DOC 55 **1349/001**

CHAMBRE DES REPRÉSENTANTS
DE BELGIQUE

16 juin 2020

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

(déposée par M. Gilles Vanden Burre,
Mme Jessika Soors et
M. François De Smet)

BELGISCHE KAMER VAN
VOLKSVERTEGENWOORDIGERS

16 juni 2020

VOORSTEL VAN RESOLUTIE

over een driejarig moratorium op het gebruik van gezichtsherkenningssoftware en -algoritmen in vaste of mobiele beveiligingscamera's in openbare en privéplaatsen

(ingediend door de heer Gilles Vanden Burre,
mevrouw Jessika Soors en
de heer François De Smet)

N-VA	:	*Nieuw-Vlaamse Alliantie*
Ecolo-Groen	:	*Ecologistes Confédérés pour l'organisation de luttes originales – Groen*
PS	:	*Parti Socialiste*
VB	:	*Vlaams Belang*
MR	:	*Mouvement Réformateur*
CD&V	:	*Christen-Democratisch en Vlaams*
PVDA-PTB	:	*Partij van de Arbeid van België – Parti du Travail de Belgique*
Open Vld	:	*Open Vlaamse liberalen en democraten*
sp.a	:	*socialistische partij anders*
cdH	:	*centre démocrate Humaniste*
DéFI	:	*Démocrate Fédéraliste Indépendant*
INDEP-ONAFH	:	*Indépendant - Onafhankelijk*

Abréviations dans la numérotation des publications:		*Afkorting bij de numering van de publicaties:*	
DOC 55 0000/000	*Document de la 55e législature, suivi du numéro de base et numéro de suivi*	*DOC 55 0000/000*	*Parlementair document van de 55e zittingsperiode + basisnummer en volgnummer*
QRVA	*Questions et Réponses écrites*	*QRVA*	*Schriftelijke Vragen en Antwoorden*
CRIV	*Version provisoire du Compte Rendu Intégral*	*CRIV*	*Voorlopige versie van het Integraal Verslag*
CRABV	*Compte Rendu Analytique*	*CRABV*	*Beknopt Verslag*
CRIV	*Compte Rendu Intégral, avec, à gauche, le compte rendu intégral et, à droite, le compte rendu analytique traduit des interventions (avec les annexes)*	*CRIV*	*Integraal Verslag, met links het definitieve integraal verslag en rechts het vertaald beknopt verslag van de toespraken (met de bijlagen)*
PLEN	*Séance plénaire*	*PLEN*	*Plenum*
COM	*Réunion de commission*	*COM*	*Commissievergadering*
MOT	*Motions déposées en conclusion d'interpellations (papier beige)*	*MOT*	*Moties tot besluit van interpellaties (beigekleurig papier)*

DÉVELOPPEMENTS

MESDAMES, MESSIEURS,

Dans notre société, de plus en plus de tâches sont désormais accomplies par des machines et des robots, un processus qui, s'il n'est pas vraiment neuf, semble aujourd'hui s'accélérer.

Cette évolution ne s'arrête pas à la robotique et au numérique mais concerne aussi la montée en puissance de l'intelligence artificielle (IA), de l'Internet des Objets (IdO) ou encore des mégadonnées (big data). Les changements dans ces domaines sont ultra rapides, amples et profonds et vont bouleverser l'ensemble des aspects de notre vie en société. À ce propos, une des questions fondamentales à se poser concernant l'IA est "que souhaitons-nous en faire?" et "dans quels domaines avons-nous l'intention d'y faire appel?".

Imaginons-nous que des logiciels apparentés à l'IA rendent des avis, voire prennent des décisions, dans des domaines aussi sensibles que la santé, la sécurité publique, la justice, ou encore la migration? Si oui, du moins en partie, avec quelles balises, quelle autorité de tutelle, ou selon quelles modalités?

En Belgique, en juillet 2019, nous apprenions par la voix du commissaire général Marc De Mesmaeker que la police allait "commencer à utiliser les caméras à reconnaissance faciale à l'aéroport de Bruxelles-National". Le commissaire général souhaitait alors que des caméras à reconnaissance faciale soient placées en certains endroits "le plus rapidement possible"[1].

Plus récemment, plusieurs événements nous ont interpellé. Par exemple, en réaction à la crise sanitaire liée au COVID-19, *Uber* envisage de rendre obligatoire dans certains pays le port du masque de protection par ses conducteurs lorsqu'ils transportent des passagers en comptant sur la reconnaissance faciale pour faire respecter les règles[2]. Par ailleurs, alors lors que le port du masque est désormais obligatoire en France dans le métro et le RER, des caméras installées à Paris dénombrent en temps réel les voyageurs non équipés. Si la RATP assure qu'il "n'a aucune finalité de verbalisation",

1 BELGA, cité par *"Des caméras avec reconnaissance faciale à Brussels Airport"*, site internet de *la Libre*, le 9 juillet 2019.

2 *"Uber veut utiliser la reconnaissance faciale pour s'assurer que ses conducteurs portent des masques",* site internet de *MetroTime*, 5 mai 2020.

TOELICHTING

DAMES EN HEREN,

Steeds meer taken in onze samenleving worden overgenomen door machines en robots. Dat proces is niet bepaald nieuw, maar het lijkt nu wel in een stroomversnelling te komen.

De evolutie blijft echter niet beperkt tot robotica en digitale toepassingen; zij behelst ook de forse opmars van de artificiële intelligentie (AI), van het *Internet of Things* (IoT) en van de megagegevensverwerking (*big data*). De veranderingen verlopen razendsnel, gaan in de breedte en de diepte en veranderen heel ons maatschappelijk systeem. Enkele van de fundamentele vragen die met betrekking tot AI rijzen, zijn: "wat willen we ermee doen?" en "in welke domeinen zijn we van plan er gebruik van te maken?".

Willen we dat met AI uitgeruste software adviezen uitbrengt of zelfs beslissingen neemt in hoogst heikele aangelegenheden als gezondheid, openbare veiligheid, justitie of migratie? Mocht zulks – dan toch deels – kunnen, binnen welk raamwerk, onder welke toezichthoudende overheid en volgens welke nadere voorwaarden moet dat dan gebeuren?

In België gaf commissaris-generaal Marc De Mesmaeker in juli 2019 aan dat de politie zou beginnen gezichtsherkenningscamera's te gebruiken op de luchthaven van Zaventem. De commissaris-generaal wilde dat die camera's er op sommige plaatsen zo snel mogelijk zouden komen[1].

Recenter zijn er ook feiten geweest die vragen oproepen. Als reactie op de COVID-19-gezondheidscrisis overweegt Uber zijn chauffeurs in sommige landen te verplichten een masker te dragen wanneer zij passagiers vervoeren, waarbij het van gezichtsherkenning gebruik wil maken om de regels in acht te doen nemen[2]. In Frankrijk is het dragen van een masker voortaan verplicht op de metro en in het RER, en in Parijs hangen camera's waar in realtime de reizigers zonder masker worden geteld. Hoewel de Parijse stadsvervoeruitbater (RATP) benadrukt dat de camera's geenszins dienen om

1 BELGA, geciteerd in *Des caméras avec reconnaissance faciale à Brussels Airport*, website van *La Libre Belgique*, 9 juli 2019.

2 *Uber veut utiliser la reconnaissance faciale pour s'assurer que ses conducteurs portent des masques,* website *MetroTime*, 5 mei 2020.

le dispositif inquiète plusieurs associations des défense des libertés[3].

Le CNIL (Commission Nationale de l'Informatique et des Libertés en France) définit la reconnaissance faciale comme suit: "*La reconnaissance faciale est une technique qui permet à partir des traits de visage: d'authentifier une personne: c'est-à-dire, vérifier qu'une personne est bien celle qu'elle prétend être (dans le cadre d'un contrôle d'accès); ou d'identifier une personne: c'est-à-dire, de retrouver une personne au sein d'un groupe d'individus, dans un lieu, une image ou une base de données*"[4].

La biométrie, quant à elle, "*regroupe l'ensemble des techniques informatiques permettant d'identifier un individu à partir de ses caractéristiques physiques, biologiques, voire comportementales (empreintes digitales, iris, voix, visage ou même la démarche)*"[5].

Aux États-Unis, la reconnaissance faciale est largement utilisée, que ce soit dans les stades de foot, les concerts, les aéroports, et par plusieurs corps de police. Par exemple, les autorités avaient utilisé la reconnaissance faciale à Annapolis après une fusillade[6].

Il est intéressant de se pencher sur l'exemple de la Californie à cet égard. Les policiers de Californie n'ont pas le droit d'utiliser des logiciels de reconnaissance faciale sur leurs caméras embarquées selon une loi ratifiée en octobre 2019 par le gouverneur démocrate de l'État. La loi concernée est la loi *"AB 1215"* ou "*Body Camera Accountability Act"*[7]. Elle a été portée par Phil Ting, député démocrate américain[8].

te bekeuren, baart deze ingreep meerdere verenigingen die voor de vrijheden opkomen, grote zorgen[3].

De Franse nationale commissie voor informatica en vrijheden (*Commission Nationale de l'Informatique et des Libertés* – CNIL) definieert gezichtsherkenning als volgt: "*La reconnaissance faciale est une technique qui permet à partir des traits de visage: d'authentifier une personne: c'est-à-dire, vérifier qu'une personne est bien celle qu'elle prétend être (dans le cadre d'un contrôle d'accès); ou d'identifier une personne: c'est-à-dire, de retrouver une personne au sein d'un groupe d'individus, dans un lieu, une image ou une base de données*".[4]

De biometrie dan weer *"regroupe l'ensemble des techniques informatiques permettant d'identifier un individu à partir de ses caractéristiques physiques, biologiques, voire comportementales (empreintes digitales, iris, voix, visage ou même la démarche)"*[5].

In de Verenigde Staten is gezichtsherkenning alomtegenwoordig bij voetbalwedstrijden, bij concerten, op luchthavens en bij heel wat politiekorpsen. Na de schietpartij in Annapolis hadden de autoriteiten gezichtsherkenning ingezet[6].

In dat opzicht is het interessant het voorbeeld van Californië onder de loep te nemen. Ingevolge een wet die in oktober 2019 door de democratische gouverneur van de staat California werd uitgevaardigd, mag de Californische politie geen dashcams met gezichtsherkenningssoftware gebruiken. De betrokken wet is de wet *AB 1215*, ook de *Body Camera Accountability Act*[7] genoemd. De geestelijke vader van de wet is Phil Ting, een afgevaardigde van de Democraten[8].

---

3 DE BAUDOUIN, P., *"A Châtelet, des caméras comptabilisent les voyageurs sans masque: une "banalisation" de la surveillance?"*, site internet de France 3, 12 mai 2020.

4 *"Définition: reconnaissance faciale"*, site internet de la CNIL.

5 *"Le contrôle d'accès biométrique sur les lieux de travail"*, site internet de la CNIL, le 28 mars 2019.

6 CONGER, K., FAUSSET R., et KOVALESKI S.F., *"San Francisco Bans Facial Recognition Technology"*, site Internet du New York Times, le 14 mai 2019. [Notre traduction]

7 *"AB-1215 Law enforcement: facial recognition and other biometric surveillance"*, California Legislative Information Website, URL: *https:///leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB1215*, consulté le 15 mai 2020.

8 AFP, cité par *"La Californie interdit la reconnaissance faciale sur les caméras des policiers"*, site internet d'RTL Info, le 10 octobre 2019.

3 DE BAUDOUIN, P., *A Châtelet, des caméras comptabilisent les voyageurs sans masque: une "banalisation" de la surveillance?*, website van France 3, 12 mei 2020.

4 *Définition: reconnaissance faciale*, website CNIL. Onze vertaling: Gezichtsherkenning is een techniek waarmee aan de hand van gelaatstrekken kan worden overgegaan tot de authenticatie van een persoon (om na te gaan of iemand wel degelijk is wie hij beweert te zijn, bijvoorbeeld in het raam van een toegangscontrole), dan wel tot de identificatie van een persoon (om een welbepaald persoon op te sporen in een groep van mensen, op een plaats, op beeldmateriaal of in een databank).

5 *Le contrôle d'accès biométrique sur les lieux de travail*, website CNIL, 28 maart 2019.

6 CONGER, K., FAUSSET R., en KOVALESKI S.F., *San Francisco Bans Facial Recognition Technology*, website New York Times, 14 mei 2019.

7 *AB-1215 Law enforcement: facial recognition and other biometric surveillance*, website California Legislative Information, zie: *https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB1215*, geraadpleegd op 15 mei 2020.

8 AFP, geciteerd in *La Californie interdit la reconnaissance faciale sur les caméras des policiers*, website RTL Info, 10 oktober 2019.

Sur le *California Legislative Information Website*, nous pouvons lire que *"This bill would prohibit a law enforcement agency or law enforcement officer from installing, activating, or using any biometric surveillance system in connection with an officer camera or data collected by an officer camera. The bill would authorize a person to bring an action for equitable or declaratory relief against a law enforcement agency or officer who violates that prohibition. (…) The bill would repeal these provisions on January 1, 2023"*[9].

Aux USA, San Francisco n'était pas seule à interdire la reconnaissance faciale l'année dernière. La ville voisine d'Oakland allait rapidement suivre, tout comme Somerville et Brookline dans le Massachusetts. En décembre 2019, San Diego suspendait un programme de reconnaissance faciale. Quarante grands festivals de musique se sont engagés à ne pas utiliser cette technologie, et des militants appellent à une interdiction à l'échelle nationale. Enfin, de nombreux candidats démocrates à la présidentielle soutiennent au moins une interdiction partielle de la technologie[10].

L'année dernière, Bradford L. Smith, le président de *Microsoft*, a averti que la technologie était trop risquée pour que les entreprises la contrôlent seules et a demandé au Congrès de superviser son utilisation[11]. Un chercheur du *Microsoft Research Montréal* a décrit la surveillance faciale comme "le plutonium de l'intelligence artificielle", ajoutant: *"it should be recognized as anathema to the health of human society, and heavily restricted as a result"*[12].

Selon le directeur du *Georgetown University's Center on Privacy and Technology: "This is the most pervasive and risky surveillance technology of the 21st century"*[13].

Par ailleurs, certaines expérimentations ont prouvé les limites d'une telle technologie. Par exemple, en juillet 2018, l'*American Civil Liberties Union* reportait qu'une technologie de reconnaissance faciale d'*Amazon*, qui est utilisée par certains services de police et d'autres organisations, *"incorrectly matched the lawmakers*

Op de website *California Legislative Information* lezen we: *"This bill would prohibit a law enforcement agency or law enforcement officer from installing, activating, or using any biometric surveillance system in connection with an officer camera or data collected by an officer camera. The bill would authorize a person to bring an action for equitable or declaratory relief against a law enforcement agency or officer who violates that prohibition. (…) The bill would repeal these provisions on January 1, 2023"*[9].

Het gebruik van gezichtsherkenning werd vorig jaar verboden in San Francisco, maar het bleef niet bij die stad. Het naburige Oakland zou al snel volgen, evenals de steden Somerville en Brookline in de staat Massachusetts. In San Diego werd in december 2019 een gezichtsherkenningsprogramma stopgezet. Veertig grote muziekfestivals hebben zich ertoe verbonden die technologie niet langer te gebruiken; intussen pleiten militanten voor een verbod over het hele land. Tot slot steunen veel democratische kandidaten voor het presidentschap een minstens gedeeltelijk verbod op die technologie[10].

Vorig jaar heeft Bradford L. Smith, de voorzitter van *Microsoft*, gewaarschuwd dat de technologie nog te gevaarlijk was om de controle ervan louter in handen van de bedrijfswereld te geven, en heeft hij het Congres gevraagd het gebruik ervan te controleren[11]. Een onderzoeker van *Microsoft Research Montréal* heeft gezichtsherkenning omschreven als "het plutonium van de artificiële intelligentie". Meer nog: *"it should be recognized as anathema to the health of human society, and heavily restricted as a result"*[12].

Bij de directeur van het *Georgetown University's Center on Privacy and Technology* klinkt het: *"This is the most pervasive and risky surveillance technology of the 21st century"*[13].

Sommige experimenten hebben bovendien de limieten van een dergelijke technologie aangetoond. Zo bracht de *American Civil Liberties Union* in juli 2018 uit dat een gezichtsherkenningstechnologie van *Amazon*, die wordt gebruikt door sommige politiediensten en andere organisaties, *"incorrectly matched the lawmakers with*

9 *"AB-1215 Law enforcement: facial recognition and other biometric surveillance"*, California Legislative Information Website, URL: *https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB1215*, consulté le 15 mai 2020.

10 SCHNEIER, B., *"Opinion: We're Banning Facial Recognition. We're Missing the Point",* site Internet du New York Times, le 20 janvier 2020. [Notre traduction]

11 CONGER, K., FAUSSET R., et KOVALESKI S.F., …

12 *Idem.*

13 *Idem.*

9 *AB-1215 Law enforcement: facial recognition and other biometric surveillance*, *op.cit*.

10 SCHNEIER, B., *Opinion: We're Banning Facial Recognition. We're Missing the Point,* website New York Times, 20 januari 2020.

11 CONGER, K., FAUSSET R., en KOVALESKI S.F., *op.cit.*

12 *Idem.*

13 *Idem.*

with people who had been charged with a crime"[14]. Et l'*American Civil Liberties Union* et d'autres groupes à but non lucratif ont appelé l'année dernière *Amazon* à cesser de vendre sa technologie *"Rekognition"* aux forces de l'ordre[15].

Une autre étude (*"Gender Shades"*) a indiqué que les systèmes d'*IBM* et de *Microsoft* étaient bien meilleurs pour identifier le genre des visages d'hommes blancs que pour identifier le genre des visages à la peau plus foncée ou les visages féminins[16].

En réaction à l'interdiction de technologies de reconnaissance faciale par plusieurs États des États-Unis, un article de SCHNEIER B. de la *Harvard Kennedy School* est particulièrement éclairant.

Considérant que *"facial recognition bans are the wrong way to fight against modern surveillance"*[17], l'auteur met en avant trois composantes importantes de la surveillance de masse que sont *"l'identification, la corrélation et la discrimination"*:

"*In all cases, modern mass surveillance has three broad components: identification, correlation and discrimination. (…) We might be completely anonymous in a system that uses unique cookies to track us as we browse the internet, but the same process of correlation and discrimination still occurs. It's the same with faces (…)*"[18].

Et d'ajouter en ce qui concerne la régulation:

"*Regulating this system means addressing all three steps of the process. A ban on facial recognition won't make any difference if, in response, surveillance systems switch to identifying people by smartphone MAC addresses. The problem is that we are being identified without our knowledge or consent, and society needs rules about when that is permissible*"[19].

Et d'affirmer qu'il faut être particulièrement vigilant à propos de la *combinaison des données*:

"Similarly, we need rules about how our data can be combined with other data, and then bought and sold

14 SINGER, N., *"Amazon's Facial Recognition Wrongly Identifies 28 Lawmakers, A.C.L.U. Says"*, site internet du New York Times, le 26 juillet 2018.
15 CONGER, K., FAUSSET R., et KOVALESKI S.F., …
16 *Idem*
17 SCHNEIER, B., *"Opinion: We're Banning Facial Recognition. We're Missing the Point",* site internet du New York Times, le 20 janvier 2020.
18 *Idem.*
19 *Idem.*

people who had been charged with a crime"[14]. De *American Civil Liberties Union* en andere groepen zonder winstoogmerk hebben vorig jaar *Amazon* ertoe opgeroepen zijn *Rekognition*-technologie niet langer te verkopen aan de ordehandhavingsdiensten[15].

Een ander onderzoek (*Gender Shades*) heeft aangetoond dat de systemen van IBM en Microsoft efficiënter zijn om het gender van gezichten van blanke mannen te identificeren, dan om te bepalen wat het geslacht is van iemand met een donkere gelaatskleur of om gezichten van vrouwen te herkennen[16].

Bruce Schneier van de *Harvard Kennedy School* schreef als reactie op het door meerdere Amerikaanse staten opgelegde verbod op gezichtsherkenningstechnologieën een bijzonder verhelderend artikel[17].

Gelet op het feit dat een verbod op gezichtsherkenning niet de juiste manier is om de strijd aan te binden tegen dergelijke toezichtsmethoden. Hij wijst erop dat massatoezicht drie belangrijke componenten omvat: identificatie, correlatie en discriminatie:

"In all cases, modern mass surveillance has three broad components: identification, correlation and discrimination. (…) We might be completely anonymous in a system that uses unique cookies to track us as we browse the internet, but the same process of correlation and discrimination still occurs. It's the same with faces (…)"[18].

Over regulering voegt hij er het volgende aan toe:

"Regulating this system means addressing all three steps of the process. A ban on facial recognition won't make any difference if, in response, surveillance systems switch to identifying people by smartphone MAC addresses. The problem is that we are being identified without our knowledge or consent, and society needs rules about when that is permissible"[19].

Hij stelt ook dat men bijzonder voorzichtig moet omspringen met het combineren van gegevens:

"Similarly, we need rules about how our data can be combined with other data, and then bought and sold

14 SINGER, N., *Amazon's Facial Recognition Wrongly Identifies 28 Lawmakers, A.C.L.U. Says*, website New York Times, 26 juli 2018.
15 CONGER, K., FAUSSET R., et KOVALESKI S.F., *op.cit.*
16 *Idem.*
17 SCHNEIER, B., *op.cit*.
18 *Idem.*
19 *Idem.*

without our knowledge or consent. The data broker industry is almost entirely unregulated; there's only one law — passed in Vermont in 2018 — that requires data brokers to register and explain in broad terms what kind of data they collect. The large internet surveillance companies like Facebook and Google collect dossiers on us more detailed than those of any police state of the previous century. Reasonable laws would prevent the worst of their abuses"[20].

En Belgique, en juillet 2019, nous apprenions que la police allait "*commencer à utiliser les caméras à reconnaissance faciale à l'aéroport de Bruxelles-National*". Et l'Organe de contrôle de l'information policière (COC) allait lancer une enquête à ce propos[21].

Un rapport approuvé le 16 septembre 2019 "*priait le responsable du traitement ou son préposé (la police fédérale "LPA") de mettre temporairement un terme à l'utilisation du système de reconnaissance faciale, à savoir le traitement de données biométriques (…)*"[22].

Dans ce rapport, nous apprenons d'abord que "*Brussels Airport Company a acheté début 2017 pour la LPA un logiciel en vue de tester un système de reconnaissance faciale. Il s'agit de quatre caméras*".[23] Et plusieurs problèmes ont été soulevés par le COC.

D'abord, les tests ayant révélé une marge d'erreur très importante (faux positifs), il y a été mis un terme en mars 2017. Par ailleurs, le COC notait que la possibilité de tester un système de reconnaissance faciale soulève des questions quant au champ d'application exact du traitement. Enfin, l'Organe de contrôle constate que la LFP (loi du 5 août 1992 sur la fonction de police), dans l'hypothèse où elle s'applique, décrit bel et bien ce qui relève de la définition d'une caméra intelligente, mais ne stipule pas dans quelles circonstances ni sous quelles conditions l'utilisation de caméras permettant la reconnaissance faciale est autorisée, et encore moins sur quel support les images peuvent/doivent être enregistrées et quelles données doivent au minimum être conservées (voir les considérants pour plus de détails)[24].

20 *Idem.*

21 *"Rapport de visite et de surveillance: Rapport intermédiaire avec mesure correctrice concernant la visite menée auprès de la police fédérale de l'aéroport de Zaventem par l'organe de contrôle de l'information policière et portant sur l'utilisation de la reconnaissance faciale à l'aéroport national de Zaventem",* site Internet du COC, 16 septembre 2019.

22 *Idem.*

23 *Idem.*

24 *Idem.*

without our knowledge or consent. The data broker industry is almost entirely unregulated; there's only one law — passed in Vermont in 2018 — that requires data brokers to register and explain in broad terms what kind of data they collect. The large internet surveillance companies like Facebook and Google collect dossiers on us more detailed than those of any police state of the previous century. Reasonable laws would prevent the worst of their abuses"[20].

In België kwam in juli 2019 het nieuws dat de politie gezichtsherkenningscamera's zou gaan gebruiken op de luchthaven van Zaventem. Het Controleorgaan op de politionele informatie (COC) zou ter zake een onderzoek instellen[21].

In een op 16 september 2019 goedgekeurd rapport werd de verwerkingsverantwoordelijke of zijn aangestelde (federale politie, LPA) verzocht "*het systeem van gezichtsherkenning, met name het verwerken van biometrische gegevens, tijdelijk te beëindigen (…)*"[22].

Uit dat rapport blijkt vooreerst dat "*begin 2017 door Brussels Airport Company (BAC) ten behoeve van de LPA software werd aangekocht voor het uittesten van een systeem van gezichtsherkenning. Het gaat om vier camera's*".[23] Het COC wees daarnaast op meerdere problemen.

Om te beginnen werd tijdens het testen een zeer grote foutenmarge vastgesteld (valse positieven). Daarom werd het testen in maart 2017 stopgezet. Voorts heeft het COC erop gewezen dat bij de mogelijkheid om een systeem voor gezichtsherkenning te testen, vragen rijzen met betrekking tot het precieze toepassingsgebied van de verwerking. Ten slotte stelt het Controleorgaan vast dat de WPA (wet van 5 augustus 1992 op het politieambt), indien van toepassing, weliswaar beschrijft wat binnen de definitie van "intelligente camera" valt, maar niet regelt in welke omstandigheden en onder welke voorwaarden het gebruik van camera's met gezichtsherkenning is toegestaan, laat staan op welke drager de beelden kunnen/moeten worden opgeslagen en welke gegevens minstens moeten worden bewaard (zie de consideransen voor meer details)[24].

20 *Idem.*

21 *Visitatie-toezichtrapport: tussentijds rapport met corrigerende maatregel betreffende de visitatie bij de federale politie van de luchthaven Zaventem door het Controleorgaan op de politionele informatie met betrekking tot het gebruik van gezichtsherkenning op de nationale luchthaven van Zaventem,* website van het COC, 16 september 2019.

22 *Idem.*

23 *Idem.*

24 *Idem.*

D'une manière plus générale, plusieurs experts en Belgique ont exposé divers limites associées à la technologie de la reconnaissance faciale.

Celle-ci pose par exemple des questions quant à l'enrôlement biométrique[25]. Qui va le pratiquer? Les services de sécurité ont entrepris ce travail pour des individus jugés à risques. Mais des entreprises privées pourraient-elles également se lancer dans un travail d'enrôlement biométrique plus "*intensif*"? "*Il y aurait beaucoup d'obstacles juridiques à une telle utilisation. Mais souvent dans ce genre de cas, tant que personne ne dépose plainte, il est difficile de savoir*", note Bruno Dumas[26]. De plus, des doutes peuvent également émerger lorsqu'il s'agit d'envisager la provenance des images servant à entraîner les algorithmes de reconnaissance[27].

Qu'en est-il au niveau européen? La Commission européenne a récemment publié un livre blanc à propos de l'intelligence artificielle. On peut y lire que "*La collecte et l'utilisation de données biométriques à des fins d'identification à distance, au moyen, par exemple, du déploiement de la reconnaissance faciale dans des lieux publics, comportent des risques particuliers en termes de droits fondamentaux. L'utilisation de systèmes d'IA pour l'identification biométrique à distance a des incidences sur les droits fondamentaux qui peuvent considérablement varier selon sa finalité, son contexte et sa portée*"[28]

Et d'ajouter: "*Il s'ensuit, conformément aux règles de l'Union en vigueur en matière de protection des données et à la Charte des droits fondamentaux de l'UE, que l'IA ne peut être utilisée à des fins d'identification biométrique à distance que lorsque cette utilisation est dûment justifiée, proportionnée et assortie de garanties adéquates*"[29].

Après avoir étudié la possibilité de mettre en place un moratoire, la Commission souhaite finalement s'en tenir à lancer un "*vaste débat*" concernant les "*exigences spécifiques pour l'identification biométrique à distance*": "*Afin de répondre aux éventuelles inquiétudes,*

Meer in het algemeen hebben meerdere experten in België erop gewezen dat de gezichtsherkenningstechnologie nogal wat beperkingen inhoudt.

Die technologie roept bijvoorbeeld vragen op betreffende de biometrische *enrolment*[25]. Wie zal die uitvoeren? De veiligheidsdiensten hebben die techniek toegepast op individuen die als risicovol worden beschouwd. Zouden privébedrijven zich echter ook mogen toeleggen op een meer "intensieve" vorm van biometrisch *enrolment*? "*Il y aurait beaucoup d'obstacles juridiques à une telle utilisation. Mais souvent dans ce genre de cas, tant que personne ne dépose plainte, il est difficile de savoir*", aldus Bruno Dumas van de *Université de Namur*[26]. Bovendien kunnen ook twijfels rijzen met betrekking tot de herkomst van de beelden op basis waarvan de herkenningsalgoritmen worden opgesteld[27].

Hoe is de situatie op Europees niveau? De Europese Commissie heeft recent een witboek over artificiële intelligentie gepubliceerd. Daarin staat het volgende te lezen: "*The gathering and use of biometric data for remote identification purposes, for instance through deployment of facial recognition in public places, carries specific risks for fundamental rights. The fundamental rights implications of using remote biometric identification AI systems can vary considerably depending on the purpose, context and scope of the use".*[28]

De Europese Commissie voegt daar het volgende aan toe: "*It follows that, in accordance with the current EU data protection rules and the Charter of Fundamental Rights, AI can only be used for remote biometric identification purposes where such use is duly justified, proportionate and subject to adequate safeguards*"[29].

Na eerst de mogelijkheid van een moratorium te hebben bestudeerd, wil de Europese Commissie het ten slotte houden bij een "ruim debat" over de "*specific requirements for remote biometric identification*": "*In order to address possible societal concerns relating*

25 Ce terme désigne toute une série d'opérations consistant à établir pour un visage une espèce de gabarit à partir notamment de ses différents éléments, des distances entre ceux-ci, d'angles. Source: COLINET, M., *"Quelle place laisser à la reconnaissance faciale?"*, site internet du Soir, le 2 octobre 2019.

26 COLINET, M., *"Quelle place laisser à la reconnaissance faciale?"*, site internet du Soir, le 2 octobre 2019.

27 *Idem.*

28 *"Livre blanc: Intelligence artificielle: Une approche européenne axée sur l'excellence et la confiance"*, Commission européenne, le 19 février 2020.

29 *"Livre blanc: Intelligence artificielle: Une approche européenne axée sur l'excellence et la confiance"*, Commission européenne, le 19 février 2020.

25 Deze term duidt op een reeks verrichtingen waarbij voor een gezicht een soort patroon wordt opgemaakt op basis van de verschillende aspecten ervan, de afstanden daartussen en de hoeken. Bron: COLINET, M., *Quelle place laisser à la reconnaissance faciale?*, website van *Le Soir*, 2 oktober 2019.

26 COLINET, M., *ibidem.*

27 *Idem.*

28 *White Paper on Artificial Intelligence – A European approach to excellence and trust*, Europese Commissie, 19 februari 2020.

29 *White Paper on Artificial Intelligence – A European approach to excellence and trust*, *op.cit.*

du point de vue de la société, quant à l'utilisation de l'IA à de telles fins dans les lieux publics et d'éviter toute fragmentation du marché intérieur, la Commission lancera un vaste débat européen sur les circonstances particulières, le cas échéant, qui pourraient justifier une telle utilisation, ainsi que sur les garanties communes à mettre en place"[30].

Le 10 juillet 2019, le *European Data Protecting Board (EDPB)* adoptait une série de lignes directrice concernant le traitement des données personnelles à travers les dispositifs vidéo. Ces lignes directrices visent à donner des conseils sur la façon d'appliquer le Règlement général sur la protection des données (RGPD) en ce qui concerne le traitement des données personnelles via des appareils vidéo.

Dans ce document, l'EDPB met en garde contre plusieurs choses.

D'abord, "*ces technologies peuvent limiter les possibilités de mouvement anonyme et d'utilisation anonyme des services et limiter généralement la possibilité de rester inaperçu". De plus, "alors que les individus peuvent être à l'aise avec la vidéosurveillance mise en place à des fins de sécurité par exemple, des garanties doivent être prises pour éviter toute utilisation abusive à des fins totalement différentes et - pour le sujet de données – inattendues (comme par exemple à des fins de marketing ou pour faire un contrôle de performances d'employés etc)". Par ailleurs, "la surveillance vidéo est devenue très performante grâce à la mise en œuvre croissante de l'analyse vidéo intelligente. Ces techniques peuvent être plus intrusives (par exemple, des technologies biométriques complexes) ou moins intrusives (par exemple, de simples algorithmes de comptage). Rester anonyme et préserver sa vie privée est en général de plus en plus difficile". De plus, "outre les problèmes de confidentialité, il existe également des risques liés à d'éventuels dysfonctionnements de ces appareils et aux biais qu'ils peuvent induire". De plus, "la vidéosurveillance n'est pas par défaut une nécessité alors qu'il existe d'autres moyens d'atteindre l'objectif sous-jacent*"[31] (voir considérants pour plus de détails avec citations complètes dans la langue originale).

Par ailleurs, même si en Europe, le RGPD et différentes législations nationales permettent d'encadrer l'utilisation et la conservation des données personnelles, certains experts plaident pour l'ajustement de tel dispositif. Pour certains d'entre eux, l'approche du RGPD est très globalisante avec une définition très large des données

[30] *Idem.*

[31] *"Guidelines 3/2019 on processing of personal data through video devices"* adopté le 10 juillet 2019, site Internet du European Data Protection Board. [Notre traduction]

to the use of AI for such purposes in public places, and to avoid fragmentation in the internal market, the Commission will launch a broad European debate on the specific circumstances, if any, which might justify such use, and on common safeguards"[30].

Op 10 juli 2019 heeft het *European Data Protecting Board* (EDPB) een aantal richtsnoeren betreffende de verwerking van persoonsgegevens via cameratoestellen aangenomen. Die richtsnoeren zijn bedoeld als advies voor de wijze waarop de Algemene Verordening Gegevensbescherming (AVG) moet worden toegepast met betrekking tot de verwerking van persoonsgegevens via cameratoestellen.

Dat document van het EDPB bevat meerdere waarschuwingen.

Ten eerste: "*these technologies may limit the possibilities of anonymous movement and anonymous use of services and generally limit the possibility of remaining unnoticed"*. Vervolgens: *"While individuals might be comfortable with video surveillance set up for a certain security purpose for example, guarantees must be taken to avoid any misuse for totally different and – to the data subject – unexpected purposes (e.g. marketing purpose, employee performance monitoring etc.).".* (…) *"Video surveillance has become high performing through the growing implementation of intelligent video analysis. These techniques can be more intrusive (e.g. complex biometric technologies) or less intrusive (e.g. simple counting algorithms). Remaining anonymous and preserving one's privacy is in general increasingly difficult."*. Daarenboven is het zo dat *"In addition to privacy issues, there are also risks related to possible malfunctions of these devices and the biases they may induce".* Ten slotte wijst men erop dat *"Video surveillance is not by default a necessity when there are other means to achieve the underlying purpose."*[31] (zie de consideransen voor meer details en volledige citaten).

Ook al kunnen de aanwending en de bewaring van persoonsgegevens in Europa via de AVG en via de verschillende nationale wetgevingen van een raamwerk worden voorzien, toch pleiten sommige deskundigen voor de bijsturing van de huidige regeling. Sommigen onder hen vinden de benadering in de AVG erg veralgemenend,

[30] *Idem.*

[31] *Guidelines 3/2019 on processing of personal data through video devices,* aangenomen op 10 juli 2019, website van het *European Data Protection Board*.

personnelles. On peut effectivement considérer qu'une photo traitée par la reconnaissance faciale, c'est plus qu'une simple donnée personnelle: "*c'est une donnée personnelle sensible ou biométrique*"[32].

Qu'en dit l'Autorité belge de protection des données?

Cette institution nationale a également fait part de plusieurs complexités et risques concernant les système d'authentification biométrique: "*personne ne peut introduire sans condition un système biométrique. Il faut, en effet, tenir compte de diverses règles complexes*"[33].

Parmi ces règles complexes, l'APD note que "*Tout d'abord, il faut que la finalité poursuivie par le responsable du traitement requière effectivement que des données personnelles soient traitées. A priori, par exemple, pas besoin pour un boulanger d'authentifier ses clients, et donc a fortiori, pas besoin de recueillir leurs données biométriques*"[34].

Elle indique par ailleurs que "*La technologie biométrique choisie doit nécessiter une participation consciente de la personne concernée lors de l'authentification. La reconnaissance faciale à distance, la collecte d'empreintes digitales ou l'enregistrement de la voix, susceptibles de se produire à l'insu de la personne concernée, présentent certains risques à cet égard*"[35].

Enfin, elle ajoute que "*Le responsable devra encore faire l'exercice de définir les catégories de lieux qui nécessitent un contrôle biométrique, et ne soumettre à la collecte de données biométriques que les personnes susceptibles de pénétrer dans ce lieu*"[36]. (Voir considérants pour plus de détails).

Qu'en est-il du cadre législatif national? Il existe en Belgique une "loi caméras"[37].

met een zeer ruime omschrijving van het begrip "persoonsgegeven". Er kan immers van worden uitgegaan dat een aan gezichtsherkenning onderworpen foto méér is dan louter een persoonsgegeven: "*c'est une donnée personnelle sensible ou biométrique*"[32].

Wat geeft de Gegevensbeschermingsautoriteit daar over aan?

Ook die nationale instelling heeft verscheidene complexe aspecten en risico's geïdentificeerd die aan de biometrische authenticatiesystemen zijn verbonden: "*Niemand kan zomaar een biometrisch systeem invoeren. Er moet immers rekening gehouden worden met verschillende, complexe regels*."[33].

Aangaande die complexe regels merkt de GBA onder meer het volgende op: "*Eerst en vooral moet het voor de verantwoordelijke voor de verwerking absoluut noodzakelijk zijn dat hij persoonsgegevens verwerkt om zijn vooropgesteld doeleinde te kunnen bereiken. Voor een bakker is het bijvoorbeeld niet noodzakelijk dat hij zijn klanten authenticeert, en het is dus a fortiori niet noodzakelijk dat hij hun biometrische gegevens inzamelt.*"[34].

Voorts stipt de GBA het volgende aan: "*eens de biometrische technologie werd gekozen, moet de persoon die eraan wordt onderworpen zich daarvan bewust zijn tijdens zijn authenticatie want het risico op onwetendheid bestaat wel degelijk, omdat gezichtsherkenning op afstand, inzameling van vingerafdrukken of registratie van de stem gemakkelijk kan gebeuren zonder medeweten van de betrokkene*"[35].

Ten slotte voegt zij daar het volgende aan toe: "*De verantwoordelijke voor de verwerking zal dus de categorieën plaatsen bepalen waar een biometrische controle noodzakelijk is en alleen van die personen de biometrische gegevens inzamelen die in het gebouw moeten zijn.*"[36] (zie de consideransen voor nadere bijzonderheden).

Hoe staat het met het nationale wetgevende kader? In België is er de zogenaamde "camerawet"[37].

---

32 STROWEL, A., cité par COLINET, *"Quelle place laisser à la reconnaissance faciale?"*, site internet du Soir, le 2 octobre 2019.

33 *"L'introduction d'un système d'authentification biométrique"*, site Internet de l'APD.

34 *Idem.*

35 *Idem.*

36 *Idem.*

37 La loi du 21 mars 2007 réglant l'installation et l'utilisation de caméras de surveillance (publiée au *Moniteur belge* du 31 mai 2007). La loi caméras s'applique à l'installation et à l'utilisation de caméras de surveillance en vue de la surveillance et du contrôle.

32 STROWEL, A., aangehaald door COLINET, *op.cit*. Onze vertaling: *Het is een gevoelig of biometrisch persoonsgegeven.*

33 *Een systeem van biometrische authenticatie invoeren*, website van de GBA.

34 *Ibidem.*

35 *Ibidem.*

36 *Ibidem.*

37 Wet van 21 maart 2007 tot regeling van de plaatsing en het gebruik van bewakingscamera's (bekendgemaakt in het *Belgisch Staatsblad* van 31 mei 2007). De camerawet is toepasselijk op "de plaatsing en het gebruik van bewakingscamera's" met het oog op toezicht en controle (artikel 3 van de camerawet).

Selon cette loi, on entend par caméra de surveillance tout système d'observation fixe ou mobile qui collecte, traite ou sauvegarde des images dans le but de: prévenir, constater ou déceler les délits; prévenir, constater ou déceler les nuisances; maintenir l'ordre public. Les autres caméras doivent en principe respecter les prescriptions de la "loi vie privée"[38].

Lorsqu'une personne installe et utilise une caméra de surveillance, celle-ci doit satisfaire aux prescriptions de la loi caméras. Deux cas font exception à la règle: les caméras de surveillance dont l'usage est réglementé par une législation particulière, comme par exemple la "loi football"; les caméras de surveillance sur le lieu de travail; dans le secteur privé, la CCT n° 68 doit être respectée[39].

Qu'en est-il lorsque la loi caméras rencontre les caméras à reconnaissance faciale?

Interrogé par le député Gilles Vanden Burre le 4 mars 2020 en commission de la Justice, le ministre Philippe De Backer précisait à ce propos que: "*La "loi caméras" n'autorise pour le moment que l'usage des caméras de surveillance intelligentes couplées à des registres ou à des fichiers à caractère personnel, en vue de la reconnaissance automatique des plaques d'immatriculation. La loi sur la fonction de police n'autorise pas non plus l'utilisation de caméras à reconnaissance faciale. Par conséquent, il est interdit aux particuliers, mais aussi aux pouvoirs publics, de se servir de caméras de surveillance à reconnaissance faciale*"[40].

Le ministre a également précisé la position de son cabinet à ce propos. Il a d'abord affirmé, qu'il n'était "*pas opposé à l'innovation en soi, mais qu'il importait de rester très vigilant et très prudent face à l'introduction d'une telle technique*". De plus, il s'est montré favorable à organiser un débat au Parlement entre experts, autorités et la Commission européenne "*pour voir comment les autres pays s'organisent à ce sujet*", mais également favorable à interroger des instances "*telles que le COC*" ainsi qu'à inclure nos citoyennes et citoyens dans le débat. Le ministre s'est par ailleurs dit "*extrêmement prudent quant à l'introduction de cette technique*", susceptible de constituer une base de données en masse. Il s'est dit également très favorable au moratoire dans "*le texte européen initial*" et d'ajouter "*qu'à l'échelle européenne, nous avons toujours poussé en faveur d'un moratoire*

"Volgens de Camerawet is een bewakingscamera elk vast of mobiel observatiesysteem dat beelden verzamelt, verwerkt of bewaart om: (…) misdrijven te voorkomen, vast te stellen of op te sporen (…) overlast te voorkomen, vast te stellen of op te sporen (…) [en] de orde te handhaven[.] Andere camera's moeten in principe de voorschriften van de Privacywet naleven."[38]

"Wanneer (…) [iemand] een bewakingscamera (…) [wil] plaatsen en gebruiken, moet die voldoen aan de voorschriften van de camerawet. Op deze regeling zijn twee uitzonderingen: (…) Bewakingscamera's die geregeld zijn door een bijzondere wetgeving zoals bijvoorbeeld de voetbalwet. (…) Bewakingscamera's op de arbeidsplaats; in de privésector moet dan cao nr. 68 worden nageleefd."[39]

Quid met de camerawet bij camera's met gezichtsherkenning?

Toen volksvertegenwoordiger Gilles Vanden Burre op 4 maart 2020 in de commissie voor Justitie minister Philippe De Backer ondervroeg, antwoordde die daarop het volgende: *"La "loi caméras" n'autorise pour le moment que l'usage des caméras de surveillance intelligentes couplées à des registres ou à des fichiers à caractère personnel, en vue de la reconnaissance automatique des plaques d'immatriculation. La loi sur la fonction de police n'autorise pas non plus l'utilisation de caméras à reconnaissance faciale. (…) Par conséquent, il est interdit aux particuliers, mais aussi aux pouvoirs publics, de se servir de caméras de surveillance à reconnaissance faciale."*[40].

Voorts heeft de minister ter zake het standpunt van zijn kabinet gepreciseerd. Ten eerste heeft hij het volgende gesteld: *"Je ne suis pas opposé à l'innovation en soi* (…)*, mais il importe de rester très vigilant et très prudent face à l'introduction d'une telle technique"*. Tevens heeft hij aangegeven gewonnen te zijn voor een debat in het Parlement tussen deskundigen, de overheid en de Europese Commissie om na te gaan hoe andere landen zich in dat verband organiseren; tegelijk is hij de idee genegen om instanties zoals het Controleorgaan op de politionele informatie te bevragen en om de burgers bij het debat te betrekken. Daarnaast heeft de minister aangestipt dat hij uitermate voorzichtig is met de invoering van die techniek, die kan neerkomen op de aanmaak van een massadatabank. Ook is hij sterk te vinden voor het moratorium in de initiële EU-tekst; bovendien stelt hij dat

38 *"Justice: respect de la vie privée; surveillance camera"*, site internet des autorités fédérales *"Belgium.be",* consulté le 15 mai 2020.

39 *Idem.*

40 Commission de la Justice de la Chambre des représentants du 4 mars 2020. URL: *https://www.lachambre.be/doc/CCRI/html/55/ic125x.html*.

38 *Justitie – Veiligheid – Privacy – Camerabewaking*, website van de federale overheid op *"Belgium.be",* geraadpleegd op 15 mei 2020.

39 *Ibidem.*

40 Commissie voor Justitie van de Kamer van volksvertegenwoordigers van 4 maart 2020. Zie *https://www.dekamer.be/doc/CCRI/html/55/ic125x.html*.

de cinq ans". Enfin, le ministre affirmait que "*tout ce qui est lié à la reconnaissance faciale participe d'un risque élevé*"[41]. L'ensemble de ces positions du ministre sont reprises dans les considérants, avec citation intégrale.

À noter que le ministre Pieter De Crem s'est également exprimé à ce propos. Répondant à une question écrite de Jessika Soors, il a affirmé que: *"Au sein de la police intégrée, un groupe de travail a en outre été mis sur pied et il se compose à la fois de juristes et d'experts de terrain dans les différents domaines de la police fédérale et de la police locale, le but étant de ne pas limiter l'analyse juridique à la reconnaissance faciale, mais de l'étendre au traitement des données biométriques en général*"[42].

Et d'ajouter que: "*Ce type de traitements peut être synonyme de gain en efficacité pour les services de sécurité. La reconnaissance faciale en tant que telle peut être une ressource intéressante pour les services de police en appui de leurs missions premières, à savoir la recherche de personnes. Cela étant, il convient avant tout de veiller à élaborer une base légale solide pour que les informations obtenues par le biais de ces logiciels puissent également être utilisées valablement, par la suite, dans le cadre de l'enquête pénale*".[43]

Les avis différents des deux ministres prouvent la nécessité de mettre en place sans tarder un débat à ce propos à la Chambre.

Enfin, notons qu'il est également important de considérer que des droits pourraient être impactés par la mise en place de la reconnaissance faciale comme le droit au respect à la vie privée (voir considérants à ce propos), mais également la protection des données personnelles ou la liberté de réunion[44].

Outre-Atlantique, les défenseurs des libertés civiles américaines pointent d'ailleurs du doigt le risque que la surveillance faciale permette d'identifier des personnes à distance ou en ligne, à leur insu ou sans leur consentement, ce qui représente des risques non négligeables, et menace par exemple la capacité des Américains à assister librement aux manifestations politiques ou

België zich op EU-niveau altijd heeft ingezet voor een vijfjarig moratorium. Ten slotte wijst de minister erop dat alles wat met gezichtsherkenning te maken heeft veel risico's inhoudt[41]. Al die standpunten van de minister zijn in de consideransen opgenomen, met opgaaf van het volledige citaat.

Er zij op gewezen dat ook minister Pieter De Crem zich daarover heeft uitgesproken. In zijn antwoord op een schriftelijke vraag van volksvertegenwoordigster Jessika Soors heeft hij aangegeven dat binnen de geïntegreerde politie bovendien een werkgroep werd opgericht met juristen en experten in het veld die vertrouwd zijn met de diverse domeinen van de federale en de lokale politie. Het ligt in de bedoeling de juridische analyse niet te beperken tot gezichtsherkenning, maar tevens na te gaan hoe het staat met de verwerking van de biometrische gegevens in het algemeen[42].

Hij voegde er nog aan toe dat die verwerking van biometrische gegevens kan bijdragen aan de efficiëntie van de veiligheidsdiensten. Gezichtsherkenning als dusdanig kan voor de politiediensten een interessante bron zijn ter ondersteuning van hun belangrijkste taak, met name de opsporing van personen. Niettemin moet er bovenal op worden toegezien dat een degelijke wettelijke grondslag wordt uitgewerkt, teneinde de aan de hand van die software verkregen informatie vervolgens op geldige wijze te kunnen gebruiken bij het strafonderzoek.[43]

De afwijkende meningen van de twee ministers bewijzen dat het noodzakelijk is om zonder enig verwijl daarover in de Kamer een debat te openen.

Ten slotte is het van belang voor ogen te houden dat rechten zouden kunnen worden aangetast door de invoering van gezichtsherkenning. Daarbij gaat het bijvoorbeeld niet alleen om de eerbiediging van de persoonlijke levenssfeer (zie ter zake de consideransen), maar ook om de bescherming van persoonsgegevens of om de vrijheid van vergadering[44].

Aan de overzijde van de Atlantische Oceaan wijzen de verdedigers van de VS-burgervrijheden ook op het gevaar dat toezicht met behulp van gezichtsherkenning het mogelijk zou maken mensen op afstand of online te herkennen zonder dat zij daarvan op de hoogte zijn of daarvoor hun toestemming hebben gegeven. Dat houdt niet te veronachtzamen risico's in en brengt bijvoorbeeld

41 *Idem.*
42 Réponse à la question parlementaire écrite n° 463 de Madame SOORS, datée du 08/04/2020, concernant "l'utilisation illégale de logiciels de reconnaissance faciale", Chambre des représentants.
43 *Idem.*
44 *"OVERVIEW: FACIAL RECOGNITION TO COMBAT CRIME",* The Danish Institute for Human Rights, décembre 2019.

41 *Ibidem.*
42 Antwoord op schriftelijke parlementaire vraag nr. 463 van mevrouw SOORS van 8 april 2020 over "l'utilisation illégale de logiciels de reconnaissance faciale", Kamer van volksvertegenwoordigers.
43 *Idem.*
44 *Overview: Facial Recognition to Combat Crime, The Danish Institute for Human Rights*, december 2019.

simplement à exercer leurs activités de manière anonyme en public[45].

À ce propos, comme le fait remarquer David Kaye, (*United Nations Special Rapporteur on freedom of opinion and expression*): "*Surveillance tools can interfere with human rights, from the right to privacy and freedom of expression to rights of association and assembly, religious belief, non-discrimination, and public participation. And yet they are not subject to any effective global or national control*"[46].

Dans le même ordre d'idée, l'Institut danois pour les droits humains, qui recommande au gouvernement danois de postposer la mise en place de la technologie de reconnaissance faciale pour combattre le crime, estime que: "*Intensive surveillance by the police may potentially affect the freedom of assembly and, to some extent, the freedom of expression. Use of facial recognition technology, for example during a demonstration, can potentially reveal information about individuals, including sensitive data such as their political affiliation*"[47].

D'ailleurs, *"The Danish Institute for Human Rights recommends that the Danish government postpone the introduction of facial recognition to combat crime until we know the human rights consequences for the right to privacy, the right to the protection of personal data and the freedom of assembly"*[48].

En somme, le développement de la technologie de reconnaissance faciale peut mener nos sociétés à se muer en système de surveillance généralisé et pourrait permettre aux autorités (mais également aux organisateurs d'événements privés) d'effectuer plusieurs contrôles d'identité quotidiens de nos citoyennes et citoyens[49]. Par conséquent, pour certains experts, nous sommes arrivés au "moment d'un choix politique" à l'égard de cette technologie[50].

Tous ces éléments plaident en faveur d'une grande prudence quant à l'implémentation en Belgique de tels systèmes de surveillance par caméras à reconnaissance faciale.

de mogelijkheid van de Amerikanen in het gedrang om vrijelijk politieke manifestaties bij te wonen of eenvoudigweg hun activiteiten anoniem in het openbaar te verrichten[45].

David Kaye, Bijzonder VN-rapporteur over de vrijheid van mening en van meningsuiting, merkte ter zkae het volgende op: *"Surveillance tools can interfere with human rights, from the right to privacy and freedom of expression to rights of association and assembly, religious belief, non-discrimination, and public participation. And yet they are not subject to any effective global or national control."*[46].

Het Deense Instituut voor de Mensenrechten, dat de Deense regering aanbeveelt om de invoering van gezichtsherkenningstechnologie ter bestrijding van criminaliteit uit te stellen, heeft een gelijkaardige kijk op de zaak: *"Intensive surveillance by the police may potentially affect the freedom of assembly and, to some extent, the freedom of expression. Use of facial recognition technology, for example during a demonstration, can potentially reveal information about individuals, including sensitive data such as their political affiliation"*[47].

Het Instituut geeft trouwens het volgende advies: "*The Danish Institute for Human Rights recommends that the Danish government postpone the introduction of facial recognition to combat crime until we know the human rights consequences for the right to privacy, the right to the protection of personal data and the freedom of assembly*"[48].

Kortom, de ontwikkeling van de gezichtsherkenningstechnologie kan ertoe leiden dat onze samenlevingen tot alomtegenwoordige toezichtsystemen verworden en dat de overheid, maar ook de organisatoren van privéevenementen, de mogelijkheid krijgen om meerdere keren per dag de identiteit van onze medeburgers te controleren[49]. Bijgevolg menen sommige deskundigen dat het ogenblik is aangebroken om een politieke keuze met betrekking tot die technologie te maken[50].

Al die elementen pleiten voor grote omzichtigheid met betrekking tot het gebruik van dergelijke toezichtsystemen met gezichtsherkenningscamera's in België.

45 CONGER, K., FAUSSET R., et KOVALESKI S.F., …
46 *"UN expert calls for immediate moratorium on the sale, transfer and use of surveillance tools",* site internet des Nations Unies Droits de l'Homme, le 25 juin 2019.
47 *"OVERVIEW: FACIAL RECOGNITION TO COMBAT CRIME",* The Danish Institute for Human Rights, décembre 2019.
48 *Idem.*
49 COLINET M., …
50 DUMAS, cité par COLINET M., …

45 CONGER, K., FAUSSET R., et KOVALESKI S.F., *op.cit.*
46 *UN expert calls for immediate moratorium on the sale, transfer and use of surveillance tools,* website van *United Nations Human Rights Office of the High Commissioner* (OHCHR), 25 juni 2019.
47 *Overview: Facial Recognition to Combat Crime, op.cit.*
48 *Ibidem.*
49 COLINET M., *op.cit.*
50 DUMAS, geciteerd door COLINET M., *op.cit.*

Le groupe Ecolo-Groen est donc demandeur d'un moratoire de 3 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 afin que le Parlement puisse mettre en place un débat sur ce sujet sensible, et pour que cette technologie intrusive ne puisse être implémentée qu'accompagnée des garanties strictes concernant les droits humains.

Gilles VANDEN BURRE (Ecolo-Groen)
Jessika SOORS (Ecolo-Groen)
François DE SMET (DéFI)

De Ecolo-Groen-fractie is derhalve voorstander van een driejarig moratorium op het gebruik van gezichtsherkenningssoftware en -algoritmes in vaste of mobiele veiligheidscamera's op openbare en private plaatsen, teneinde het Parlement de mogelijkheid te bieden een debat te voeren over dit gevoelige onderwerp en om ervoor te zorgen dat die ingrijpende technologie alleen mag worden toegepast wanneer zij gepaard gaat met strikte waarborgen voor de rechten van de mens.

PROPOSITION DE RÉSOLUTION

La Chambre des représentants,

A. considérant que selon le *European Data Protecting Board*, "*The intensive use of video devices has an impact on citizen's behaviour. Significant implementation of such tools in many spheres of the individuals' life will put an additional pressure on the individual to prevent the detection of what might be perceived as anomalies. De facto, these technologies may limit the possibilities of anonymous movement and anonymous use of services and generally limit the possibility of remaining unnoticed. Data protection implications are massive*"[51];

B. considérant que selon le *European Data Protecting Board*, "*While individuals might be comfortable with video surveillance set up for a certain security purpose for example, guarantees must be taken to avoid any misuse for totally different and – to the data subject – unexpected purposes (e.g. marketing purpose, employee performance monitoring etc.). In addition, many tools are now implemented to exploit the images captured and turn traditional cameras into smart cameras. The amount of data generated by the video, combined with these tools and techniques increase the risks of secondary use (whether related or not to the purpose originally assigned to the system) or even the risks of misuse. The general principles in GDPR (Article 5), should always be carefully considered when dealing with video surveillance."*[52];

C. considérant que selon le *European Data Protecting Board*, "*Video surveillance systems in many ways change the way professionals from the private and public sector interact in private or public places for the purpose of enhancing security, obtaining audience analysis, delivering personalized advertising, etc. Video surveillance has become high performing through the growing implementation of intelligent video analysis. These techniques can be more intrusive (e.g. complex biometric technologies) or less intrusive (e.g. simple counting algorithms). Remaining anonymous and preserving one's privacy is in general increasingly difficult. The data protection issues raised in each situation may differ, so will the legal analysis when using one or the other of these technologies.*"[53];

[51] *"Guidelines 3/2019 on processing of personal data through video devices"* adopté le 10 juillet 2019, site internet du *European Data Protection Board*.
[52] *Idem.*
[53] *Idem.*

VOORSTEL VAN RESOLUTIE

De Kamer van volksvertegenwoordigers,

A. overwegende dat het Europees Comité voor gegevensbescherming het volgende stelt: "*The intensive use of video devices has an impact on citizen's behaviour. Significant implementation of such tools in many spheres of the individuals' life will put an additional pressure on the individual to prevent the detection of what might be perceived as anomalies. De facto, these technologies may limit the possibilities of anonymous movement and anonymous use of services and generally limit the possibility of remaining unnoticed. Data protection implications are massive.*"[51];

B. overwegende dat het Europees Comité voor gegevensbescherming voorts het volgende vaststelt: "*While individuals might be comfortable with video surveillance set up for a certain security purpose for example, guarantees must be taken to avoid any misuse for totally different and – to the data subject – unexpected purposes (e.g. marketing purpose, employee performance monitoring etc.). In addition, many tools are now implemented to exploit the images captured and turn traditional cameras into smart cameras. The amount of data generated by the video, combined with these tools and techniques increase the risks of secondary use (whether related or not to the purpose originally assigned to the system) or even the risks of misuse. The general principles in GDPR (Article 5), should always be carefully considered when dealing with video surveillance.*"[52];

C. overwegende dat volgens het Europees Comité voor gegevensbescherming ook het volgende geldt: "*Video surveillance systems in many ways change the way professionals from the private and public sector interact in private or public places for the purpose of enhancing security, obtaining audience analysis, delivering personalized advertising, etc. Video surveillance has become high performing through the growing implementation of intelligent video analysis. These techniques can be more intrusive (e.g. complex biometric technologies) or less intrusive (e.g. simple counting algorithms). Remaining anonymous and preserving one's privacy is in general increasingly difficult. The data protection issues raised in each situation may differ, so will the legal analysis when using one or the other of these technologies.*"[53];

[51] *Guidelines 3/2019 on processing of personal data through video devices*, *aangenomen op 10 juli 2019, website van het Europees Comité voor gegevensbescherming*.
[52] *Ibidem.*
[53] *Ibidem.*

D. considérant que selon le *European Data Protecting Board*, "*In addition to privacy issues, there are also risks related to possible malfunctions of these devices and the biases they may induce. Researchers report that software used for facial identification, recognition, or analysis performs differently based on the age, gender, and ethnicity of the person it's identifying. Algorithms would perform based on different demographics, thus, bias in facial recognition threatens to reinforce the prejudices of society. That is why, data controllers must also ensure that biometric data processing deriving from video surveillance be subject to regular assessment of its relevance and sufficiency of guarantees provided.*"[54];

E. considérant que selon le *European Data Protecting Board*, "*Video surveillance is not by default a necessity when there are other means to achieve the underlying purpose. Otherwise we risk a change in cultural norms leading to the acceptance of lack of privacy as the general outset.*"[55];

F. considérant que l'Autorité de protection des données considère que concernant l'introduction d'un système d'authentification biométrique, "*personne ne peut introduire sans condition un système biométrique. Il faut, en effet, tenir compte de diverses règles complexes*"[56];

G. considérant que l'Autorité de protection des données considère que concernant l'introduction d'un système d'authentification biométrique, il faut tenir compte du caractère nécessaire d'une telle introduction, notamment que "*il faut que la finalité poursuivie par le responsable du traitement requière effectivement que des données personnelles soient traitées*"[57];

H. considérant que l'Autorité de protection des données considère que concernant l'introduction d'un système d'authentification biométrique, il faut tenir compte du caractère proportionné d'une telle introduction, notamment que "*la technologie biométrique choisie doit nécessiter une participation consciente de la personne concernée lors de l'authentification. La reconnaissance faciale à distance, la collecte d'empreintes digitales ou l'enregistrement de la voix, susceptibles de se produire* à

[54] *Idem.*
[55] *Idem.*
[56] *"L'introduction d'un système d'authentification biométrique"*, site internet de l'APD, consulté le 15 mai 2020.
[57] *Idem.*

D. overwegende dat het Europees Comité voor gegevensbescherming bovendien wijst op het volgende: "*In addition to privacy issues, there are also risks related to possible malfunctions of these devices and the biases they may induce. Researchers report that software used for facial identification, recognition, or analysis performs differently based on the age, gender, and ethnicity of the person it's identifying. Algorithms would perform based on different demographics, thus, bias in facial recognition threatens to reinforce the prejudices of society. That is why, data controllers must also ensure that biometric data processing deriving from video surveillance be subject to regular assessment of its relevance and sufficiency of guarantees provided.*"[54];

E. overwegende dat het Europees Comité voor gegevensbescherming ook nog het volgende aangeeft: "*Video surveillance is not by default a necessity when there are other means to achieve the underlying purpose. Otherwise we risk a change in cultural norms leading to the acceptance of lack of privacy as the general outset.*"[55];

F. overwegende dat de Gegevensbeschermingsautoriteit met betrekking tot de invoering van een systeem van biometrische authenticatie het volgende stelt: "*Niemand kan zomaar een biometrisch systeem invoeren. Er moet immers rekening gehouden worden met verschillende, complexe regels.*"[56];

G. overwegende dat de Gegevensbeschermingsautoriteit van oordeel is dat bij de invoering van een systeem voor biometrische authenticatie rekening moet worden gehouden met de noodzaak van een dergelijke invoering; meer bepaald "*moet het voor de verantwoordelijke voor de verwerking absoluut noodzakelijk zijn dat hij persoonsgegevens verwerkt om zijn vooropgesteld doeleinde te kunnen bereiken*"[57];

H. overwegende dat volgens de Gegevensbeschermingsautoriteit met betrekking tot de invoering van een systeem voor biometrische authenticatie voorts rekening moet worden gehouden met de proportionaliteit van een dergelijke invoering en dat de GBA meer bepaald wijst op het volgende: "*eens de biometrische technologie werd gekozen, moet de persoon die eraan wordt onderworpen zich daarvan bewust zijn tijdens zijn authenticatie, want het risico op onwetendheid bestaat wel degelijk,*

[54] *Ibidem.*
[55] *Ibidem.*
[56] *Een systeem van biometrische authenticatie invoeren*, website van de GBA, geraadpleegd op 15 mei 2020 (*https://www.gegevensbeschermingsautoriteit.be/een-systeem-van-biometrische-authenticatie-invoeren*).
[57] *Ibidem.*

l'insu de la personne concernée, présentent certains risques à cet égard"[58];

I. considérant que l'Autorité de protection des données considère que concernant l'introduction d'un système d'authentification biométrique, il faut tenir compte du caractère proportionné d'une telle introduction, notamment que "*le système doit présenter un niveau de sécurité suffisamment élevé*"[59];

J. considérant que l'Autorité de protection des données considère que concernant l'introduction d'un système d'authentification biométrique, "*les règles dont il faut tenir compte sont donc multiples et complexes*"[60];

K. considérant que l'Autorité de protection des données considère que concernant l'introduction d'un système d'authentification biométrique, "*Le responsable devra encore faire l'exercice de définir les catégories de lieux qui nécessitent un contrôle biométrique, et ne soumettre à la collecte de données biométriques que les personnes susceptibles de pénétrer dans ce lieu. Notons à ce sujet que pour limiter l'accès à un lieu à certain groupe d'individus, il n'est pas forcément toujours nécessaire de traiter des données personnelles directement identifiantes (tel que le nom) des individus disposant du droit d'accès. Ainsi tant qu'une personne est titulaire du droit d'entrer et que la biométrie permet de le vérifier, il n'est pas nécessaire de lier l'information biométrique à des données additionnelles identifiantes*"[61];

L. considérant que, interrogé par le député Gilles Vanden Burre le 4 mars 2020 en commission de la Justice, le ministre Philippe De Backer déclarait: "*Je ne suis pas opposé à l'innovation en soi, puisqu'il existe aussi des applications positives de la reconnaissance faciale, mais il importe de rester très vigilant et très prudent face à l'introduction d'une telle technique dans la société. J'estime donc que nous devons poursuivre ce débat ici. C'est peut-être mieux de prendre son temps avant d'introduire cet outil dans la société. Je plaide donc pour une prise en main de ce dossier par le Parlement, qui dispose de beaucoup de pouvoir en cette période d'affaires courantes gouvernementales. Il faudra organiser une rencontre avec les experts, les autorités compétentes, la Commission européenne, pour voir comment les autres pays s'organisent à ce sujet*"[62];

omdat gezichtsherkenning op afstand, inzameling van vingerafdrukken of registratie van de stem gemakkelijk kan gebeuren zonder medeweten van de betrokkene"[58];

I. overwegende dat de Gegevensbeschermingsautoriteit met betrekking tot de invoering van een systeem voor biometrische authenticatie meent dat rekening moet worden gehouden met de proportionaliteit van een dergelijke invoering en derhalve het volgende stelt: "*het systeem moet afdoende beveiligd worden*"[59];

J. overwegende dat de Gegevensbeschermingsautoriteit er in dat verband op wijst dat "*met verschillende, complexe regels*"[60] rekening moet worden gehouden;

K. overwegende dat de Gegevensbeschermingsautoriteit ter zake nog het volgende aanstipt: "*De verantwoordelijke voor de verwerking zal dus de categorieën plaatsen bepalen waar een biometrische controle noodzakelijk is en alleen van die personen de biometrische gegevens inzamelen die in het gebouw moeten zijn. Om anderzijds toegang tot een ruimte te beperken tot een bepaalde groep individuen, is het niet steeds noodzakelijk om gegevens te verwerken (zoals de naam) waarmee directe identificatie mogelijk wordt van de personen die beschikken over een recht van toegang. Zolang een persoon dus beschikt over een recht van toegang en dit met biometrie kan worden gecontroleerd, is het onnodig de biometrische informatie te koppelen aan bijkomende identificatiemiddelen.*"[61];

L. overwegende dat minister Philippe De Backer op 4 maart 2020 in de commissie voor Justitie op een vraag van volksvertegenwoordiger Gilles Vanden Burre het volgende heeft geantwoord: "*Je ne suis pas opposé à l'innovation en soi, puisqu'il existe aussi des applications positives de la reconnaissance faciale, mais il importe de rester très vigilant et très prudent face à l'introduction d'une telle technique dans la société. J'estime donc que nous devons poursuivre ce débat ici. C'est peut-être mieux de prendre son temps avant d'introduire cet outil dans la société. Je plaide donc pour une prise en main de ce dossier par le Parlement, qui dispose de beaucoup de pouvoir en cette période d'affaires courantes gouvernementales. Il faudra organiser une rencontre avec les experts, les autorités compétentes, la Commission européenne, pour voir comment les autres pays s'organisent à ce sujet.*"[62];

---

58 *Idem.*
59 *Idem.*
60 *Idem.*
61 *Idem.*
62 Commission de la Justice de la Chambre des représentants du 4 mars 2020. URL: *https://www.lachambre.be/doc/CCRI/html/55/ic125x.html*.

58 *Ibidem.*
59 *Ibidem.*
60 *Ibidem.*
61 *Ibidem.*
62 Commissie voor Justitie van de Kamer van volksvertegenwoordigers, 4 maart 2020. Te raadplegen op: *https://www.dekamer.be/doc/CCRI/html/55/ic125x.html*.

M. considérant que, interrogé par le député Gilles Vanden Burre le 4 mars 2020 en commission de la Justice, le ministre Philippe De Backer déclarait: "*En tout cas, je reste extrêmement prudent quant à l'introduction de cette technique, susceptible de constituer une base de données en masse. J'étais très favorable au moratoire qui figurait dans le texte européen initial. Apparemment, il a disparu. Dès lors, tout ce qui est lié à la reconnaissance faciale participe d'un risque élevé. Cela signifie qu'il importe de l'encadrer juridiquement, au moyen de textes légaux très précis, et de rester extrêmement prudent face à cette technique*"[63];

N. considérant que, interrogé par le député Gilles Vanden Burre le 4 mars 2020 en commission de la Justice, le ministre Philippe De Backer déclarait: "*Vous avez mentionné la possibilité de certaines exceptions. Cependant, vous savez aussi qu'à l'échelle européenne, nous avons toujours poussé en faveur d'un moratoire de cinq ans. Dans le dernier texte européen que j'ai consulté, il n'y figure plus. Or cela me semble nécessaire, parce que nous devons réfléchir à l'impact d'une telle technique sur la société. C'est pourquoi je suis très favorable à la tenue d'un débat au Parlement et/ou avec des instances telles que le COC (Organe de contrôle de l'information policière) ainsi qu'avec nos concitoyens, pour voir si c'est nécessaire et, si oui, dans quel contexte*"[64];

O. considérant que dans son "*rapport intermédiaire avec mesure correctrice concernant la visite menée auprès de la police fédérale de l'aéroport de Zaventem par l'organe de contrôle de l'information policière et portant sur l'utilisation de la reconnaissance faciale à l'aéroport national de Zaventem*" le COC (Organe de contrôle de l'information policière) indique que "*L'Organe de contrôle a (ensuite) mené le 9 août 2019 une visite auprès de la police fédérale de l'aéroport de Zaventem*". *Le contrôle* "*visait concrètement à se faire une idée de la technologie utilisée et à obtenir des informations au sujet du timing prévu, du fondement légal concret, des finalités du traitement, des données à caractère personnel traitées, des mesures prises en matière de*

M. overwegende dat minister Philippe De Backer op 4 maart 2020 in de commissie voor Justitie het volgende heeft geantwoord op een vraag van volksvertegenwoordiger Gilles Vanden Burre: "*En tout cas, je reste extrêmement prudent quant à l'introduction de cette technique, susceptible de constituer une base de données en masse. J'étais très favorable au moratoire qui figurait dans le texte européen initial. Apparemment, il a disparu. Dès lors, tout ce qui est lié à la reconnaissance faciale participe d'un risque élevé. Cela signifie qu'il importe de l'encadrer juridiquement, au moyen de textes légaux très précis, et de rester extrêmement prudent face à cette technique.*"[63];

N. overwegende dat minister Philippe De Backer op 4 maart 2020 in de commissie voor Justitie het volgende heeft geantwoord op een vraag van volksvertegenwoordiger Gilles Vanden Burre: "*Vous avez mentionné la possibilité de certaines exceptions. Cependant, vous savez aussi qu'à l'échelle européenne, nous avons toujours poussé en faveur d'un moratoire de cinq ans. Dans le dernier texte européen que j'ai consulté, il n'y figure plus. Or cela me semble nécessaire, parce que nous devons réfléchir à l'impact d'une telle technique sur la société. C'est pourquoi je suis très favorable à la tenue d'un débat au Parlement et/ou avec des instances telles que le COC (Organe de contrôle de l'information policière) ainsi qu'avec nos concitoyens, pour voir si c'est nécessaire et, si oui, dans quel contexte.*"[64];

O. overwegende dat het Controleorgaan op de politionele informatie (COC) in zijn "*Tussentijds rapport met corrigerende maatregel betreffende de visitatie bij de federale politie van de luchthaven Zaventem door het Controleorgaan op de politionele informatie met betrekking tot het gebruik van gezichtsherkenning op de nationale lucthaven van Zaventem*" het volgende aangeeft: "Vervolgens heeft het Controleorgaan op 9 augustus 2019 een visitatie uitgevoerd bij de federale politie van de luchthaven van Zaventem (hierna afgekort als "LPA"). Met de visitatie werd (…) beoogd concreet inzicht te krijgen in de gebruikte technologie en informatie te bekomen over de voorziene timing, de concrete wettelijke grondslag, de doeleinden van de verwerking, de

63 *Idem.*

64 Commission de la Justice de la Chambre des représentants du 4 mars 2020. URL: *https://www.lachambre.be/doc/CCRI/html/55/ic125x.html*.

63 *Idem.*

64 Commissie voor Justitie van de Kamer van volksvertegenwoordigers, *op.cit*.

sécurité de l'information, de la durée de conservation des données et des banques de données de photographies utilisées"[65];

P. considérant que dans ce rapport, le COC indique que "*Brussels Airport Company* (BAC) *a acheté début 2017 pour la LPA un logiciel en vue de tester un système de reconnaissance faciale. Il s'agit de quatre caméras. (…) Les tests ayant révélé une marge d'erreur très importante (faux positifs), il y a été mis un terme en mars 2017. De nombreux problèmes avaient notamment été constatés au niveau de la reconnaissance de la couleur de peau, des lunettes et, dans une moindre mesure, de la pilosité (moustache, barbe, etc.). L'utilisation de la reconnaissance faciale se trouvait par conséquent encore dans une phase de test*";

Q. considérant que dans ce rapport, le COC indique que "*La possibilité de tester un système de reconnaissance faciale soulève en premier lieu des questions quant au champ d'application exact du traitement. Lors de la détermination du cadre juridique correct, il n'est en effet pas possible d'établir d'emblée s'il est déjà question, au niveau de l'environnement de test ou pendant une période de test, du traitement de données à caractère personnel dans le cadre de la recherche et de la poursuite – et donc si la LFP et le titre II de la LPD trouvent application. Or, la réponse à cette question est cruciale pour désigner le fondement légal, le niveau de décision habilité au sein de la police à décider de recourir à la reconnaissance faciale, la nature du support de stockage et la durée de conservation, et le niveau de sécurité de l'information à observer (caractère opérationnel ou non)*";

R. considérant que dans ce rapport, le COC indique que "*En second lieu et à titre subsidiaire, l'Organe de contrôle constate toutefois que la LFP, dans l'hypothèse où elle s'applique, décrit bel et bien ce qui relève de la définition d'une caméra intelligente, mais ne stipule pas dans quelles circonstances ni sous quelles conditions l'utilisation de caméras permettant la reconnaissance faciale est autorisée, et encore moins sur quel support les images peuvent/doivent être enregistrées et quelles données doivent au minimum être conservées. Dans l'état actuel de la législation, le législateur a exclusivement voulu réglementer la création d'une banque de données technique pour les images ANPR. Selon toutes les informations recueillies par l'Organe de contrôle, les "snapshots" sont bel et bien conservés*

verwerkte persoonsgegevens, de informatieveiligheidsmaatregelen, de bewaarduur van de gegevens en de gebruikte foto-databanken."[65];

P. overwegende dat het COC in dat rapport aanstipt "dat begin 2017 door Brussels Airport Company (BAC) *ten behoeve van de LPA software werd aangekocht voor het uittesten van een systeem van gezichtsherkenning. Het gaat om vier camera's. (…) Omdat tijdens het testen een zeer grote foutenmarge (valse positieven) werd vastgesteld, werd het testen van het systeem in maart 2017 stopgezet. Zo waren er tal van problemen met de herkenning van huidskleur, brillen en, in mindere mate, de lichaamsbeharing (snor, baard enzovoort). Het gebruik van gezichtsherkenning bevond zich bijgevolg nog in een testfase.*";

Q. overwegende dat het COC in dat rapport op het volgende wijst: "*In de eerste plaats echter rijzen, bij de mogelijkheid om een systeem voor gezichtsherkenning te testen, vragen naar het precieze toepassingsgebied van de verwerking. Bij het bepalen van het correcte juridisch kader is het immers niet meteen zonneklaar of op het niveau van de testomgeving of tijdens een testperiode reeds sprake is van de verwerking van persoonsgegevens in het kader van opsporing en vervolging en dus de toepassing van de WPA en titel II WGB. Het antwoord op deze vraag is van cruciaal belang voor het aanduiden van de wettelijke grondslag, het beslissingsniveau bij de politie om gezichtsherkenning in te zetten, de aard van en termijn van het opslagmedium en het niveau van het informatieveiligheid (al dan niet operationeel karakter).*";

R. overwegende dat het COC in dat rapport het volgende aangeeft: "*In de tweede plaats en subsidiair stelt het Controleorgaan evenwel vast dat de WPA, indien van toepassing, weliswaar beschrijft wat binnen de definitie van "intelligente camera" valt, maar niet regelt in welke omstandigheden en onder welke voorwaarden het gebruik van camera's met gezichtsherkenning is toegestaan, laat staan op welke drager de beelden kunnen/moeten worden opgeslagen en welke gegevens minstens moeten bewaard worden. In de huidige stand van de wetgeving heeft de wetgever uitsluitend de oprichting van een technische gegevensbank voor ANPR-beelden willen regelen. Uit alles wat het Controleorgaan thans heeft begrepen worden de snapshots wel degelijk (tijdelijk) bewaard wat, nogmaals indien*

[65] *"Rapport de visite et de surveillance: Rapport intermédiaire avec mesure correctrice concernant la visite menée auprès de la police fédérale de l'aéroport de Zaventem par l'organe de contrôle de l'information policière et portant sur l'utilisation de la reconnaissance faciale à l'aéroport national de Zaventem",* site Internet du COC, 16 septembre 2019.

[65] *Visitatie-toezichtrapport: Tussentijds rapport met corrigerende maatregel betreffende de visitatie bij de federale politie van de luchthaven Zaventem door het Controleorgaan op de politionele informatie met betrekking tot het gebruik van gezichtsherkenning op de nationale luchthaven van Zaventem*, website van het COC, 16 september 2019.

(temporairement), ce qui implique – à nouveau dans l'hypothèse où la LFP/LPD trouve(nt) application – la création d'une banque de données technique contenant des données biométriques, ce qui n'est pas possible dans l'état actuel de la législation";

S. étant donné que des sociétés privées ainsi que des autorités publiques mettent en place ce type de technologie (caméras à reconnaissance faciale ou caméras thermiques par exemple) afin de lutter contre la pandémie du COVID-19, alors que d'autres autorités interdisent d'utilisation de telles technologies;

T. étant donné que plusieurs experts du domaine mettent en garde contre de nombreuses limites ou dangers associé(e)s à ces technologies, et que plusieurs expériences démontrent ces limites et dangers;

U. considérant que le ministre de l'Intérieur Peter De Crem a déclaré qu'il souhaitait introduire la reconnaissance faciale et qu'il est donc nécessaire que la Chambre des représentants lance sans tarder un débat à ce sujet;

V. considérant qu'il est important de considérer que des droits pourraient être impactés avec la mise en place de la reconnaissance faciale, comme le droit au respect de la vie privée, la protection des données personnelles ou la liberté de réunion[66];

W. considérant l'article 12 de la Déclaration universelle des droits de l'homme qui déclare que "*Nul ne sera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes à son honneur et à sa réputation. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes*"[67];

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

66 *"OVERVIEW: FACIAL RECOGNITION TO COMBAT CRIME"*, The Danish Institute for Human Rights, décembre 2019.

67 *https://www.un.org/fr/universal-declaration-human-rights/*.

de WPA/WGB van toepassing is, betekent dat er een technische gegevensbank met biometrische gegevens wordt aangelegd, wat actueel wettelijk niet mogelijk is.";

S. aangezien zowel privéondernemingen als overheden van dit soort technologie gebruik maken (bijvoorbeeld camera's met gezichtsherkenning of thermische camera's) om de COVID-19-pandemie aan te pakken, terwijl andere overheden het gebruik van dergelijke technologieën verbieden;

T. aangezien meerdere deskundigen ter zake waarschuwen voor de vele aan die technologieën verbonden grenzen of gevaren, en dat verschillende experimenten die grenzen en gevaren aantonen;

U. overwegende dat minister van Binnenlandse Zaken Pieter De Crem heeft verklaard dat hij de gezichtsherkenning wil invoeren en dat de Kamer van volksvertegenwoordigers daarover dus onverwijld een debat dient te voeren;

V. overwegende dat het belangrijk is in aanmerking te nemen dat de invoering van gezichtsherkenning bepaalde rechten kan aantasten, zoals het recht op de eerbiediging van het privéleven, de bescherming van de persoonsgegevens of de vrijheid van vergadering[66];

W. overwegende dat artikel 12 van de Universele Verklaring van de Rechten van de Mens bepaalt dat "*Niemand (…) onderworpen [zal] worden aan willekeurige inmenging in zijn persoonlijke aangelegenheden, in zijn gezin, zijn tehuis of zijn briefwisseling, noch aan enige aantasting van zijn eer of goede naam. Tegen een dergelijke inmenging of aantasting heeft een ieder recht op bescherming door de wet.*"[67];

X. overwegende dat artikel 8 van het Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden aangaande het recht op eerbiediging van privé, familie- en gezinsleven het volgende bepaalt: "*Een ieder heeft recht op respect voor zijn privéleven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie. Geen inmenging van enig openbaar gezag is toegestaan in de uitoefening van dit recht, dan voor zover bij de wet is voorzien en in een democratische samenleving noodzakelijk is in het belang van de nationale veiligheid, de openbare veiligheid of het economisch welzijn van het land, het voorkomen van*

66 *Overview: Facial Recognition to Combat Crime, The Danish Institute for Human Rights*, december 2019.

67 *https://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/dut.pdf*.

la santé ou de la morale, ou à la protection des droits et libertés d'autrui"[68];

Y. considérant l'article 7 de la Charte des droits fondamentaux de l'Union européenne qui concerne le respect de la vie privée et familiale et qui stipule que "*Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de ses communications*"[69];

Z. considérant l'article 22 de la Constitution belge qui stipule que "*Chacun a droit au respect de sa vie privée et familiale, sauf dans les cas et conditions fixés par la loi. La loi, le décret ou la règle visée à l'article 134 garantissent la protection de ce droit*"[70];

Z1. considérant que David Kaye (*The United Nations Special Rapporteur on freedom of opinion and expression*) "*called for an immediate moratorium on the sale, transfer and use of surveillance technology until human rights-compliant regulatory frameworks are in place*"[71];

Z2. considérant qu'on ne connaît pas encore l'impact précis qu'aura la technologie de reconnaissance faciale sur les droits humains, alors qu'il s'agit d'une question essentielle, et qu'il est par conséquent important de ne pas implémenter la technologie avant qu'on en connaisse toutes les implications;

Z3. considérant que selon la Commission européenne: "*La collecte et l'utilisation de données biométriques à des fins d'identification à distance, au moyen, par exemple, du déploiement de la reconnaissance faciale dans des lieux publics, comportent des risques particuliers en termes de droits fondamentaux. L'utilisation de systèmes d'IA pour l'identification biométrique à distance a des incidences sur les droits fondamentaux qui peuvent considérablement varier selon sa finalité, son contexte et sa portée*"[72];

Z4. considérant que selon la Commission européenne: "*Il s'ensuit, conformément aux règles de l'Union en*

wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden of voor de bescherming van de rechten en vrijheden van anderen"[68];

Y. overwegende dat artikel 7 van het Handvest van de grondrechten van de Europese Unie aangaande de eerbiediging van het privéleven en het familie- en gezinsleven het volgende bepaalt: "*Eenieder heeft recht op eerbiediging van zijn privéleven, zijn familie- en gezinsleven, zijn woning en zijn communicatie*"[69];

Z. overwegende dat artikel 22 van de Belgische Grondwet het volgende bepaalt: "*Ieder heeft recht op eerbiediging van zijn privéleven en zijn gezinsleven, behoudens in de gevallen en onder de voorwaarden door de wet bepaald. De wet, het decreet of de in artikel 134 bedoelde regel waarborgen de bescherming van dat recht*"[70];

Z1. overwegende dat David Kaye, Bijzonder rapporteur van de Verenigde Naties over de vrijheid van mening en van meningsuiting, "*called for an immediate moratorium on the sale, transfer and use of surveillance technology until human rights-compliant regulatory frameworks are in place*"[71];

Z2. overwegende dat de precieze impact van de gezichtsherkenningstechnologie op de mensenrechten nog niet gekend is, hoewel die kennis van wezenlijk belang is, en dat het derhalve belangrijk is van die technologie geen gebruik te maken voordat alle gevolgen in kaart zijn gebracht;

Z3. overwegende dat de Europese Commissie het volgende aangeeft: *"The gathering and use of biometric data for remote identification purposes, for instance through deployment of facial recognition in public places, carries specific risks for fundamental rights. The fundamental rights implications of using remote biometric identification AI systems can vary considerably depending on the purpose, context and scope of the use*"[72];

Z4. overwegende dat de Europese Commissie het volgende toevoegt: *"It follows that, in accordance with*

---

68 *https://www.echr.coe.int/Documents/Convention_FRA.pdf*.
69 *https://www.europarl.europa.eu/charter/pdf/text_fr.pdf*.
70 *http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&cn=1994021730&table_name=loi*.
71 *"UN expert calls for immediate moratorium on the sale, transfer and use of surveillance tools",* site Internet des Nations Unies Droits de l'Homme, le 25 juin 2019.
72 *"Livre blanc: Intelligence artificielle: Une approche européenne axée sur l'excellence et la confiance"*, Commission Européenne, le 19 février 2020.

68 *https://www.echr.coe.int/Documents/Convention_NLD.pdf*.
69 *https://www.europarl.europa.eu/charter/pdf/text_nl.pdf*.
70 *http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=nl&la=N&cn=1994021730&table_name=wet*.
71 *UN expert calls for immediate moratorium on the sale, transfer and use of surveillance tools",* 25 juni 2019, zie *https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=24736*.
72 *White Paper on Artificial Intelligence – A European approach to excellence and trust,* Europese Commissie, 19 februari 2020.

vigueur en matière de protection des données et à la Charte des droits fondamentaux de l'UE, que l'IA ne peut être utilisée à des fins d'identification biométrique à distance que lorsque cette utilisation est dûment justifiée, proportionnée et assortie de garanties adéquates[73]"[74];

Z5. considérant que selon la Commission européenne: "*Afin de répondre aux éventuelles inquiétudes, du point de vue de la société, quant à l'utilisation de l'IA à de telles fins dans les lieux publics et d'éviter toute fragmentation du marché intérieur, la Commission lancera un vaste débat européen sur les circonstances particulières, le cas échéant, qui pourraient justifier une telle utilisation, ainsi que sur les garanties communes à mettre en place*"[75];

DEMANDE AU GOUVERNEMENT FÉDÉRAL:

1. de mettre en place 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;

2. de mettre en place un débat à la Chambre des représentants sur ce sujet sensible, pour que cette technologie intrusive ne puisse être implémentée qu'à condition d'être accompagnée de garanties strictes concernant les droits humains.

20 mai 2020

Gilles VANDEN BURRE (Ecolo-Groen)
Jessika SOORS (Ecolo-Groen)
François DE SMET (DéFI)

the current EU data protection rules and the Charter of Fundamental Rights, AI can only be used for remote biometric identification purposes where such use is duly justified, proportionate and subject to adequate safeguards[73]"[74];

Z5. overwegende dat de Europese Commissie het volgende aanstipt: *"In order to address possible societal concerns relating to the use of AI for such purposes in public places, and to avoid fragmentation in the internal market, the Commission will launch a broad European debate on the specific circumstances, if any, which might justify such use, and on common safeguards*"[75];

VERZOEKT DE FEDERALE REGERING:

1. een moratorium van drie jaar in te stellen op het gebruik van software en van algoritmen voor gezichtsherkenning in vaste of mobiele veiligheidscamera's, in openbare en privéplaatsen;

2. ervoor zorgen dat in de Kamer van volksvertegenwoordigers een debat over dit gevoelige onderwerp wordt gehouden, opdat van deze intrusieve technologie alleen gebruik kan worden gemaakt als ze gepaard gaat met strikte garanties inzake de inachtneming van de rechten van de mens.

20 mei 2020

[73] Souligné par nous.
[74] *"Libre blanc: Intelligence artificielle: Une approche européenne axée sur l'excellence et la confiance"*, Commission Européenne, le 19 février 2020.
[75] *idem.*

[73] Wij onderstrepen.
[74] *White Paper on Artificial Intelligence – A European approach to excellence and trust, op.cit.*
[75] *Ibidem.*

Imprimerie centrale – Centrale drukkerij