliales notamment. Le piratage concernait des données pour la période allant de 2006 à septembre 2022.[10]

Nous rappelons un élément fondamental du débat : on peut facilement changer son mot de passe, pas son visage ! »

**M. Rémy Farge** : « Nous considérons que Bruxelles peut être une ville et une Région exemplaires.

En raison des risques très importants qu'entraînerait l'usage de la reconnaissance faciale dans l'espace public bruxellois, nous pensons qu'une transparence totale sur les

In zijn advies betreffende een voorstel van resolutie over het instellen van een driejarig moratorium, schreef het COC: "Een ander belangrijk aspect is de kennis en knowhow bij de GPI zelf. Op dat vlak is het COC helemaal niet gerustgesteld. Er is bij de GPI in het algemeen een reëel expertiseprobleem (juridische basiskennis, IT-expertise, digitale vaardigheden, enz.). […] we kunnen gerust stellen dat de Belgische opleiding minimaal is en de vergelijking met het buitenland vaak niet kan doorstaan […]."

*Risico's op lekken en hacking*

Het gebruik van gezichtsherkenning impliceert de aanleg en het gebruik van biometrische databanken die sjablonen of profielen verzamelen die specifiek zijn voor elk gezicht. Dergelijke databanken brengen echter een reëel risico op hacking met zich, waarvan de gevolgen onherstelbaar kunnen zijn voor de personen in kwestie.

In het Verenigd Koninkrijk zijn 28 miljoen gegevens, goed voor in totaal ruim 23 gigabyte, op het internet beland door toedoen van hackers die gebruikmaakten van een veiligheidslek in een softwaresysteem ontwikkeld door Suprema, dat onder meer de Metropolitan Police, defensiebedrijven en banken uit 83 landen onder zijn klanten mag rekenen. De gelekte gegevens bevatten niet alleen gebruikersnamen en niet-versleutelde wachtwoorden, toegangsregisters voor apparatuur, veiligheidsniveaus en machtigingen, maar ook vingerafdrukken en gezichtsherkenningsopnamen van miljoenen mensen. Naast het risico dat er met toegangscontrolesystemen voor beveiligde locaties geknoeid kan worden, vonden waarnemers de toegang tot biometrische gegevens het grootste probleem, omdat die per definitie niet gewijzigd kunnen worden.

In november 2022 waren ook de Belgische politiediensten het slachtoffer van hacking, waarbij grote aantallen gevoelige gegevens verspreid raakten, met zware gevolgen. Een hacker had het op de politiezone Zwijndrecht in de provincie Antwerpen gemunt en publiceerde duizenden nummerplaten, snelheidsboetes en processen-verbaal met foto's van slachtoffers van huiselijk geweld. De gegevens hadden betrekking op de periode van 2006 tot september 2022.[20]

Wij wijzen op een fundamenteel aspect van het debat: je wachtwoord kun je gemakkelijk aanpassen, je gezicht niet!"

**De heer Rémy Farge**: "Wij zijn van mening dat Brussel een modelstad en -gewest kan worden.

Gezien de grote risico's verbonden aan het gebruik van gezichtsherkenning in de openbare ruimte in Brussel, achten

[10] Le Soir, 24.11.2022 - L'une des plus grandes fuites de données publiques en Belgique: une zone de police piratée, des milliers de PV et amendes en ligne https://www.lesoir.be/479150/article/2022-11-24/lune-des-plus-grandesfuites-de-donnees-publiques-en-belgique-une-zone-de-police

[20] Le Soir, 24.11.2022 - L'une des plus grandes fuites de données publiques en Belgique: une zone de police piratée, des milliers de PV et amendes en ligne https://www.lesoir.be/479150/article/2022-11-24/lune-des-plus-grandesfuites-de-donnees-publiques-en-belgique-une-zone-de-police

projets en cours est nécessaire.

D'autres villes ont pris une mesure forte pour protéger leurs citoyens : on cite souvent la ville de San Francisco, mais à quelques centaines de kilomètres de Bruxelles, Saint-Gall, Zurich et Lausanne, trois villes suisses, ont pris des mesures très fortes contre l'usage de la reconnaissance faciale dans l'espace public.

Nous appelons le Parlement bruxellois :

1. à adopter une résolution s'engageant à faire respecter les bases légales interdisant l'utilisation de la reconnaissance faciale par les autorités publiques régionales et la police ;

2. à contrôler effectivement et suivre le respect de la résolution ; à clarifier en outre s'il existe des fichiers biométriques constitués au sein des zones de police bruxelloises, notamment à des fins de maintien de l'ordre ; à mandater la commission de contrôle bruxelloise ou tout autre organe de contrôle compétent qui pourrait être chargé d'effectuer ce contrôle in concreto ; à réitérer à intervalle régulier le contrôle du respect de l'interdiction des technologies de surveillance biométrique et à rendre publics les avis de la commission de contrôle bruxelloise, afin d'assurer une meilleure transparence et d'augmenter la confiance des citoyens ;

3. à exercer pleinement sa compétence de contrôle du respect du cadre actuel sur le sol bruxellois ; à effectuer un contrôle de la plateforme de mutualisation des images de vidéosurveillance, et à 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 et à s'assurer auprès des autorités et organes de contrôle compétents qu'aucune base légale ne permet l'utilisation de la reconnaissance faciale, aussi pour des missions de police judiciaire ;

4. à faire toute la transparence sur :

- les pratiques et usages précis, les logiciels utilisés, le monitoring effectué ;

- 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. »

wij volledige transparantie over de lopende projecten noodzakelijk.

Andere steden hebben krachtig ingegrepen om hun burgers te beschermen: vaak wordt verwezen naar San Francisco, maar op enkele honderden kilometers van Brussel hebben drie Zwitserse steden (Sankt Gallen, Zürich en Lausanne) verregaande maatregelen genomen tegen het gebruik van gezichtsherkenning in de openbare ruimte.

Wij roepen het Brussels Parlement op:

1. een resolutie goed te keuren met de verbintenis om respect af te dwingen voor de wettelijke bepalingen die het gebruik van gezichtsherkenning door de gewestelijke overheden en door de politie verbieden;

2. de naleving van die resolutie effectief op te volgen en te controleren; na te gaan of er biometrische bestanden zijn aangelegd bij de Brusselse politiezones, met name voor de ordehandhaving; de Brusselse Controlecommissie of eender welke andere bevoegde controle-instantie te machtigen om die controle effectief uit te voeren; de naleving van het verbod op biometrische surveillancetechnologieën regelmatig opnieuw te controleren; en de adviezen van de Brusselse Controlecommissie bekend te maken, om zo de transparantie en het vertrouwen van de burgers te vergroten;

3. zijn bevoegdheid om de naleving van de wetgeving op het Brusselse grondgebied te controleren, ten volle uit te oefenen; controle uit te oefenen op het gewestelijke platform voor het bundelen van videobewakingsbeelden en na te gaan of er achteraf geen enkele 'matching' (het vinden van overeenstemming via gezichtsherkenningssoftware) wordt uitgevoerd op basis van de beelden gedeeld op dat platform; en tegenover de bevoegde overheden en controle-instanties te benadrukken dat er geen wettelijke basis bestaat voor het gebruik van gezichtsherkenning, ook niet voor opdrachten van de gerechtelijke politie;

4. volledige transparantie te geven over:

- de precieze praktijken en gebruiken, de gebruikte softwaretoepassingen, de uitgevoerde monitoring;

- de overheidsopdrachten, om ervoor te zorgen dat geen financiering wordt toegekend aan de ontwikkeling van biometrische bestanden of van technologieën waarmee biometrische surveillance kan worden uitgevoerd op het grondgebied van het Brussels Hoofdstedelijk Gewest;

- de lijst van de onderaannemers, dienstverleners en bedrijven, op gewestelijk en federaal niveau, die betrokken zijn bij de (gebundelde) videobewaking in Brussel. »

## III. Échange de vues

**M. Hicham Talhi** remercie les coauteurs de la pétition pour leur présentation. Il estime que la rapidité avec laquelle plus de 1.000 signatures ont été récoltées démontre l'intérêt des Bruxellois et des Bruxelloises sur cet enjeu crucial. Il est rappelé, à juste titre, la responsabilité du législateur, aussi en tant que contrôleur du cadre légal.

Il a été exposé combien le cadre légal peut rapidement ne pas être respecté sous des prétextes d'opportunités ou à l'occasion du renouvellement d'un marché public, ou simplement pour des raisons pragmatiques d'augmentation de l'efficacité.

Dans le cadre de cette commission, on a déjà entendu des interpellations au ministre-président, auquel la sixième réforme de l'État a conféré une compétence de coordination, sur le non-usage de l'intelligence artificielle.

Des éléments ont été pointés sur les dérives potentielles de cette intelligence, qui n'est pas neutre et qui comporte effectivement une série de biais intégrés dans les algorithmes, qui ne sont pas neutres. Ceux-ci mènent à une discrimination des personnes vulnérables et, en l'occurrence, des personnes de couleur pour qui l'identification se fait de manière erronée. Il est donc important d'y accorder une attention toute particulière.

Il indique encore que son groupe a soutenu la résolution concernant l'intelligence artificielle au Parlement européen, qui sera votée le mois prochain.

Par ailleurs, il rejoint les coauteurs de la pétition sur l'ensemble des éléments qu'ils ont évoqués sur les libertés fondamentales et qui sont non négociables, quel que soit le prétexte utilisé pour implémenter des logiciels d'intelligence artificielle.

Pour ceux qui pensent que l'intelligence artificielle concerne un futur très très lointain, il explique qu'aujourd'hui, en Chine, il existe déjà un système de contrôle social à points, qui a des conséquences directes pour la vie de milliards de citoyens à qui il est interdit de voyager, qui voient leur image affichée en public, qui reçoivent des appels intempestifs parce qu'ils n'auraient pas honoré une dette, pas payé une amende ou pas traversé sur un passage pour piétons. Ce n'est certainement pas le type de système qu'il souhaite pour Bruxelles

Il estime qu'une audition de la commission de contrôle bruxelloise pourrait être intéressante, dès lors qu'elle a dans ses missions le contrôle du traitement des échanges d'images des caméras de surveillance dans le cadre de la mutualisation des services régionaux.

Enfin, il souligne que les technologies d'intelligence artificielle sont déjà implémentées aujourd'hui dans toute une série de domaines. Il estime, au vu du fait que les forces de l'ordre font utilisent de façon massive la banque de données

## III. Gedachtewisseling

**De heer Hicham Talhi** dankt de mede-indieners van de petitie voor hun uiteenzetting. Hij is van mening dat de snelheid waarmee meer dan 1.000 handtekeningen zijn verzameld, de belangstelling van de Brusselaars voor deze essentiële kwestie aantoont. Terecht wordt gewezen op de verantwoordelijkheid van de wetgever, ook als controleur van het wettelijk kader.

Er is uitgelegd hoe snel dat wettelijk kader met de voeten getreden kan worden wegens de zogenaamde kansen die niet-naleving biedt, bij de verlenging van een overheidsopdracht of gewoon uit pragmatische overwegingen van efficiëntiewinst.

Tijdens vergaderingen van deze commissie werden al interpellaties over de niet-toepassing van artificiële intelligentie gericht aan de minister-president in het kader van de coördinatiebevoegdheid waarover hij als gevolg van de zesde staatshervorming beschikt.

Er zijn mogelijke problemen met deze niet-neutrale technologie aangehaald, waarvan de niet-neutrale algoritmen een aantal vooroordelen bevatten. Ze leiden tot discriminatie van kwetsbare personen en meer bepaald van mensen van kleur, bij wie de identificatie vaak misloopt. Dat vergt bijzondere aandacht.

Hij voegt eraan toe dat zijn fractie de resolutie over artificiële intelligentie die volgende maand in het Europees Parlement ter stemming wordt voorgelegd, heeft gesteund.

Hij is het op alle punten met de mede-indieners van de petitie eens wat de fundamentele vrijheden betreft, die niet voor onderhandeling vatbaar zijn, ongeacht de redenen die worden ingeroepen om software voor artificiële intelligentie in te zetten.

Diegenen die zouden denken dat artificiële intelligentie verre toekomstmuziek is, wijst hij op het in China reeds bestaande puntensysteem voor sociale controle, dat rechtstreekse impact heeft op het leven van miljarden burgers, die bijvoorbeeld niet meer mogen reizen, hun foto in het openbaar zien uithangen of storende telefoontjes krijgen in verband met een openstaande schuld, een niet-betaalde boete of omdat ze niet via het zebrapad zijn overgestoken. Dat is zeker niet wat hij voor Brussel wenst.

Hij is van mening dat een hoorzitting met de Brusselse Controlecommissie interessant kan zijn, aangezien tot haar taken het toezicht behoort op de verwerking van de videobewakingsbeelden die worden uitgewisseld tussen de verschillende gewestelijke diensten.

Tot slot benadrukt hij dat technologie voor artificiële intelligentie vandaag al in een heel aantal domeinen wordt gebruikt. Gelet op het feit dat de ordediensten de algemene nationale gegevensbank (ANG) massaal gebruiken, is hij

nationale, qu'on ne peut faire confiance à un cadre légal. Il faut donc empêcher la compilation de données de façon généralisée. En tout cas, le fait qu'il faille une résolution en la matière démontre à quel point chacun doit être vigilant par rapport à cette matière.

**Mme Dominique Dufourny** indique que son groupe reconnaît la sensibilité et la complexité du sujet. L'utilisation des technologies de pointe pour des questions de sécurité soulève toujours des interrogations, mais aussi des inquiétudes qui sont légitimes et qui doivent être traitées. Ce fut le cas pour la vidéosurveillance lors de sa « normalisation » et c'est aujourd'hui le cas pour les nouvelles technologies telles que le recours aux bodycams pour le personnel policier opérationnel ou encore l'usage de logiciels de reconnaissance faciale par la police fédérale et les zones de police.

S'il est vrai que ce débat doit s'inviter dans toutes les assemblées du pays, il faut préciser que ce dossier relève d'autres niveaux de pouvoir : l'UE et le fédéral.

L'UE s'est saisie de la question plus large de l'usage des formes d'intelligence artificielle à des fins de sécurité. Selon les travaux de ces institutions, la technologie de reconnaissance faciale n'est pas à exclure purement et simplement, mais elle doit être encadrée et limitée à des situations spécifiques. Il est question de sécurité nationale, de l'existence d'un danger pour les infrastructures sensibles ou encore de questions de santé.

L'usage de cette technologie à des fins répressives ne constitue donc pas la norme, mais il reste possible moyennant certaines conditions et garanties, comme la nature de la situation ou encore les conséquences de l'utilisation du système pour les droits et libertés de toutes les personnes concernées.

L'organe de contrôle de l'information policière rappelle que « c'est sur cette base que les États membres peuvent prévoir la possibilité d'autoriser totalement ou partiellement l'utilisation susmentionnée de systèmes biométriques. Ce qui signifie que la Belgique pourrait prévoir des dispositions plus restrictives ou plus strictes dans son propre droit national. »

Le fédéral s'est saisi de cette question, puisque des travaux sont en cours pour discuter d'un fondement juridique qui apportera les garanties nécessaires et qui permettra d'éviter les dérives ou les polémiques qu'on a connues par le passé. Une commission consultative éthique « sécurité » a été mise en place et des débats ont lieu à la Chambre des représentants.

Pour en témoigner, nous pouvons reprendre les déclarations de la ministre de l'Intérieur, qui indique que « la reconnaissance faciale est certainement une piste intéressante à exploiter à terme pour soutenir le fonctionnement de la police dans l'exercice des missions de police administrative et judiciaire. Bien entendu, cela n'est possible qu'avec une base juridique correcte, afin que les informations obtenues puissent être utilisées de manière juridiquement valable. »

van mening dat een wettelijk kader geen garantie biedt. We moeten dus voorkomen dat gegevens op veralgemeende wijze worden verzameld. Het feit dat in deze kwestie een resolutie nodig is, toont alvast aan hoe waakzaam we daaromtrent moeten zijn.

**Mevrouw Dominique Dufourny** laat verstaan dat haar fractie erkent hoe gevoelig en complex dit onderwerp is. Het gebruik van spitstechnologie voor veiligheidsdoeleinden roept altijd vragen en bezorgdheden op, die legitiem zijn en een antwoord verdienen. Dat was het geval toen videobewaking "genormaliseerd" werd, en is vandaag het geval voor nieuwe technologieën zoals het gebruik van bodycams door politiepersoneel of het gebruik van gezichtsherkenningssoftware door de federale politie en de politiezones.

Hoewel het goed is dat elk parlement van dit land dit debat voert, moeten we erop wijzen dat dit dossier tot de bevoegdheid van andere bestuursniveaus behoort, namelijk de Europese Unie en de federale overheid.

De Europese Unie heeft zich gebogen over de ruimere kwestie van het gebruik van artificiële intelligentie met veiligheidsdoeleinden. Volgens de werkzaamheden van de EU-instellingen mogen we gezichtsherkenningstechnologie niet zonder meer verbieden, maar moeten we ze reguleren en enkel in specifieke situaties gebruiken, zoals ter bescherming van de nationale veiligheid of de veiligheid van gevoelige infrastructuur, of om gezondheidsredenen.

Het gebruik van die technologie voor handhaving is dus niet de norm, maar blijft mogelijk onder bepaalde voorwaarden en met bepaalde garanties, die verband houden met de aard van de situatie of de gevolgen van het gebruik van het systeem voor de rechten en vrijheden van de betrokken personen.

Het Controleorgaan op de Politionele Informatie (COC) wijst erop dat "de lidstaten op deze basis in de mogelijkheid kunnen voorzien om het bovenvermelde gebruik van biometrische systemen geheel of gedeeltelijk toe te staan. Dat betekent dat België restrictievere of strengere bepalingen in zijn eigen nationale recht mag opnemen."

De federale overheid is met de kwestie bezig, want er lopen momenteel werkzaamheden om te bekijken welke rechtsgrond de nodige garanties kan bieden en misbruiken en polemieken kan voorkomen zoals we die in het verleden gekend hebben. Er is een ethische adviescommissie "veiligheid" opgericht en er hebben debatten plaatsgevonden in de Kamer van Volksvertegenwoordigers.

Daarvan getuigen de volgende verklaringen van de minister van Binnenlandse Zaken: "Gezichtsherkenning is zeker een interessante mogelijkheid die we op termijn kunnen gebruiken om de politie te ondersteunen bij de uitvoering van haar administratieve en gerechtelijke taken. Dat is uiteraard enkel mogelijk met een correcte juridische basis, opdat de verkregen informatie op een rechtsgeldige manier kan worden gebruikt."

Dans le même esprit, le secrétaire d'État Mathieu Michel ajoute qu'il doit y avoir en Belgique un changement de paradigme en matière d'utilisation des caméras intelligentes. Il précise qu'« actuellement, tout ce qui n'est pas interdit est autorisé. Or, de plus en plus de technologies débarquent sans même qu'on ait pu imaginer leurs effets. Après débat à la Chambre, la loi devra déterminer une série d'utilisations autorisées pour ces technologies. Tout le reste devra être interdit. »

L'ensemble de ces déclarations publiques tendent à prouver qu'il existe une prise de conscience sur les risques encourus avec l'usage des technologies comme la reconnaissance faciale, mais qu'il peut aussi exister une façon de travailler en garantissant les droits et libertés de chacun. C'est pourquoi il importe de cibler l'utilisation de ce type d'outils, qui présentent un réel avantage dans la gestion de certains événements.

Il semble donc prématuré de soutenir sans nuance les demandes de pétitionnaires qui visent surtout à interdire purement et simplement le déploiement des technologies de reconnaissance faciale dans les lieux publics et leur utilisation par les autorités à des fins d'identification, alors même que des réflexions ont lieu pour déterminer un cadre normatif clair, précis et transparent, en ce compris en cas d'usage de la reconnaissance faciale à des fins répressives.

On peut craindre que le processus soit ralenti si on multiplie les instances de débat et si on refait à la Région, ce qui est fait au fédéral.

Notons que les contacts avec les services de terrain tendent à prouver que ces techniques présentent bien des avantages et constitueraient une réelle plus-value dans le travail policier sous certaines conditions. Ce sont donc ces mêmes services qui appellent nos autorités à légiférer pour disposer de règles strictes et connues de tous.

Enfin, pour la clarté du propos, il serait bon d'entendre les auteurs sur leurs demandes spécifiques. Dans leur introduction, il est question des caméras de la zone de basses émissions. Cela signifie-t-il une remise en cause de l'ensemble des technologies de reconnaissance en Région bruxelloise ? Ou vise-t-on plus spécifiquement la reconnaissance faciale ? Qu'est-il attendu de safe.brussels, compte tenu des compétences régionales limitées en la matière ?

**Mme Fadila Laanan** remarque que l'utilisation de la reconnaissance faciale dans l'espace public a des effets graves sur l'exercice des droits humains et sur les libertés fondamentales. Cette technologie pourrait en effet devenir un puissant instrument de surveillance de masse si elle était légalisée. Elle souligne encore que la reconnaissance des individus pour la surveillance des foules viole la Charte de droits fondamentaux de l'Union européenne.

L'usage de cette technologie dans nos rues nous rendrait tous identifiables en permanence, en tout cas, tous surveillés et potentiellement tous suspects. En effet, cela revient à

In dezelfde geest voegde staatssecretaris Mathieu Michel daaraan toe dat België een paradigmawissel nodig heeft inzake het gebruik van intelligente camera's. Hij verklaarde: "Vandaag is alles toegestaan wat niet verboden is. Maar meer en meer technologieën raken in gebruik voor we ons hun effecten nog maar hebben kunnen voorstellen. Na het debat in de Kamer zal de wet een reeks toegestane toepassingen voor deze technologieën moeten vastleggen. De rest moet worden verboden."

Al die publieke verklaringen lijken aan te tonen dat er een bewustwording aan de gang is van de risico's verbonden aan het gebruik van technologieën zoals die voor gezichtsherkenning, maar dat het ook mogelijk is ermee om te gaan op een manier die eenieders rechten en vrijheden garandeert. Daarom is het belangrijk dat soort tools, die een reëel voordeel inhouden om bepaalde evenementen in goede banen te leiden, gericht in te zetten.

Hij lijkt dus voorbarig om de verzoeken van de indieners van de petitie ongenuanceerd in te willigen. Zij willen een totaalverbod op het gebruik van gezichtsherkenningstechnologie in de openbare ruimte en op het gebruik ervan door de overheid met het oog op het identificeren van personen, terwijl er op dit eigenste moment wordt nagedacht over een duidelijk, welomlijnd en transparant regelgevend kader, ook voor het gebruik van gezichtsherkenning voor handhavingsdoeleinden.

Het valt te vrezen dat dit proces vertraagd wordt als we het debat op verschillende plaatsen tegelijk voeren en in het gewest het werk van het federaal parlement overdoen.

Ik wijs er graag op dat contacten met de diensten op het terrein leren dat de technieken voordelen bieden en onder bepaalde voorwaarden een echte meerwaarde kunnen betekenen voor het politiewerk. Dezelfde diensten roepen de overheden op om te zorgen voor een wetgevend kader met strikte regels, die bij iedereen bekend zijn.

Tot slot zou het de helderheid ten goede komen als we van de indieners mochten vernemen wat hun precieze verzoeken zijn. In hun inleiding spreken ze over de LEZ-camera's. Betekent dat dat ze zich keren tegen alle herkenningstechnologieën in het Brussels Gewest, of gaat het hun meer bepaald om gezichtsherkenning? Wat verwachten ze van safe.brussels, gezien de beperkte gewestelijke bevoegdheden ter zake?

**Mevrouw Fadila Laanan** merkt op dat het gebruik van gezichtsherkenning in de publieke ruimte een grote impact heeft op het respect voor mensenrechten en fundamentele vrijheden. Als de technologie wettelijk verankerd wordt, zou ze namelijk een krachtig instrument voor massasurveillance kunnen worden. Zij onderstreept voorts dat de herkenning van individuen met het oog op het bewaken van mensenmassa's ingaat tegen het Handvest van de grondrechten van de Europese Unie.

Het inzetten van deze technologie in onze straten zou ons allemaal permanent identificeerbaar maken; iedereen zou bewaakt worden en potentieel verdacht zijn. Het zou onze

donner à nos autorités le pouvoir d'identifier l'intégralité de la population simplement parce qu'elle est dans l'espace public, ce qui constitue une atteinte à la vie privée et à la liberté individuelle. Cela restreint considérablement le droit à l'anonymat des citoyens. On voit les dérives dans d'autres pays, comme en Chine, où on exclut des personnes sur la base de leur situation économique et en ayant recours à la reconnaissance faciale.

Elle indique également savoir qu'une enquête effectuée auprès de 11.000 consommateurs dans le monde, dont mille en Belgique, dans le cadre du "Security index" d'Unisys, a démontré que 75 % des Belges interrogés n'apprécient par exemple pas l'utilisation la reconnaissance faciale pour la détection d'infos liées au covid, telles que la vaccination ou les infections. Une immense majorité, près de 91 %, ne souhaite pas que la reconnaissance faciale soit exploitée par les magasins pour leur conseiller des produits personnalisés. En général, les Belges ne sont tout simplement pas fans de cette technologie. 64 % ne veulent pas que leur visage soit scanné lors du passage aux frontières et 61 % y sont également opposés lors des opérations d'embarquement dans un avion. Tout juste la moitié la trouverait encore acceptable pour la police en vue d'identifier des malfaiteurs, mais il n'empêche que la population n'est en général pas enthousiaste.

Cela démontre encore une fois que notre population est opposée à ces technologique, et cela est très important.

Dans la pétition, il est indiqué que la police a mis en place une « commission consultative éthique sécurité » chargée d'évaluer l'utilisation éthique et efficace des technologies et des méthodes d'enquête et d'intervention, et qu'il n'existe aucune transparence sur les travaux en cours. Elle demande si les orateurs ont essayé d'interroger la ministre de l'Intérieur sur le sujet ? Ont-ils essayé de disposer des informations sur cette commission et via quel biais ?

Il est également dit qu'il existe une volonté politique d'avoir recours à la reconnaissance faciale, dans le chef de la ministre fédérale de l'Intérieur, Annelies Verlinden, qui préconisait en 2021 l'usage de celle-ci, « à condition que les garanties soient suffisantes en termes de respect des droits de l'homme ». Quelles garanties légales a-t-elle mis en avant ? Que savent les orateurs sur sa position ? A-t-elle évolué depuis 2021 ?

Elle demande également s'ils disposent d'informations sur les dangers et les dérives de l'utilisation de la reconnaissance faciale dans d'autres pays européen.

Mme Margrethe Vestager, la vice-présidente de l'UE au numérique, rappelait que l'utilisation de la reconnaissance faciale de masse pour identifier automatiquement les citoyens était en contradiction avec le règlement général sur la protection des données (RGPD). En effet, cette technologie ne répond pas à un des points les plus importants du règlement, à savoir l'obtention du consentement d'une personne pour le traitement de ses données personnelles. Quel est l'avis des orateurs sur le sujet ?

overheden de macht geven de volledige bevolking te identificeren gewoon omdat ze zich in de openbare ruimte bevindt, wat een inbreuk vormt op de privacy en de individuele vrijheid. Het perkt het recht van burgers op anonimiteit sterk in. We zien tot welke misbruiken dat leidt in landen als China, waar mensen aan de hand van gezichtsherkenning worden uitgesloten op basis van hun economische toestand.

Zij verwijst ook naar een enquête die in het kader van de 'Security index' van Unisys is uitgevoerd bij 11.000 consumenten over de hele wereld, waaronder 1.000 in België, waaruit blijkt dat 75% van de ondervraagde Belgen niet gediend is van het gebruik van gezichtsherkenning om bijvoorbeeld informatie op te sporen over een covidvaccinatie of -infectie. Een overweldigende meerderheid (bijna 91%) wil niet weten van het gebruik van gezichtsherkenning door winkels om persoonlijk productadvies te geven. Over het algemeen zijn de Belgen gewoon geen fan van deze technologie. 64% wil niet dat zijn gezicht gescand wordt bij een grensovergang en 61% is ertegen als hij aan boord van een vliegtuig gaat. Net de helft zou het nog aanvaardbaar vinden dat de politie gezichtsherkenning gebruikt om misdadigers te identificeren, maar dat belet niet dat de bevolking over het algemeen niet enthousiast is.

Het toont nogmaals aan dat onze bevolking gekant is tegen deze technologie, en dat is heel belangrijk.

De petitie vermeldt dat de politie een ethische adviescommissie "veiligheid" heeft opgericht om zich te buigen over het ethische en efficiënte gebruik van onderzoeks- en interventietechnologieën en -methodes, en dat er geen transparantie bestaat over de lopende werkzaamheden. Het parlementslid stelt de vraag of de sprekers getracht hebben de minister van Binnenlandse Zaken hierover te ondervragen. Hebben ze geprobeerd informatie over deze commissie te verkrijgen en zo ja, via welke weg?

Er wordt ook gesteld dat de federale minister van Binnenlandse Zaken de politieke wil heeft om van gezichtsherkenning gebruik te maken: in 2021 sprak zij zich uit voor het gebruik daarvan "op voorwaarde dat er voldoende waarborgen bestaan inzake respect voor de mensenrechten". Welke wettelijke garanties heeft zij naar voren geschoven? Wat weten de sprekers over haar standpunt? Is dat sinds 2021 geëvolueerd?

Zij vraagt ook of de sprekers informatie hebben over de gevaren en misbruiken verbonden met het gebruik van gezichtsherkenning in andere Europese landen.

Mevrouw Margrethe Vestager, de vice-voorzitter van de Europese Commissie, bevoegd voor digitalisering, wees erop dat het gebruik van massagezichtsherkenning om burgers automatisch te identificeren in strijd is met de Algemene verordening gegevensbescherming (*General Data Protection Regulation,* GDPR). De technologie voldoet immers niet aan een van de belangrijkste punten van die verordening, namelijk het verkrijgen van de instemming van de persoon in kwestie voor het verwerken van zijn

Elle indique également avoir eu des échos concernant le cadre juridique existant, qui est mal appliqué et qui présente des problèmes de mise en œuvre. Ainsi, ces technologies devraient être interdites par le RGPD, mais cette interdiction n'existe pas dans la réalité. Les orateurs peuvent-ils confirmer cela ?

Enfin, une étude européenne sur le sujet a déjà démontré qu'onze pays européen l'utilisent déjà de façon régulière. Les orateurs disposent-ils d'informations quant à une réglementation européenne en la matière ?

Elle conclut en se disant heureuse d'avoir pu accueillir les orateurs sur un sujet aussi important.

**Mme Els Rochette** remercie les invités pour leur exposé intéressant, ainsi que les organisations de défense des droits humains et les plus de 1.000 signataires pour avoir mis sur la table ce sujet important.

Elle admet qu'au début, elle ne voyait pas très bien quel rôle le Parlement de la Région de Bruxelles-Capitale pouvait jouer dans cette matière, mais elle l'a compris clairement à la fin de l'exposé.

Bien que la question de la reconnaissance faciale soit une compétence fédérale, elle concerne tout un chacun, en particulier à Bruxelles. Le droit des Bruxellois au respect de la vie privée est très cher à son parti et il doit être garanti.

Les orateurs ont mentionné les risques majeurs qui vont de pair avec l'utilisation de cette technologie, notamment le problème de la discrimination raciale. Elle fait remarquer que le profilage est déjà un problème lors des contrôles de police. Elle conçoit donc sans peine que, si de telles technologies étaient déployées, ce problème pourrait encore s'aggraver. Le droit à la liberté d'expression pourrait également être menacé.

Elle a entendu que divers tests ont mis en lumière de nombreuses erreurs prenant la forme de faux positifs et de faux négatifs.

L'oratrice se dit choquée d'apprendre que toute caméra de surveillance peut être équipée d'un logiciel de reconnaissance faciale. C'est une chose dont on n'a pas assez conscience aujourd'hui. Elle demande si les caméras privées peuvent également en être équipées.

Elle indique que le risque de voir des données biométriques tomber entre de mauvaises mains doit être pris très au sérieux.

Eu égard à tous ces éléments, la députée indique qu'une base légale est essentielle pour pouvoir utiliser ces technologies. Son groupe soutient la demande des pétitionnaires en faveur de l'adoption d'un tel cadre. Elle regrette que le projet de résolution concernant un moratoire

persoonsgegevens. Wat is de mening van de sprekers daarover?

Zij heeft ook vernomen dat het bestaande juridische kader slecht wordt toegepast en dat er problemen zijn met de uitvoering. Zo zouden deze technologieën op basis van de GDPR verboden moeten zijn, maar in de realiteit zijn ze dat niet. Kunnen de sprekers dat bevestigen?

Tot slot heeft een Europese studie over het onderwerp aangetoond dat elf Europese landen al geregeld gebruikmaken van gezichtsherkenning. Hebben de sprekers informatie over de Europese regelgeving ter zake?

Het verheugt haar sprekers over zo'n belangrijk onderwerp te mogen verwelkomen.

**Mevrouw Els Rochette** dankt de gasten voor hun interessante toelichting en ook de mensenrechtenorganisaties en de meer dan 1.000 ondertekenaars voor het aanbrengen van dit belangrijke thema.

Ze geeft toe dat het haar aanvankelijk niet duidelijk was welke rol het Brussels Hoofdstedelijk Parlement in deze zou kunnen spelen, maar dat werd duidelijk aan het einde van de toelichting.

De gezichtsherkenningsproblematiek is weliswaar een federale bevoegdheid, maar niettemin een die iedereen aanbelangt, zeker in Brussel. Het recht op privacy van de Brusselaars ligt haar partij heel nauw aan het hart en dat moet gegarandeerd worden.

De sprekers benoemden de grote risico's die gepaard gaan met het gebruik van de technologie, waaronder het probleem van raciale discriminatie. Ze merkt op dat profilering bij politiecontroles nu al een probleem is. Zij kan zich dus inbeelden dat wanneer dergelijke technologieën zouden worden ingezet, het probleem nog zou kunnen verergeren. Voorts zou het recht op vrije meningsuiting in gevaar kunnen komen.

Zij heeft goed gehoord dat bij tests is gebleken dat er veel fouten waren onder de vorm van vals positieve en vals negatieve resultaten.

De spreekster zegt geschokt te zijn over het feit dat elke bewakingscamera met een gezichtsherkenningsoftware kan worden uitgerust. Dat is iets dat men vandaag te weinig beseft. Ze vraagt of ook private camera's daarmee kunnen worden uitgerust?

Zij geeft aan dat we het gevaar dat biometrische gegevens in verkeerde handen kunnen terechtkomen zeer ernstig moeten nemen.

Rekening houdend met dat alles geeft de volksvertegenwoordiger aan dat een wettelijke basis cruciaal is om dergelijke technologieën te mogen gebruiken. Haar fractie ondersteunt de vraag van de indieners van de petitie om een dergelijk kader uit te werken. Ze geeft nog

de trois ans, déposé en mai 2020, n'ait toujours pas été examiné et que, pendant tout ce temps, les tests ont donc pu se poursuivre.

Elle demande s'il existe une étude sur les avantages et inconvénients de la technologie de reconnaissance faciale. Quelle est la position des pétitionnaires au sujet de l'utilisation de cette technologie dans des cas très exceptionnels, par exemple pour résoudre des crimes graves tels que la pédopornographie ? Elle demande quelle est la situation en Suisse. Cette technologie n'y est-elle jamais autorisée ou est-elle utilisée dans des cas exceptionnels ?

Plusieurs tests et expériences ont déjà été menés, notamment à l'aéroport, dont les résultats auraient révélé de nombreux faux positifs. Elle demande qui décide d'organiser de tels tests. Et en cas d'erreur, vers qui peuvent se tourner les personnes victimes de ces tests pour déposer plainte ou être indemnisées ? Quelle instance est-elle chargée du suivi de ces tests ? Ces tests sont-ils contrôlés ?

**Mme Leila Lahssaini** remercie le MRAX et la Ligue des droits humains d'interpeller les responsables politiques sur cette question. Il lui semble important de ne pas avoir attendu qu'il soit trop tard et que des textes aient déjà été adoptés.

Elle rappelle que des mandataires de son parti, le PTB, ont déjà interpellé au niveau fédéral la ministre de l'Intérieur quand les informations sur l'utilisation illégales des technologies de reconnaissance faciale par la police étaient ressorties.

Il devrait être évident, mais ce ne l'est pas tant que cela, que la police et les autres institutions respectent le cadre légal. Malheureusement, devant l'existence des technologies de reconnaissance faciale, la tentation de les utiliser est grande. Il ne faut donc pas être naïf par rapport à cette utilisation et continuer de demander d'avoir accès aux études et aux contrôles de l'utilisation de ces technologies. Elle remarque à ce sujet qu'il est toujours compliqué d'avoir un contrôle réellement transparent des activités policières.

L'oratrice indique également qu'il est intéressant que les pétitionnaires aient indiqué dans leurs développements que ces technologies ont un impact sociétal. Elle remarque que de plus en plus de caméras sont mises en place pour faire respecter la propreté publique, ou dans les transports en commun. Petit à petit, ces différents types de caméras sont installés et, finalement, tout un réseau de captage d'images voit le jour. Au final, cet ensemble de caméras de contrôle est assez rarement mis en question.

Dès lors, il est important d'avoir ce débat ici et ailleurs, et ce d'autant plus que la mise en place de ces systèmes est souvent justifiée par des motifs auxquels on peut difficilement s'opposer, comme par exemple la lutte contre le terrorisme, la grande criminalité. Dès lors, dans le cadre du débat d'idées, il est difficile d'aborder les risques que ces caméras peuvent engendrer. Pourtant, on a déjà observé par le passé qu'un glissement s'opère ensuite pour permettre l'utilisation de

aan te betreuren dat de ontwerpresolutie met betrekking tot een driejarig moratorium, die in mei 2020 werd ingediend, nog steeds niet is behandeld en dat, de tests daardoor al die tijd konden worden verdergezet.

Zij vraagt of er een onderzoek bestaat met betrekking tot de voor- en nadelen van gezichtsherkenningstechnologie? Wat is het standpunt van de indieners van de petitie met betrekking tot het gebruik van die technologie in zeer uitzonderlijke gevallen om ernstige misdaden op te lossen zoals bijvoorbeeld kinderporno? Ze vraagt wat de situatie is in Zwitserland. Wordt die technologie er nooit toegelaten of wordt ze in uitzonderlijke gevallen wel gebruikt?

Er werden al verschillende tests en experimenten gedaan, onder andere op de luchthaven, die heel wat vals positieve resultaten zouden hebben opgeleverd. Ze vraagt wie er beslist over het organiseren van dergelijke tests. En kunnen de mensen die slachtoffer werden van die tests, bij fouten, ergens terecht om een klacht in te dienen of een schadevergoeding te bekomen? Welke instantie staat in voor de opvolging van de tests? Worden de tests gemonitord?

**Mevrouw Leila Lahssaini** dankt het MRAX en de Ligue des Droits Humains om de politici over deze kwestie te hebben aangesproken. Het lijkt haar belangrijk dat er niet gewacht is tot het te laat was en dat er al teksten zijn aangenomen.

Zij wijst erop dat mandatarissen van haar partij, de PTB, de federale minister van Binnenlandse Zaken al hebben geïnterpelleerd nadat bekend was geraakt dat de politie op onwettige wijze gezichtsherkenningssoftware had gebruikt.

Het zou vanzelfsprekend moeten zijn – maar dat blijkt het dus niet te zijn – dat de politie en andere instellingen het wettelijke kader respecteren. Zodra gezichtsherkenningstechnologie beschikbaar is, is de verleiding jammer genoeg groot om die te gebruiken. We mogen dus niet naïef zijn en moeten toegang blijven vragen tot de studies ter zake en tot de controles op het gebruik van deze technologie. Zij merkt in dit verband op dat "het altijd moeilijk is om politieactiviteiten transparant te controleren".

De spreekster vindt het ook interessant dat de indieners in hun toelichting hebben gewezen op de maatschappelijke impact van de technologieën. Zij merkt op dat er almaar meer camera's worden geplaatst om toezicht te houden op de openbare netheid, alsook in het openbaar vervoer. Stap voor stap worden diverse cameratypes geplaatst en zo ontstaat een heel netwerk van beeldregistratie, dat ons controleert en waar zelden vragen over worden gesteld.

Het is daarom belangrijk het debat hier en elders te voeren, temeer omdat die systemen vaak worden ingevoerd met motieven waar weinig tegen in te brengen valt, zoals de strijd tegen terreur of zware misdaad. Dat maakt het moeilijk om in debatten de risico's aan te kaarten die het gebruik van camera's met zich meebrengt. Nochtans hebben we in het verleden al gezien dat het gebruik ervan dreigt af te glijden

cette technologie pour des faits moins graves, comme c'est par exemple le cas avec les caméras ANPR.

Ainsi, elle cite l'exemple, au niveau fédéral, de la loi qui prévoit une peine d'interdiction de manifester. Elle se demande concrètement comment on pourrait mettre en place une telle interdiction de manifester. On pourrait, pour ce faire, avoir recours à ce type de technologie, qui permet de contrôler facilement un groupe de personnes dans l'espace public et de rendre possible ce type de peines.

Elle regrette également que le parlement fédéral n'ait malheureusement toujours pas discuté de la proposition, déposée il y a trois ans, et prévoyant un moratoire de trois ans sur l'utilisation de technologies de reconnaissance faciale. Elle estime que le Parlement devrait également aller dans ce sens.

Par ailleurs, elle indique connaître le sentiment des orateurs par rapport au projet Smartmove, qui a pour but de recourir aux caméras ANPR pour instaurer une taxe kilométrique à Bruxelles. Cela n'implique certes pas de données biométriques, mais bien un contrôle des déplacements dans l'espace public. Cela implique également que toute personne qui se déplacerait à Bruxelles devrait, à l'avance, indiquer exactement le trajet dans une application, qui est en cours de test. Si ces indications n'étaient pas respectées, une amende serait infligée immédiatement. Au niveau de l'utilisation des données personnelles, le fait de contrôler les citoyens dans leurs déplacements dans l'espace public lui pose un réel problème en matière de vie privée. Pourtant le Gouvernement bruxellois a déjà dépensé plusieurs millions d'euros pour la mise en place de ce système.

**M. Sadik Köksal** remercie les trois personnes, qui ont amené un débat très intéressant.

Il rappelle que l'on a pu apprendre par la presse qu'il y avait eu des utilisations de la technologie de reconnaissance faciale. Ce qui l'inquiète particulièrement, c'est le fait que, dans un premier temps, même le COC n'avait pas obtenu les informations réelles concernant ces tests. Ce n'est que dans un second temps, suite à la publication d'un autre article de presse publié aux États-Unis, que l'organe de contrôle a pu interpeller à nouveau les responsables de ces tests. Il souligne qu'il est inadmissible qu'on ait tenté de cacher au COC que de tels tests avaient lieu. Ce mensonge met en doute la relation de l'organe de contrôle et des responsables qui, malheureusement, ont omis volontairement certains éléments.

L'orateur constate qu'aujourd'hui, il n'existe pas de cadre juridique permettant de manière stricte et contrôlée de faire un tel usage. S'il y a des périodes de test, il faut que cela se fasse dans un cadre bien déterminé et sous une autorité de contrôle.

Si le député comprend bien que les pétitionnaires souhaitent l'interdiction de l'utilisation de la reconnaissance faciale tant qu'il n'y a pas de cadre légal, il demande s'ils s'opposent également à son utilisation dans des cas particuliers, tels que des disparitions d'enfants. À titre d'exemple, l'année dernière 1.515 enfants ont disparu et 5 % d'entre eux, soit 75 enfants, n'ont malheureusement toujours

naar lichtere feiten, zoals het geval is met de ANPR-camera's.

Zij haalt het voorbeeld aan van de federale wet die een manifestatieverbod met een boete wil bestraffen. Zij vraagt zich af hoe zo'n manifestatieverbod concreet kan worden afgedwongen. Met dit soort technologie wordt het gemakkelijk een groep mensen in de openbare ruimte te controleren en boetes op te leggen.

Zij betreurt ook dat het federale parlement het drie jaar geleden ingediende voorstel nog steeds niet besproken heeft, dat voorzag in een moratorium van drie jaar op het gebruik van gezichtsherkenningstechnologie. Zij is van mening dat het Brussels Parlement zich in dezelfde zin moet uitspreken.

Zij geeft aan dat ze ook weet hoe de sprekers staan tegenover het project Smart Move, dat de ANPR-camera's wil inzetten om een kilometerheffing in Brussel in te voeren. Daar zijn weliswaar geen biometrische gegevens bij betrokken, maar het impliceert wel de controle van de verplaatsingen die mensen in de openbare ruimte maken. Iedereen die zich in Brussel verplaatst, zou vooraf zijn precieze route moeten ingeven in een app, die momenteel getest wordt. Wie van zijn reisweg afwijkt, zou onmiddellijk een boete krijgen. Dergelijk gebruik van persoonsgegevens, waarbij de verplaatsingen van burgers in de openbare ruimte gecontroleerd worden, vormt in haar ogen een echt privacyprobleem. Toch heeft de Brusselse regering al miljoenen euro's uitgegeven voor de invoering van het systeem.

**De heer Sadik Köksal** dankt de drie sprekers, die een heel interessant debat op gang hebben gebracht.

Hij herinnert eraan dat de pers verscheidene gevallen van het gebruik van gezichtsherkenningssoftware heeft gemeld. Wat hem bijzonder verontrust, is het feit dat zelfs het COC aanvankelijk de correcte informatie over die tests niet kreeg. Pas na het verschijnen van een nieuw persartikel in de Verenigde Staten kon het COC de verantwoordelijken voor die tests opnieuw ondervragen. Hij vindt het onaanvaardbaar dat getracht is het bestaan van die tests voor het COC verborgen te houden. Die leugen roept twijfels op over de relatie tussen het COC en de verantwoordelijken, die jammer genoeg bepaalde informatie bewust hebben achtergehouden.

De spreker stelt vast dat er vandaag geen juridisch kader is dat dit soort gebruik op een strikt gecontroleerde manier mogelijk maakt. Als er testfases zijn, moeten die binnen een welomlijnd kader plaatsvinden en onder het toezicht van een controle-instantie.

Het parlementslid begrijpt dat de indieners een verbod op het gebruik van gezichtsherkenning willen zolang er geen wettelijk kader bestaat, maar vraagt zich af of ze daar ook tegen gekant zijn in specifieke gevallen, zoals wanneer kinderen vermist zijn. Vorig jaar zijn er bijvoorbeeld 1.515 kinderen verdwenen, van wie er 75 nog steeds vermist zijn. Het doelgericht en verantwoord inzetten van deze nieuwe

pas été retrouvés. Les nouvelles technologies permettraient certainement, dans certains cas d'utilisation à bon escient, de résoudre certaines de ces disparitions.

Il y a également l'exemple, suite aux attentats de mars 2016, de l'homme au chapeau que l'on a pu voir jusque du côté de la place Meiser, sans toutefois être certain qu'il s'agissait bien de la bonne personne.

**M. Christophe De Beukelaer** remarque que le sujet abordé aujourd'hui est important, et il constate avec inquiétude qu'il y a actuellement dans la société une dérive de plus en plus sécuritaire, sans qu'il n'y ait pour autant beaucoup de sécurité, et une dérive vers de plus en plus de surveillance et de centralisation de l'information.

Il constate que pour des motifs toujours très louables, comme la sécurité ou la santé, on met en place de plus en plus de contrôles et de surveillance à tous les niveaux.

À ce propos, il tente d'alerter, et il profite de ce débat pour le faire à nouveau, sur la surveillance au niveau financier. C'est un sujet dont on parle très peu, mais c'est pourtant un sujet majeur parce qu'avec le développement de l'euro numérique, c'est potentiellement une vraie surveillance de masse de toutes les transactions financières qui serait mise en place.

En ce qui concerne la question abordée aujourd'hui, il souhaite remarquer que, contrairement à ce qui a été dit, la technologie est bien neutre par nature. Mais c'est la façon dont elle est mise en œuvre qui ne l'est pas. L'intelligence artificielle est orientée par les humains. Avec un couteau, on peut beurrer une tartine ou tuer une personne. Il en va de même pour les nouvelles technologies.

Il se demande dès lors quelle est la différence entre la reconnaissance faciale grâce à l'intelligence artificielle et ce qui se fait déjà maintenant. N'est-ce pas la même chose mais de façon beaucoup plus efficace ? Aujourd'hui, dans certains cas, la police essaie déjà de reconnaître certaines personnes sur des images de vidéosurveillance. Des bases de données existent donc déjà. Il indique pouvoir suivre le raisonnement qui fait que l'on s'oppose à des procédés trop efficaces.

Comme certains de ses collègues, il demande si les pétitionnaires remettent aussi en cause la façon dont on fonctionne aujourd'hui et le fait d'avoir certaines caméras et d'avoir des humains derrière des écrans qui essaient de reconnaître certaines personnes. Est-ce que cela va déjà trop loin ? Ou est-ce l'ajout de la couche d'intelligence artificielle qui pose réellement problème ?

Par rapport aux données biométriques, il indique bien entendre qu'elles sont uniques. Mais sans ces données, d'autres techniques de ressemblance pourraient certainement être utilisées. Il demande si cela serait plus acceptable, ou si le problème est le même ?

Enfin, il souligne que tout le monde est concerné par la lutte contre la pédophilie ou contre le terrorisme. Dès lors, il n'a pas envie de se prononcer à l'emporte-pièce sur la question de savoir si, oui ou non, il soutient toutes les

technologieën zou zeker kunnen helpen om een aantal van die verdwijningen op te lossen.

Er is ook het voorbeeld van de man met het hoedje, die na de aanslagen van maart 2016 gevolgd kon worden tot in de buurt van het Meiserplein, hoewel niet vaststaat dat het om de juiste persoon ging.

**De heer Christophe De Beukelaer** merkt op dat het onderwerp dat vandaag wordt besproken, belangrijk is en stelt bezorgd vast dat de maatschappij afglijdt naar een veiligheidsdrang die jammer genoeg niet voor echte veiligheid zorgt, en naar almaar meer controledrang en centraal gegevensbeheer.

Hij stelt vast dat, om lovenswaardige redenen zoals veiligheid of gezondheid, almaar meer controle en toezicht wordt georganiseerd.

In dat kader maakt hij van dit debat gebruik om opnieuw te waarschuwen voor financieel toezicht, een onderwerp dat maar zelden ter sprake komt. Het is nochtans erg belangrijk, want met de ontwikkeling van de digitale euro bestaat de kans dat massaal toezicht op financiële transacties wordt ingevoerd.

Over de vandaag besproken kwestie merkt hij op dat, in tegenstelling tot wat is gezegd, de technologie van nature neutraal is. De manier waarop ze wordt gebruikt is dat echter niet. Artificiële intelligentie wordt door mensen gestuurd. Met een mes kun je een boterham smeren of iemand doden. We kunnen eenzelfde vergelijking maken voor nieuwe technologieën.

Hij vraagt zich dan ook af wat het verschil is tussen gezichtsherkenning met behulp van artificiële intelligentie en wat nu al gebeurt. Is het niet gewoon hetzelfde, maar dan veel efficiënter? Vandaag probeert de politie in sommige gevallen ook al om bepaalde personen op beelden van bewakingscamera's te herkennen. Er zijn al databanken. Hij zegt dat hij de redenering achter het verzet tegen te efficiënte processen kan volgen.

Net als sommige van zijn collega's, vraagt hij of de ondertekenaars van de petitie ook de huidige aanpak, de aanwezigheid van bepaalde camera's en het feit dat mensen op beeldschermen bepaalde personen trachten te herkennen, ter discussie stellen. Gaat dat al te ver? Of hebben ze vooral een probleem met het toevoegen van het gebruik van artificiële intelligentie?

Hij stelt dat hij begrijpt dat biometrische gegevens uniek zijn. Zonder die gegevens zouden er echter ongetwijfeld andere herkenningstechnieken kunnen worden gebruikt. Zouden die aanvaardbaarder zijn, of gelden dezelfde bezwaren?

Ten slotte benadrukt hij dat de strijd tegen pedofilie of tegen terrorisme iedereen aangaat. Hij wil zich dan ook niet nadrukkelijk uitspreken voor of tegen de aanbevelingen van de indieners van de petitie.

recommandations des pétitionnaires.

Il souhaite donc obtenir des réponses aux questions qu'il a posées avant de pouvoir se prononcer.

**M. Mathias Vanden Borre** indique que le débat sur la reconnaissance faciale est par nature fondamental et qu'il vit également dans la société.

Il est convaincu qu'il n'est pas possible de donner des réponses catégoriques à cette question, mais qu'il faut peser le pour et le contre et que chaque situation doit être appréciée à l'aune de la réalité. Il constate que les évolutions de ces dix dernières années dans le domaine de la sécurité publique et privée sont fortement liées aux développements technologiques et à l'innovation. La question de savoir comment concilier l'intégration des évolutions et de la technologie, d'une part, et le respect de la vie privée, d'autre part, est donc importante.

Il se dit toutefois convaincu que si l'on parvient à déployer la technologie avec justesse, on pourra faire de grandes avancées dans le domaine de la sécurité. Il ne s'agit pas seulement de la reconnaissance faciale, mais aussi d'autres futures technologies qui permettront d'avoir un fonctionnement plus efficace, plus économique et plus écologique.

Bien sûr, le revers de la médaille, c'est que ces nouvelles technologies comportent des risques potentiels. C'est pourquoi tout ce qui est techniquement possible n'est pas forcément souhaitable. Il faut donc rester critique quand on réfléchit à dans quelle mesure la technologie et l'innovation peuvent rendre notre société plus sûre.

De nombreux acteurs cherchent activement à renouveler les méthodes d'exécution de leurs tâches en investissant dans la technologie et l'innovation. Étant donné que la prestation de services doit toujours être centrale, la technologie peut être utile pour recueillir des preuves, faire des constats, reconnaître les comportements dangereux, etc.

Enfin, il indique qu'il faut continuer à se demander dans quelle mesure les technologies disponibles peuvent être utiles. Il souligne par exemple que l'évolution démographique qu'on connaît pose des problèmes de capacité à toutes les institutions. Il est également vrai que de très nombreux membres des personnels de sécurité, que ce soit à la police, à la défense ou dans les services de sécurité, prendront leur retraite et que les recrutements ne pourront pas suivre les départs. L'une des solutions à ces défis de capacité peut être trouvée du côté de la technologie. Le débat ne porte pas seulement sur la numérisation et l'automatisation, il y a aussi un besoin aigu d'améliorer les services de sécurité de la Région au moyen de stratégies et de processus adaptés.

Selon l'orateur, la technologie doit permettre d'améliorer le service et de renforcer la capacité politique et opérationnelle à relever les défis actuels et futurs. C'est pourquoi il faut également des organisations plus fortes, plus flexibles, ayant la capacité et les connaissances suffisantes pour faire face aux développements actuels et futurs. Il pense par exemple à une meilleure collaboration entre les six zones

Hij wenst met andere woorden een antwoord te krijgen zijn de vragen alvorens hij zich kan uitspreken.

**De heer Mathias Vanden Borre** geeft aan dat het debat over gezichtsherkenning fundamenteel van aard is en dat het ook maatschappelijk leeft.

Hij is ervan overtuigd dat er geen zwart-wit antwoorden kunnen worden geformuleerd op dit vraagstuk, maar dat er afwegingen moeten worden gemaakt en dat elke situatie aan de realiteit moet worden getoetst. Hij stelt vast dat het voorbije decennium de evoluties in het publieke private veiligheidsdomein sterk zijn verbonden met technologische ontwikkelingen en innovatie. De vraag hoe men de integratie van evoluties en technologie kan verzoenen met de privacy, is dan ook belangrijk.

Hij zegt wel overtuigd te zijn dat, indien men erin slaagt om de technologie op de juiste manier in te zetten, een grote vooruitgang kan geboekt worden op het vlak van de veiligheid. Zo is er niet enkel sprake van gezichtsherkenning, maar ook van andere aankomende technologieën die de kans geven om niet alleen effeciënter, maar ook economischer en ecologischer te werken.

De keerzijde van de medaille is natuurlijk dat dergelijke nieuwe technologieën potentiële risico's met zich brengen. Daarom is niet alles wat technisch mogelijk is, ook wenselijk. Het is dan ook nodig om kritisch te blijven nadenken over de mate waarin technologie en innovatie onze samenleving veiliger kunnen maken.

Heel wat actoren investeren in technologie en innovatie om hun werkwijze te moderniseren. Gelet op het feit dat de dienstverlening steeds centraal zou moet staan, kan technologie nuttig zijn om bewijsmateriaal te verzamelen, vaststellingen te doen, onveilige gedragingen te erkennen, enz.

Tot slot geeft hij aan dat nodig is te blijven nadenken over de mate waarin beschikbare technologieën toch nuttig kunnen zijn. Hij wijst er bijvoorbeeld op dat men te maken heeft met een demografische evolutie die alle instellingen voor capaciteitsuitdagingen plaatst. Voorts is het zo dat heel veel veiligheidsmedewerkers, bij politie, defensie of veiligheidsdiensten, met pensioen gaan en dat de instroom de uitstroom niet zal kunnen volgen. Eén van de oplossingen met betrekking tot die capaciteitsuitdagingen kan gevonden worden in technologie. Het debat gaat niet alleen over digitalisering en automatisering, maar er is ook een acute noodzaak om de veiligheidsdiensten van het Gewest van te verbeteren via aangepaste strategieën en processen.

Volgens de spreker moet de technologie leiden tot betere dienstverlening en een groter beleids- en operationeel vermogen om huidige en toekomstige uitdagingen het hoofd te bieden. Daarom moeten er ook sterkere en wendbare organisaties zijn die voldoende kennis en capaciteit hebben om de huidige en toekomstige ontwikkelingen aan te kunnen. Hij denkt, bijvoorbeeld, aan betere samenwerking

de police. En effet, aujourd'hui, les six zones de police ont des approches radicalement différentes face aux nombreux défis.

Enfin, il déclare qu'il continuera à suivre ce dossier, tout comme ses collègues au niveau fédéral. Il dit que son parti est favorable à la poursuite du débat.

**Mme Joke Blockx** répond qu'elle comprend que plusieurs parlementaires estiment qu'il conviendrait de chercher, au moyen d'un cadre légal, un équilibre entre la sécurité et les droits fondamentaux afin d'appliquer la reconnaissance faciale dans les dossiers exceptionnellement graves. Elle signale toutefois que les experts de la protection de la vie privée s'accordent à dire qu'il est extrêmement difficile, sinon impossible, de parvenir à un tel équilibre. En effet, la technologie n'est pas parfaite ; les erreurs sont inhérentes au système. Par conséquent, si ces technologies étaient déployées à grande échelle, les droits fondamentaux seraient par définition menacés. La question est de savoir si nous voulons une société qui applique la surveillance de masse d'une manière qui viole les droits fondamentaux à court et à long terme. Qu'adviendra-t-il en cas de problème avec ces données ?

L'oratrice tient également à souligner qu'on parle ici de données biométriques, soit des données uniques qui, en principe, ne peuvent pas faire l'objet d'un traitement. Elle ajoute que toute exception à cette règle, qui nécessiterait le traitement des données, doit être nécessaire, sans qu'on puisse en faire une description générale. Jusqu'à présent, cette certitude n'existe pas. Les questions qui ont été posées prouvent par exemple que l'on ignore combien de technologies il existe, à quelles fins elles sont utilisées, quels risques elles font courir et quel est leur impact. C'est pourquoi la technologie de reconnaissance faciale doit tout d'abord rester interdite.

En ce qui concerne les tests, l'oratrice indique que c'est la police elle-même qui en prend la décision, avec le soutien du pouvoir exécutif, mais sans l'autorisation du législateur. C'est évidemment très problématique. Lors des tests menés à l'aéroport de Zaventem en 2017, même le COC n'en a pas été informé. C'est pourtant une obligation et le strict minimum.

Elle note ensuite qu'une surveillance de masse est aujourd'hui installée, sans que les citoyens de ce pays en sachent rien.

Les victimes de l'utilisation de ces technologies peuvent s'adresser aux différents organes chargés de contrôler l'utilisation des caméras. Pour l'utilisation de ces technologies par la police, il faut s'adresser au COC. Mais tout ce qu'on peut faire, c'est lui demander si on figure où que ce soit dans une base de données de la police. Mais le COC lui-même, l'organe de contrôle, ne pourra pas consulter cette base de données. Aujourd'hui, les données de la police échappent presque à tout contrôle citoyen.

L'oratrice ajoute que la technologie est très vaste et qu'elle peut en effet apporter des réponses à de nombreux

tussen de zes politiezones. Vandaag hebben de zes politiezones immers een totaal andere benadering van de vele uitdagingen.

Tot slot geeft hij aan dit thema te zullen blijven opvolgen en ook zijn collega's op in het federaal parlement zullen dat doen. Hij zegt dat zijn partij er voorstander van is om het debat permanent te blijven voeren.

**Mevrouw Joke Blockx** antwoordt dat zij begrip heeft voor het feit dat verscheidene volksvertegenwoordigers menen dat er middels een wettelijk kader naar een evenwicht zou moeten worden gestreefd tussen veiligheid en fundamentele rechten, om gezichtsherkenning te kunnen toepassen in uitzonderlijk zware dossiers. Ze geeft evenwel aan dat er een consensus bestaat bij privacy-experts over het feit dat het bereiken van een dergelijk tegenwicht bijzonder moeilijk, zo niet onmogelijk is. De technologie is immers niet foutloos, de fouten zijn inherent aan het systeem. Als dergelijke technologieën dan ook op grote schaal zouden worden ingezet, dan komen de fundamentele rechten per definitie in gevaar. De vraag is of wij een samenleving willen die massasurveillance toepast op een manier die de fundamentele rechten op korte en lange termijn schendt. Wat als er iets misgaat met die data?

Voorts wil zij benadrukken dat er sprake is van biometrische gegevens. Dat zijn unieke gegevens die in principe niet mogen worden verwerkt. De spreker geeft nog aan dat eventuele uitzonderingen op die regel, die een verwerking van de gegevens noodzakelijk zou maken, noodzakelijk moet zijn, zonder dat die algemeen omschreven mag worden. Tot nu toe bestaat die zekerheid niet. De vragen die werden gesteld bewijzen, bijvoorbeeld, dat men niet weet hoeveel technologieën er zijn, waarvoor ze worden gebruikt, welke risico's ze met zich brengen en welke impact ze hebben. Daarom moet de technologie van gezichtsherkenning in de eerste plaats verboden blijven.

Met betrekking tot de tests, geeft de spreker aan dat de politie daar momenteel zelf over beslist, met de steun van de uitvoerende macht, maar zonder toelating van de wetgevende macht. Dat is natuurlijk zeer problematisch. Bij de tests in de luchthaven van Zaventem in 2017 werd zelfs het COC niet op de hoogte gebracht. Dat is nochtans verplicht en het absolute minimum.

Voorts merkt zij op dat er vandaag massasurveillance geïnstalleerd is, zonder dat de burgers van dit land daar iets van weten.

De slachtoffers van het gebruik van dergelijke technologieën kunnen terecht bij verscheidene instanties die bevoegd zijn voor het toezicht op het gebruik van camera's. In het geval van het gebruik van dergelijke technologie door de politie, moet men zich richten tot het COC. Daar kan echter enkel worden nagevraagd of men ergens in een politiedatabank zit. Het COC, het toezichtsorgaan, kan zelf die databank niet raadplegen. Vandaag worden politiedata enorm afgeschermd van controle door de burgers.

Voorts geeft zij nog aan dat technologie heel ruim is en inderdaad in staat is om oplossingen te bieden op heel wat

défis. Toutefois, en ce qui concerne la reconnaissance faciale et les données biométriques, elle répète que leur utilisation, y compris par des entreprises privées, sans consultation adéquate des personnes concernées, présente des risques majeurs. C'est pourquoi, très concrètement, elle plaide une fois encore pour une interdiction des technologies de reconnaissance faciale.

**Mme Nicha Mbuli** indique qu'en ce qui concerne les personnes qui font l'objet de profilage par la reconnaissance faciale, il est particulièrement difficile de se faire entendre. Il est déjà difficile pour une personne qui subit la discrimination et le racisme au quotidien de prouver qu'elle a été discriminée. Alors prouver qu'on a été discriminé par la technologie, ce sera encore plus difficile.

Elle remarque en outre qu'il existe une législation de lutte contre les discriminations, une loi générale sur toutes les formes de discrimination, mais que cette loi ne prend pas en compte toutes les formes de discrimination qui peuvent arriver aujourd'hui avec la reconnaissance faciale.

Si certains estiment que les nouvelles technologies faciliteront le travail policier, l'oratrice pense qu'il est plutôt question d'une déresponsabilisation de la police. En effet, ce sera la machine qui va signaler à la police qu'il y a eu un "*match*". Le policier ne fera plus appel à son expertise ou à sa connaissance du terrain, mais c'est la machine qui décidera et le policier ne fera plus qu'appliquer cette décision.

Elle pense également que, peu importe la façon dont sont constituées les bases de données, il sera toujours question de catégoriser les personnes selon des idées plutôt racialistes. Faire confiance à des machines et promouvoir la neutralité des machines constitue vraiment un danger pour tout le combat qui a été mené concernant la lutte contre les discriminations et le racisme.

**M. Rémy Farge** précise que des phases test ont eu lieu en toute illégalité et sans transparence et à côté il est étudié comment il sera possible de rendre légales les pratiques qui ont été réalisées de façon illégale. Des commissions sont mises en place pour envisager, semble-t-il, à l'avenir un cadre qui permettrait l'usage de ces technologies. Le fait que l'on ne dispose pas d'informations en la matière, illustre bien le manque de volonté de travailler en toute transparence. Le débat nous est confisqué et il est encommissionné pour que le cadre légal puisse être pensé en toute indépendance.

Il indique penser que Bruxelles peut être un modèle sur la question. Au vu de ses compétences, au vu de ce que l'on observe à Bruxelles et de ce qui a été décrit précédemment, une position forte et argumentée de Bruxelles pourrait également sonner un petit peu l'alerte au niveau fédéral et constituer une forme de pression qui pourrait résonner au niveau fédéral aussi.

Il insiste encore sur la nécessité de plus de transparence. La Ligue des droits humains a lancé une campagne de demande d'accès aux documents administratifs pour poser toute une série de questions, notamment au sujet des

uitdagingen. Maar, met betrekking tot de gezichtsherkenning en het gebruik van biometrische data, herhaalt de spreker dat wanneer die gebruikt wordt, ook door privébedrijven, zonder dat de betrokkenen daar fatsoenlijk over worden ingelicht, er grote risico's zijn. Daarom pleit ze nogmaals, zeer concreet, voor een verbod op de gezichtsherkenningstechnologieën.

**Mevrouw Nicha Mbuli** stelt dat het voor personen die te maken krijgen met profilering via gezichtsherkenning bijzonder moeilijk is om gehoord te worden. Het is voor iemand die dagelijks met discriminatie en racisme te maken krijgt al moeilijk om aan te tonen dat hij of zij gediscrimineerd wordt. Bewijzen dat de technologie je discrimineert, zal nog moeilijker zijn.

Zij merkt voorts op dat er een wet ter bestrijding van discriminatie bestaat, een algemene wet over alle vormen van discriminatie, die echter geen rekening houdt met alle vormen van discriminatie die er met de komst van gezichtsherkenning nog kunnen bij komen.

Sommigen zijn van mening dat de nieuwe technologieën het werk van de politie zullen vereenvoudigen. Zij denkt echter dat ze er eerder toe zullen leiden dat iedere verantwoordelijkheid bij de politie wordt weggenomen. Het zal immers de machine zijn die aan de politie meldt dat ze een overeenkomst heeft gevonden. De agent zal niet langer zijn ervaring of zijn terreinkennis gebruiken. De machine beslist en de politie past die beslissing toe.

Daarnaast meent ze dat het weinig uitmaakt hoe databanken zijn opgebouwd. Mensen zullen nog steeds op basis van eerder racialistische ideeën gecategoriseerd worden. Vertrouwen hebben in machines en hun neutraliteit promoten vormt echt een gevaar voor al het werk dat is verricht in de strijd tegen discriminatie en racisme.

**De heer Rémy Farge** verklaart dat er zonder transparantie illegale testen plaatsvonden. Daarnaast wordt onderzocht hoe illegaal toegepaste praktijken kunnen worden gelegaliseerd. Er worden commissies opgericht die schijnbaar in de toekomst een kader voor het gebruik van de betrokken technologieën moeten uitwerken. Het feit dat daarover geen informatie beschikbaar is, toont duidelijk aan dat de bereidheid om transparant te werken ontbreekt. Op die manier wordt het debat bij de indieners van de petitie weggehaald en aan een commissie toevertrouwd, zodat die in alle onafhankelijkheid een wettelijk kader kan uitwerken.

Hij zegt te denken dat Brussel een model kan zijn. Gezien de bevoegdheden van Brussel, gezien wat we in Brussel waarnemen en wat eerder werd beschreven, zou een sterk en goed onderbouwd standpunt van Brussel ook federaal een alarm kunnen laten afgaan en een zekere druk kunnen uitoefenen die federaal voelbaar zou kunnen zijn.

Hij wijst nogmaals op de noodzaak van meer transparantie. De Ligue des droits humains startte een campagne om toegang te vragen tot de administratieve documenten om een reeks vragen te kunnen stellen, in het

dispositifs de surveillance utilisés en Région bruxelloise. Pour l'heure aucune réponse n'a été donné par safe.brussels. Il y a donc là aussi des enjeux de transparence.

Pour ce qui est des questions concernant un cadre légal qui permettrait quelques exceptions à l'interdiction d'utiliser la reconnaissance faciale, l'orateur indique que des phénomènes tels que les disparitions d'enfants, le terrorisme ou la criminalité grave doivent être absolument combattus et qu'il ne veut en rien les minimiser. Il met également en garde quant au fait que de telles exceptions ne constituent pas une proection pour les citoyens, mais sont en réalité une porte ouverte ou un tapis rouge pour les grandes entreprises qui développent ces solutions et qui n'auront de cesse d'élargir au maximum le champ de ces exceptions.

Les caméras ANPR peuvent servir d'exemple en la matière. Au début, il a été question de lutte contre le terrorisme et de motifs écologiques à Bruxelles. Par la suite, on voit qu'il est très facile, par la publication d'arrêtés, d'augmenter les finalités et les usages de ces caméras.

Un rapport d'Amnesty International aux Pays-Bas a constaté que dans la ville de Roermond, il était question de discriminations dans des projets de police prédictive, où les personnes venant de pays de l'Est risquaient des contrôles systématiques. Il s'agissait là d'une pratique absolument discriminatoire que permettaient les caméras ANPR déjà installées dans la ville.

Il estime que quand il est question de traiter des données biométriques, il existe un risque de facto. L'exception, quelle qu'elle soit, constituera une porte ouverte où s'engouffreront sans aucun doute les entreprises, qui n'attendent que cela.

Dès lors, le principe de subsidiarité doit être le guide. S'il est demandé une interdiction totale de la reconnaissance faciale, ce n'est pas parce qu'on ne veut pas traiter ces phénomènes-là, mais bien parce qu'il faut poser la question des meilleures méthodes qui permettraient de lutter contre le phénomène et qui soient les moins attentatoires aux droits fondamentaux. Il considère que pour chaque question posée, des réponses moins attentatoires que la reconnaissance faciale existent. A titre d'exemple, pour la problématique des disparitions d'enfants, le secteur de l'aide à la jeunesse est en première ligne à Bruxelles sur les questions de fugues et de disparitions, mais que ce secteur manque cruellement de moyens. Pourtant, il est au contact des familles et des enfants et il est le plus à même de répondre à ces problèmes et de comprendre ces problématiques, avec l'aide des chercheurs notamment, alors que la technologie ne permet aucunement de répondre à ces questions.

Il indique encore que le terme de solutionnisme technologique lui importe beaucoup parce qu'en fait, non seulement la technologie ne répond pas aux questions mais en plus, elle empêche de répondre aux vraies questions qui permettraient de trouver de bonnes solutions.

bijzonder over de in Brussel ingezette bewakingsmiddelen. Tot nu toe heeft safe.brussels daar niet op gereageerd. Ook daar laat de transparantie dus nog te wensen over.

Met betrekking tot vragen over een wettelijk kader dat enkele uitzonderingen zou toestaan op het verbod op het gebruik van gezichtsherkenning, wijst hij erop dat verschijnselen als de verdwijning van kinderen, terrorisme en zware criminaliteit absoluut moeten worden bestreden en dat hij die geenszins wil bagatelliseren. Hij waarschuwt ook dat dergelijke uitzonderingen geen bescherming voor burgers vormen, maar in feite een open deur of een rode loper zijn voor grote bedrijven die deze oplossingen ontwikkelen en niet zullen rusten voor de reikwijdte van deze uitzonderingen zo groot mogelijk is.

De ANPR-camera's kunnen wat dat betreft als voorbeeld dienen. Aanvankelijk ging het in Brussel over de strijd tegen het terrorisme en over ecologische motieven. Vervolgens zagen we dat het erg eenvoudig is om via de publicatie van besluiten de toepassingen en het gebruik van de camera's uit te breiden.

In een verslag komt Amnesty International Nederland tot de vaststelling dat in de stad Roermond sprake was van discriminatie in voorspellende politieprojecten, waarbij personen die uit Oostbloklanden kwamen, het risico liepen systematisch te worden gecontroleerd. Het ging om een discriminerende praktijk die mogelijk werd door eerder in de stad geplaatste ANPR-camera's.

Hij is van mening dat er de facto een risico bestaat als biometrische gegevens behandeld worden. Om het even welke uitzondering zal een opening bieden waar de bedrijven, die daarop zitten te wachten, zich gretig in zullen storten.

Daarom moet het subsidiariteitsbeginsel vooropstaan. Als er om een volledig verbod op gezichtsherkenning wordt gevraagd, is dat niet omdat de betrokkenen niet willen dat dergelijke fenomenen niet worden aangepakt, maar omdat moet worden onderzocht welke de beste methoden zijn om het fenomeen te bestrijden die de grondrechten het minst aantasten. Hij gelooft dat er minder indringende oplossingen zijn dan gezichtsherkenning voor elke vraag die wordt gesteld. Wat bijvoorbeeld de kwestie van vermiste kinderen betreft, staat de jeugdzorgsector in Brussel in de frontlinie als het gaat om weglopers en verdwijningen, maar deze sector beschikt over veel te weinig middelen. Toch staat de sector in contact met gezinnen en kinderen en is hij het beste in staat om op problemen te reageren en ze te begrijpen, met de hulp van onderzoekers in het bijzonder, terwijl technologie die vragen niet kan beantwoorden.

Hij wijst er voorts op dat de term technologisch oplossingsgericht denken belangrijk is, omdat de technologie in feite niet alleen geen antwoord biedt op de vragen, maar bovendien verhindert om in te gaan op de reële vragen, wat het vinden van goede oplossingen mogelijk zou maken.

Une étude du Royaume-Uni, un des pays les plus équipés en vidéosurveillance en général et qui utilise la reconnaissance faciale depuis 2016, a démontré que 80 % des suspects signalés par le logiciel étaient en fait des innocents.

L'orateur indique qu'il pourrait aussi parler de la ville de Cologne, en Allemagne, qui place des caméras près de lieux sensibles. En Italie, c'est le cas dans les lieux sensibles, dans des cabinets médicaux, des bars, des lieux de culte ou encore des lieux fréquentés par des personnes LGBTQIA+, etc. Dans la ville de Côme, en Italie, des systèmes de surveillance biométrique ont été installés contre celles et ceux qui flânaient en rue. En fait cela visait les personnes sans domicile fixe qui tentaient d'exister dans l'espace public. Et en Pologne, il semblerait que la reconnaissance faciale était également utilisée lors de la crise du covid pour contrôler le respect des mesures prises.

Il réagit à la question qui concernait le fait qu'après les attentats de Bruxelles, l'homme au chapeau a été recherché. Un homme, Fayçal Cheffou, a fait l'objet d'une arrestation extrêmement violente, une expérience traumatisante au cours de laquelle il aurait pu mourir, alors que l'enquête a rapidement démontré qu'en fait, il ne s'agissait pas de l'homme impliqué dans les attentats. Mais qu'en aurait-il été si c'était une machine qui avait dû identifier une personne sur la base d'une photo un peu floue. Cette personne innocente aurait-elle pu être lavée de tout soupçon ? Qui sera, demain, en mesure de contredire les conclusions de la machine ? La question se pose réellement.

Il conclut en indiquant qu'il ne faut pas croire qu'une demande d'interdiction de la reconnaissance faciale telle que proposée, manque de nuances. Au contraire, elle invite à la nuance parce qu'elle invite à repenser les phénomènes sociaux un par un, sans souscrire à l'idée d'une technologie qui résoudrait tout en une fois. De plus, quelles que soient les exceptions prévues par un cadre légal, il subsisterait toujours un risque de piratage et donc d'utilisation de nos données biométriques par des personnes malveillantes. Le risque de discrimination ou le risque que le champ des exceptions soit élargi par la suite avec des usages qui se multiplient, notamment pour des personnes qui n'ont rien à se reprocher, comme par exemple des manifestants ou des personnes sans-papiers qui tentent de survivre à Bruxelles, sont bien réels et aucun cadre légal ne pourrait, à long terme ou même à court terme, les prévenir.

Enfin, il indique encore que la reconnaissance faciale ou la surveillance biométrique ne correspondent pas à des pratiques existantes, avec de la technologie en plus. En effet, la surveillance biométrique est une surveillance de masse, avec tous les dangers qui ont été décrits.

Il rappelle que le Parlement bruxellois a des compétences qui lui permettent d'agir. Une résolution, par exemple, permettrait une prise de position qui serait exemplaire en Belgique et en Europe.

Uit een studie uit het Verenigd Koninkrijk, een van de landen waar de camerabewaking in het algemeen het verst is uitgebouwd en waar sinds 2016 gezichtsherkenning wordt gebruikt, bleek dat 80% van de door software gesignaleerde verdachten eigenlijk onschuldig was.

De spreker stelt dat hij het ook over de Duitse stad Keulen zou kunnen hebben, die in de buurt van gevoelige plekken camera's plaatst. In Italië gebeurt dat op gevoelige plekken, in dokterskabinetten, in bars, in gebedshuizen, op plaatsen waar LGBTQIA+-personen komen enzovoort. In de Italiaanse stad Como zijn biometrische bewakingssystemen geïnstalleerd tegen mensen die op straat rondhingen, dus mensen zonder vast adres die in de openbare ruimte trachtten te overleven. In Polen zou gezichtsherkenning dan weer gebruikt zijn tijdens de covidcrisis om te controleren of de maatregelen werden nageleefd.

Hij reageert op de vraag die betrekking had op het feit dat na de aanslagen in Brussel de man met het hoedje werd gezocht. Een man, Faycal Cheffou, werd op een bijzonder gewelddadige manier gearresteerd. Dat was een traumatiserende ervaring, waarbij hij had kunnen sterven, terwijl het onderzoek snel aantoonde dat het niet om de man ging die bij de aanslagen betrokken was. Wat zou er echter zijn gebeurd wanneer het een machine was geweest die een persoon had moeten identificeren op basis van een wat wazige foto? Zou die onschuldige persoon dan ook van alle verdenkingen gezuiverd zijn? Wie zal in de toekomst de conclusies van de machine kunnen weerleggen? Dat is iets wat we ons moeten afvragen.

Vervolgens stelt hij dat we niet moeten denken dat de vraag om een verbod op gezichtsherkenning onvoldoende genuanceerd is. Integendeel, ze zet aan tot nuanceren, want ze stimuleert ons om de sociale fenomenen een voor een opnieuw onder de loep te nemen, zonder te kiezen voor één technologie die alles in één keer zou kunnen oplossen. Bovendien zou er, ongeacht welke uitzonderingen er binnen het wettelijke kader mogelijk zouden zijn, altijd een risico bestaan op hacking en dus op het gebruik van onze biometrische gegevens door kwaadwillige personen. Het risico op discriminatie of het risico dat het toepassingsgebied van de uitzonderingen vervolgens wordt uitgebreid doordat de technologie voor almaar meer doeleinden wordt gebruikt, is met name voor personen die niets misdaan hebben, zoals manifestanten of mensen zonder papieren die trachten te overleven in Brussel, wel degelijk reëel en kan op de lange termijn of zelfs op korte termijn met geen enkel wettelijk kader worden voorkomen.

Ten slotte wijst hij er nog op dat gezichtsherkenning of biometrisch toezicht niet overeenstemmen met bestaande praktijken waar het gebruik van technologie bovenop komt. Biometrisch toezicht is immers een vorm van massatoezicht, dat gepaard gaat met de eerder beschreven gevaren.

Hij wijst erop dat het Brussels Parlement over bevoegdheden beschikt om op te treden. Zo zou het bijvoorbeeld in een resolutie een standpunt kunnen innemen dat België en Europa tot voorbeeld zou kunnen dienen.

**M. Hicham Talhi** indique vouloir absolument s'inscrire en faux contre les propos de M. De Beukelaer concernant la neutralité des technologies.

Il rappelle également que la technologie dépasse actuellement déjà le cadre légal. Par ailleurs, il souhaiterait restreindre ce cadre. Certes, le fait d'être filmé pour prévenir, par exemple, des faits de terrorisme peut se justifier, mais il faudrait alors veiller à ce que ce soit la seule application de cette technologie.

Il souligne encore que pour certains de ses collègues, la société démocratique est un acquis intangible, mais rien ne le garantit. On ignore, par exemple, quelles seront les forces en présence à l'issue des prochaines élections. Le fait de permette un usage de ces technologies nous rendrait, dans un tel cas, vulnérables.

Par ailleurs, il y a aussi le risque que l'intelligence artificielle cherche par elle-même à remplir la tâche qui lui a été assignée, en contournant les barrières qui seraient érigées, avec toutes les dérives que cela pourrait apporter.

Il ne souhaite donc pas que nos policiers soient équipés, demain, de casques Apple pro avec l'intelligence artificielle intégrée, en pensant que ce serait une amélioration de nos sociétés.

La position de son groupe est claire, il faut faire respecter le cadre légal et il est favorable au dépôt d'une résolution en ce sens. Par ailleurs, il rappelle être favorable à une audition de la commission de contrôle bruxellois pour voir où en est l'utilisation de cette technologie.

Il remercie encore les coauteurs de la pétition d'avoir rappelé au Parlement la responsabilité du pouvoir législatif en la matière.

**Le président** remercie à son tour les trois orateurs, représentants de tous ceux qui ont signé la pétition.

Leur exposé très pédagogique a permis aux membres de la commission de bien comprendre quelle est leur position.

La commission va maintenant réfléchir aux deux éléments qui lui ont été soumis par le rapporteur, à savoir la possibilité de rédiger une résolution et le fait d'auditionner, éventuellement, der représentants de notre institution bruxelloise de contrôle.

**De heer Hicham Talhi** maakt uitdrukkelijk bezwaar tegen de uitspraken van de heer De Beukelaer over de neutraliteit van de technologie.

Hij wijst erop dat de technologie nu al buiten het wettelijke kader treedt. Zelf zou hij overigens dat kader willen beperken. Personen filmen om bijvoorbeeld terroristische daden te voorkomen, valt misschien wel te rechtvaardigen, maar in dat geval moet erop worden toegezien dat de technologie uitsluitend daarvoor wordt gebruikt.

Hij benadrukt verder dat voor sommige van zijn collega's de democratische samenleving een onaantastbare verworvenheid is, maar niets kan dat garanderen. Zo weten we bijvoorbeeld helemaal niet wie er na de volgende verkiezingen aan de macht zal zijn. Het gebruik van dergelijke technologieën toelaten, maakt ons in een dergelijk geval kwetsbaar.

Het risico bestaat overigens dat artificiële intelligentietoepassingen zelf trachten de opdracht uit te voeren die ze toegewezen kregen en daarbij de opgetrokken barrières omzeilen, wat allerlei ontsporingen kan veroorzaken.

Hij wil dan ook niet dat onze politieagenten in de toekomst een Apple pro-koptelefoon met ingebouwde artificiële intelligentie krijgen, waarbij er wordt van uitgegaan dat dat een verbetering zou zijn voor onze samenleving.

Het standpunt van zijn fractie is duidelijk: de naleving van het wettelijke kader moet worden afgedwongen. Hij is voorstander van de indiening van een resolutie in die zin. Hij staat trouwens positief tegenover een hoorzitting met de Brusselse controlecommissie om na te gaan hoever het gebruik van de technologie staat.

Hij dankt tot slot de coauteurs van de petitie omdat ze de verantwoordelijkheid van de wetgever op dit gebied onder de aandacht van het parlement hebben gebracht.

**De voorzitter** dankt op zijn beurt de drie sprekers, die alle ondertekenaars van de petitie vertegenwoordigen.

Hun erg leerzame uiteenzetting heeft ervoor gezorgd dat de commissieleden een duidelijk beeld hebben gekregen van hun standpunt.

De commissie zal nu de twee voorstellen van de rapporteur bekijken, namelijk de mogelijkheid om een resolutie op te stellen en een eventuele hoorzitting met vertegenwoordigers van de Brusselse controle-instelling.

## IV. Clôture des débats

La commission décide de clore l'échange de vues et de publier un rapport qui sera transmis, pour information, au ministre-président du Gouvernement de la Région de Bruxelles-Capitale.

*- Confiance est faite au rapporteur pour la rédaction du rapport.*

*Le rapporteur* *Le président*

Hicham TALHI Guy VANHENGEL

## IV. Afsluiting van de bespreking

De commissie beslist om de gedachtewisseling te sluiten en een verslag te publiceren dat, ter informatie, zal worden verzonden naar de minister-president van de Brusselse Hoofdstedelijke Regering.

*- Vertrouwen wordt geschonken aan de rapporteur voor het opstellen van het verslag.*

*De rapporteur* *De voorzitter*

Hicham TALHI Guy VANHENGEL