DOC 55 **2716/001**

CHAMBRE DES REPRÉSENTANTS
DE BELGIQUE

23 mai 2022

ENQUÊTE DE CONTRÔLE DE L'ORGANE DE CONTRÔLE DE L'INFORMATION POLICIÈRE CONCERNANT L'UTILISATION DE *CLEARVIEW AI* PAR LA POLICE INTÉGRÉE

Audition

RAPPORT

FAIT AU NOM DE LA COMMISSION
DE L'INTÉRIEUR,
DE LA SÉCURITÉ, DE LA MIGRATION ET
DES MATIÈRES ADMINISTRATIVES
PAR
MME **Julie CHANSON**

SOMMAIRE Pages

BELGISCHE KAMER VAN
VOLKSVERTEGENWOORDIGERS

23 mei 2022

TOEZICHTONDERZOEK VAN HET CONTROLEORGAAN OP DE POLITIONELE INFORMATIE MET BETREKKING TOT HET GEBRUIK VAN *CLEARVIEW AI* DOOR DE GEÏNTEGREERDE POLITIE

Hoorzitting

VERSLAG

NAMENS DE COMMISSIE
VOOR BINNENLANDSE ZAKEN,
VEILIGHEID, MIGRATIE EN
BESTUURSZAKEN
UITGEBRACHT DOOR
MEVROUW **Julie CHANSON**

INHOUD Blz.

07092

Composition de la commission à la date de dépôt du rapport/
Samenstelling van de commissie op de datum van indiening van het verslag
Président/Voorzitter: Ortwin Depoortere

A. — Titulaires / Vaste leden:

N-VA	Sigrid Goethals, Yngvild Ingels, Koen Metsu
Ecolo-Groen	Julie Chanson, Simon Moutquin, Eva Platteau
PS	Hervé Rigot, Daniel Senesael, Eric Thiébaut
VB	Ortwin Depoortere, Dries Van Langenhove
MR	Philippe Pivin, Caroline Taquin
CD&V	Franky Demon
PVDA-PTB	Nabil Boukili
Open Vld	Tim Vandenput
Vooruit	Bert Moyaers

B. — Suppléants / Plaatsvervangers:

Christoph D'Haese, Joy Donné, Tomas Roggeman, Darya Safai
N ., Wouter De Vriendt, Claire Hugon, Stefaan Van Hecke
Khalil Aouasti, Hugues Bayet, André Flahaut, Ahmed Laaouej
Frank Troosters, Tom Van Grieken, Hans Verreyt
Denis Ducarme, Philippe Goffin, Florence Reuter
Jan Briers, Nahima Lanjri
Gaby Colebunders, Greet Daems
Katja Gabriëls, Marianne Verhaert
Ben Segers, Anja Vanrobaeys

C. — Membres sans voix délibérative / Niet-stemgerechtigde leden:

Les Engagés	Vanessa Matz
INDEP	Emir Kir
ONAFH	Emir Kir

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*
Vooruit	:	*Vooruit*
Les Engagés	:	*Les Engagés*
DéFI	:	*Démocrate Fédéraliste Indépendant*
INDEP-ONAFH	:	*Indépendant - Onafhankelijk*

Abréviations dans la numérotation des publications:		*Afkorting bij de nummering 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 vertaalde beknopt verslag van de toespraken (met de bijlagen)*
PLEN	*Séance plénière*	*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)*

MESDAMES, MESSIEURS,

Votre commission a consacré sa réunion du 9 mars 2022 à une audition portant sur l'enquête de contrôle de l'Organe de contrôle de l'information policière concernant l'utilisation de *Clearview AI* par la police intégrée.

I. — **PROCÉDURE**

La commission a décidé d'organiser cette audition lors de sa réunion du 19 octobre 2021.

En réponse à l'invitation à l'audition, l'Organe de contrôle a proposé que celle-ci ait lieu après la clôture de l'enquête qu'il menait dans cette affaire. La commission a accepté cette proposition.

Le rapport de contrôle a été remis à la présidente de la Chambre et à la commission le 14 février 2022.

MM. Frank Schuermans, membre-conseiller, et Ronny Saelens, commissaire-enquêteur, auprès de l'Organe de contrôle de l'information policière (COC) ont été entendus au cours de la réunion du 9 mars 2022.

II. — **EXPOSÉ INTRODUCTIF**

M. Frank Schuermans, membre-conseiller de l'Organe de contrôle de l'information policière (COC), revient aux origines de l'affaire: le contrôle du COC concernait le recours potentiel à l'application de reconnaissance faciale *Clearview AI* par la police intégrée (GPI)*. Clearview AI* est une application commerciale américaine qui permet de comparer au moyen d'un logiciel de reconnaissance faciale des photos avec des photos conservées dans la banque de données de *Clearview*.

Après un article de presse du 28 février 2020, l'Organe de contrôle a adressé le 2 mars 2020 un courrier au "Comité stratégique Information et ICT" de la GPI avec la question suivante: "La GPI belge ou l'une de ses composantes utilise ou expérimente actuellement avec la technologie de reconnaissance faciale (FRT)?".

Le 19 mai 2020, le COC a reçu la réponse suivante: "Sur la base des informations disponibles actuellement,

DAMES EN HEREN,

Uw commissie heeft haar vergadering van 9 maart 2022 gewijd aan een hoorzitting over het toezichtonderzoek van het Controleorgaan op de politionele informatie met betrekking tot het gebruik van *Clearview AI* door de geïntegreerde politie.

I. — **PROCEDURE**

De commissie heeft tot deze hoorzitting beslist tijdens haar vergadering van 19 oktober 2021.

Het Controleorgaan heeft in antwoord op de uitnodiging voor de hoorzitting voorgesteld om deze te laten plaatsvinden na de afronding van het onderzoek dat het orgaan ter zake voerde. De commissie is op dit voorstel ingegaan.

Het toezichtsrapport werd aan de Kamervoorzitster en de commissie bezorgd op 14 februari 2022.

Tijdens de vergadering van 9 maart 2022 werden de heren Frank Schuermans, lid-raadsheer, en de heer Ronny Saelens, commissaris-onderzoeker, van het Controleorgaan op de politionele informatie (COC), gehoord.

II. — **INLEIDENDE UITEENZETTING**

De heer Frank Schuermans, lid-raadsheer van het Controleorgaan op de politionele informatie (COC), bespreekt hoe de bal aan het rollen is gegaan. Het toezichtsonderzoek van het COC betrof het mogelijke gebruik van de gezichtsherkenningssoftware *Clearview AI* door de geïntegreerde politie (GPI). *Clearview AI* is een Amerikaanse commerciële informaticatoepassing waarmee middels gezichtsherkenningsoftware foto's kunnen worden vergeleken met foto's die worden bewaard in de gegevensbank van *Clearview*.

Naar aanleiding van een op 28 februari 2020 verschenen persartikel heeft het Controleorgaan op 2 maart 2020 een brief gericht aan het Strategisch Comité Informatie en ICT van de GPI, met daarin de volgende vraag: "Wordt actueel gebruik gemaakt of geëxperimenteerd met FRT door de Belgische GPI of één van haar onderdelen (hetzij de federale politie, hetzij een lokale politie)?".

Op 19 mei 2020 heeft het COC het volgende antwoord ontvangen: "Op basis van de thans beschikbare informatie

nous n'avons pas connaissance, au niveau organisationnel de la Police fédérale, d'une utilisation de logiciels de reconnaissance faciale au sein des services de police. Il n'existe pas non plus à ce stade d'intentions ni de projets d'utiliser de tels logiciels étant donné qu'une base légale plus solide est requise (…)". Le COC était donc convaincu que la police belge n'utilisait pas *Clearview*.

Le 25 août 2021, un nouvel article a été publié sur le site *Buzzfeednews* qui indiquait que la police fédérale belge aurait utilisé cette technologie entre 100 et 500 fois. Il y était aussi question d'une réunion d'Europol en octobre 2019, à laquelle la Belgique aurait participé et lors de laquelle le recours à cette technologie aurait été fait. Le COC a donc une nouvelle fois interrogé le 27 août 2021 le Commissaire général de la police fédérale qui a répondu le 22 septembre 2021. Il en ressort que la réalité était bien différente de la communication de mai 2020.

Afin d'obtenir toute la clarté, le COC a posé le 1er octobre 2021 un série de questions complémentaires. Le 18 octobre 2021, le Commissaire général a transmis le dossier de l'enquête interne.

L'enquête comprend trois parties. La première avait pour but de retracer les faits exacts et de vérifier dans quelle mesure la police fédérale avait respecté ses obligations légales. Sur cette base, deux membres de la DJSOC, qui avaient utilisé l'application dans le cadre d'Europol et par la suite, ont été entendus. Enfin, il a été procédé à l'évaluation juridique de l'utilisation de *Clearview*.

Le 10 janvier 2022, le projet de rapport a été transmis en prélecture au Commissaire général. Le 28 janvier 2022, le COC a reçu les remarques du CG. Le 4 février 2022, le rapport définitif a été approuvé par le COC.

L'utilisation de la technologie de reconnaissance faciale est un traitement de données à caractère personnel biométriques. Celles-ci sont, tout comme les empreintes digitales ou palmaires, particulièrement sensibles, car elles contiennent des caractéristiques personnelles uniques. Le processus de traitement est divisé essentiellement en trois phases. Après l'enregistrement de la photo (première phase), il est recouru à un logiciel qui a été conçu pour reconnaître les caractéristiques uniques de la personne sur la photo (deuxième phase). C'est au cours de cette phase qu'a lieu le traitement des données biométriques, à travers la conversion des

is er binnen de Federale Politie op organisatieniveau geen kennis over het gebruik van gezichtsherkenningssoftware binnen de politiediensten. Er zijn op dit moment ook geen intenties om dit soort software te gaan inzetten aangezien er een meer solide wettelijke basis vereist is (...)." Derhalve was het COC ervan overtuigd dat de Belgische politie geen gebruik maakte van *Clearview*.

Op 25 augustus 2021 werd een nieuw artikel gepubliceerd op de webstek *Buzzfeednews*, waarin werd aangegeven dat de Belgische federale politie die technologie tussen 100 en 500 keer zou hebben gebruikt. Er was in dat artikel ook sprake van een Europolvergadering in oktober 2019, waaraan België zou hebben deelgenomen en tijdens welke die technologie zou zijn gebruikt. Het COC heeft daarom op 27 augustus 2021 opnieuw vragen gesteld aan de Commissaris-generaal van de federale politie, die op 22 september 2021 heeft geantwoord. Uit dat antwoord bleek dat de werkelijkheid heel anders was dan in mei 2020 was meegedeeld.

Teneinde klaarheid te scheppen, heeft het COC op 1 oktober 2021 een aantal aanvullende vragen gesteld. Op 18 oktober 2021 heeft de Commissaris-generaal het dossier van het intern onderzoek bezorgd.

Het onderzoek bevat drie onderdelen. Het eerste had als doel de exacte feiten te achterhalen, alsook na te gaan in welke mate de federale politie haar wettelijke verplichtingen was nagekomen. Op basis daarvan werden vervolgens twee leden van *DJSOC* gehoord die de applicatie hebben gebruikt bij Europol en nadien. Tot slot werd overgegaan tot de juridische aftoetsing van het gebruik *Clearview*.

Op 10 januari 2022 werd het ontwerprapport in prelectuur bezorgd aan de Commissaris-generaal (CG). Op 28 januari 2022 ontving het COC diens opmerkingen. Op 4 februari 2022 werd het definitief rapport goedgekeurd door het COC.

Het gebruik van gezichtsherkenningstechnologie is een verwerking van biometrische persoonsgegevens. Deze zijn, zoals vinger- of handpalmafdrukken, bijzonder gevoelig omdat ze unieke persoonskenmerken bevatten. Het verwerkingsproces bestaat in essentie uit drie fasen. Nadat de foto wordt vastgelegd (eerste fase), wordt gebruik gemaakt van software die ontwikkeld wordt om unieke persoonskenmerken op die foto te herkennen (tweede fase). Het is in die fase dat de verwerking van biometrische gegevens gebeurt waarbij de "ruwe" gegevens in een unieke cijfercode worden omgezet (de zgn. template). Die template wordt dan vergeleken met andere

données “brutes” en un code chiffré unique (ce que l’on appelle un *template*). Ce *template* est ensuite comparé à d’autres images disponibles (troisième phase). En cas de résultat positif (*hit*), celui-ci doit être validé (*match*).

Dans un contexte policier, l’utilisation de la FRT poursuit *grosso modo* deux objectifs: l’identification à partir d’une recherche non ciblée ou ciblée de personnes.

Dans le cas d’une reconnaissance faciale non ciblée réalisée en public, une quantité très importante de photos ou d’images est comparée à une liste de personnes recherchées ou disparues. L’application de la reconnaissance faciale fonctionne à distance (*remote*). Elle est en principe “non ciblée” parce que les images ou photos d’un groupe non différencié de personnes sont captées. Il s’agit d’une situation “non suspect versus suspect/personne disparue” (N: 1).

En cas de reconnaissance faciale ciblée, les photos de suspects ou de personnes disparues sont comparées avec des photos ou des images recueillies par des caméras placées dans des lieux accessibles au public et il s’agit donc de l’opération inverse. Il s’agit d’une opération de recherche ciblée: l’image d’un suspect ou d’une victime est comparée avec des photos ou images (mises à disposition) en vue d’identifier ce suspect ou cette victime. L’application *Clearview* concerne une reconnaissance faciale ciblée en vue d’une identification réactive de victimes et d’auteurs. On recherche une ou des personnes spécifiques (auteurs ou victimes) parmi un nombre (in)déterminé de personnes (situation 1: N).

Selon ses propres dires, *Clearview* n’est accessible que pour les *“law enforcement agencies”. Clearview* exploite une banque de données gigantesque de photos et images de personnes qui sont accessibles sur Internet. L’entreprise propose une version de test gratuite pour trente jours. Le site de *Clearview* comporte un lien dénommé “*request trial*”. Lorsque l’utilisateur clique sur ce lien, il voit s’afficher un écran mentionnant que l’application est uniquement accessible à la police et que la véracité de cette qualité doit être établie sur la base d’une validation de la part du responsable hiérarchique de l’utilisateur du compte. Une fois le processus d’enregistrement terminé, l’utilisateur peut activer son compte. Lorsque l’utilisateur s’identifie avec son compte, il reçoit un lien qui lui permet de charger une photo. L’application compare automatiquement chaque photo avec la banque de données *Clearview*. Si la comparaison aboutit à un résultat positif, l’utilisateur reçoit un lien de la source dans laquelle *Clearview* a recueilli (*“scrapted”*) les photos (provenant d’internet). Enfin, le lien vers l’endroit où se trouve la photo peut renvoyer lui-même à une ou plusieurs autres sources numériques

beschikbare beelden (derde fase). Een positief resultaat (hit) moet vervolgens gevalideerd worden (match).

In een politionele context beoogt het gebruik van FRT grosso modo twee doelstellingen: identificatie op basis van een ongerichte dan wel gerichte opzoeking van personen.

Bij ongerichte publieke gezichtsherkenning wordt een omvangrijke hoeveelheid foto’s of beelden vergeleken met een lijst van gezochte/vermiste personen. De toepassing van de gezichtsherkenning werkt op afstand (*remote*). Ze is in beginsel “ongericht” omdat de beelden/foto’s van een ongedifferentieerde groep personen worden gecapteerd. Het betreft een “niet-verdachte versus verdachte/vermiste persoon”-situatie (N op 1).

Bij gerichte gezichtsherkenning worden de foto’s van verdachten of vermisten vergeleken met foto’s of beelden die door camera’s op publiek toegankelijk plaatsen worden verzameld en dat is dus de omgekeerde beweging. Dit is een gerichte opsporingshandeling: de afbeelding van een verdachte of slachtoffer wordt vergeleken met (ter beschikking gestelde) foto’s of beelden met het oog op de identificatie van die verdachte of dat slachtoffer. De *Clearview*-applicatie betreft een gerichte gezichtsherkenning met het oog op een reactieve identificatie van slachtoffer of dader. Er wordt gezocht naar een specifieke persoon (dader of slachtoffer) in een (on)bepaald aantal personen (1 op N-situatie).

Clearview zegt zelf dat de software van het bedrijf alleen toegankelijk is voor “*law enforcement agencies*”. De onderneming maakt gebruik van een enorm grote databank met via het internet toegankelijke foto’s en beelden van mensen. Het bedrijf biedt een testversie aan die dertig dagen gratis is. Op de webstek van *Clearview* staat een link met de woorden “*request trial*”. Wanneer de gebruiker op die link klikt, komt hij terecht op een scherm waarop wordt vermeld dat de toepassing alleen toegankelijk is voor politiediensten en dat die hoedanigheid moet worden aangetoond aan de hand van een bevestiging door de leidinggevende van de accountgebruiker. Wanneer de registratie is afgerond, kan de gebruiker zijn account activeren. Telkens als de gebruiker zich via zijn account aanmeldt, ontvangt hij een link waarmee een foto kan worden geüpload. De software vergelijkt elke foto automatisch met de gegevens in de databank van *Clearview*. Wanneer de vergelijking een positief resultaat oplevert, ontvangt de gebruiker een link naar de bron waar *Clearview* de (van het internet afkomstige) foto’s heeft gevonden (“*scrapted*”). Tot slot kan de link naar de plaats waar de foto zich bevindt, zelf

dans lesquelles d'autres photos sont éventuellement disponibles. L'application est très conviviale.

L'application a été utilisée pour la première fois par le service *Child abuse* de la DGJ/DJSOC entre le 14 et le 25 octobre 2019 durant la *taskforce* d'Europol, qui s'est déroulée dans le cadre des dossiers du *National Center for Missing and Exploited Children* américain. Ce centre collecte des images d'auteurs et de victimes potentiels, dont l'identité n'est pas connue et les faits éventuels n'ont pas encore été localisés dans le temps et l'espace. Lors de cette *taskforce,* les possibilités de la technologie ont été appliquées à des données de ce centre. Même après la *taskforce*, des photos et des images ont encore été utilisées dans le cadre d'enquêtes sur d'éventuels abus sexuels sur des mineurs. La dernière activité remonterait au 10 février 2020, après quoi les comptes ont été clôturés à l'initiative de *Clearview*.

Le DJSOC aurait effectué au total 78 recherches dans la banque de données de *Clearview,* sans jamais aboutir à un résultat positif dans le cadre des enquêtes menées en Belgique.

Deux questions se posent dans le cadre de l'enquête. Qui, au sein de la police fédérale, était au courant de l'utilisation de *Clearview* ou aurait dû l'être? Son utilisation est-elle et était-elle légale?

L'enquête du COC révèle que la DJSOC a été informée verbalement de l'utilisation de l'application *Clearview* immédiatement après la *taskforce,* et de manière formelle et par écrit au moins le 7 novembre 2019. Il est donc problématique, car incorrect, que le CG réponde, dans sa lettre du 19 mai 2020 adressée au COC, que "(...) nous n'avons pas connaissance (...) de l'utilisation de logiciels de reconnaissance faciale au sein des services de police". Ce n'est qu'après une nouvelle demande du COC, formulée le 27 août 2021, qu'une enquête interne sérieuse a eu lieu.

Indépendamment de l'utilisation illicite, d'un point de vue légal, de l'application par deux enquêteurs individuels (par ailleurs très zélés) de la DJSOC, le COC reproche surtout à la DGJ d'avoir manifestement dissimulé cette information, intentionnellement ou non, non seulement au COC, mais également au CG. Une telle attitude est incompatible avec le devoir de coopération imposé par la loi et est surtout problématique en raison du fait qu'une autorité de contrôle doit, en principe, pouvoir se fier à la véracité et la réalité des réponses des chefs de police. Le CG réplique qu'il ne perçoit de la part de la DGJ aucune volonté délibérée de dissimulation et met plutôt en avant un concours de circonstances. Le COC

doorverwijzen naar één of meer digitale bronnen waar eventueel andere foto's te vinden zijn. De toepassing is heel gebruiksvriendelijk.

De applicatie werd door de dienst *Child abuse* van DGJ/DJSOC voor het eerst tussen 14 en 25 oktober 2019 gebruikt tijdens de taskforce bij Europol, die plaatsvond in het raam van dossiers van het Amerikaanse *National Center for Missing and Exploited Children*. Dit centrum verzamelt beelden van potentiële daders en slachtoffers van wie de identiteit niet bekend is en van eventuele feiten die nog niet gelokaliseerd zijn in tijd en ruimte. Tijdens deze taskforce werden de mogelijkheden van de technologie toegepast op gegevens van dat centrum. Ook na afloop van de taskforce werd op foto's en beelden in het raam van onderzoeken naar potentieel seksueel misbruik van minderjarigen voortgewerkt. De laatste activiteit zou op 10 februari 2020 hebben plaatsgevonden, waarna de accounts op initiatief van *Clearview* werden afgesloten.

DJSOC zou in totaal 78 opzoekingen in de gegevensbank van *Clearview* hebben uitgevoerd zonder dat er, voor onderzoeken in België, een opsporingsmatig positief resultaat zou zijn geweest.

Er rezen twee onderzoeksvragen. Wie was er binnen de federale politie op de hoogte, of had dat moeten zijn, van het gebruik van *Clearview*? Is en was het gebruik ervan wettelijk?

Uit het onderzoek van het COC blijkt dat DJSOC onmiddellijk na afloop van de taskforce mondeling, en op zijn minst op 7 november 2019 formeel schriftelijk, op de hoogte was van het gebruik van de *Clearview*-applicatie. Het is dus problematisch, want niet correct, dat de CG in zijn brief van 19 mei 2020 aan het COC antwoordt, dat er "(...) geen kennis (is) over het gebruik van gezichtsherkenningssoftware binnen de politiediensten". Een ernstig intern onderzoek vindt eigenlijk pas plaats na de hernieuwde vraag van het COC van 27 augustus 2021.

Nog afgezien van het wettelijk onrechtmatig gebruik van de applicatie door twee (overigens gedreven) individuele onderzoekers van DJSOC, tilt het COC eigenlijk het zwaarst aan die – al dan niet bewuste – verzwijging, kennelijk niet enkel ten aanzien van het COC, maar ook ten aanzien van de CG. Een dergelijke houding is strijdig met de wettelijke medewerkingsplicht en is vooral problematisch omdat een toezichthouder er in beginsel moet op kunnen vertrouwen dat de antwoorden van politiechefs realiteits- en waarheidsgetrouw zijn. De CG repliceert geen moedwillige verzwijging te zien vanuit DGJ en wijst eerder op een samenloop van omstandigheden. Het COC neemt daar akte van en kan alleen maar hopen

en prend acte et ne peut qu'espérer que ce genre de communication – qui, disons, laisse à désirer – ne se reproduira plus.

Il ressort du dossier que la police judiciaire fédérale (PJF) a appliqué la technologie à des données à caractère personnel policières (photos et images). Le fait que ces images n'auraient pas eu trait à des "dossiers belges" n'y change rien. Le cadre juridique actuel s'applique sans restriction. La PJF a communiqué des données policières à une entreprise tierce privée étrangère. Une telle communication de données ne trouve nullement appui dans la législation belge.

En effet, à la lumière de la qualité de la base légale imposée par la jurisprudence pour le traitement de données biométriques par des autorités répressives, une base légale spécifique et claire est requise, en ce sens que les circonstances et conditions du recours à cette technologie doivent être définies dans une norme de droit et accompagnées de garanties de sécurité spécifiques et adéquates. Le COC a déjà souligné cela précédemment dans le dossier de la police de l'aéroport de Zaventem où il a dû prendre la mesure correctrice d'arrêter un système de reconnaissance faciale.

Dans le cas présent, des données policières ont été transmises à un destinataire se trouvant dans un pays tiers (hors de l'UE) sans qu'il ne soit établi que ce dernier garantit un niveau de protection adéquat et en dépit des dispositions de la loi du 5 août 1992 sur la fonction de police (LFP) qui s'opposent à une telle communication à une instance ou entreprise privée belge, européenne, et *a fortiori* américaine.

Il relève de la responsabilité du responsable du traitement – en l'occurrence la PJF – d'examiner si l'utilisation expérimentale de cette technologie était légalement possible. En faisant une analyse d'impact relative à la protection des données (AIPD), obligatoirement prévue par la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel (LPD), il aurait été évident qu'on était hors de la loi. La PJF n'a pas fait une telle analyse.

L'utilisation de *Clearview* par la DJSOC et l'utilisation de la FRT par la police de l'aéroport de Bruxelles-National ont en commun qu'elles se sont dans les deux cas déroulées au cours d'une phase dite "de test". Mais même dans ce cas, la loi doit être respectée. La différence essentielle entre les deux cas se situe surtout dans le processus de traitement sous-jacent. L'utilisateur de *Clearview* n'exerce aucun contrôle sur le traitement des données

dat dit soort van manke communicatie – zo zullen we het dan maar noemen – zich niet meer herhaalt.

Uit het dossier blijkt dat de federale gerechtelijke politie (FGP) de technologie heeft toegepast op politionele persoonsgegevens (foto's en afbeeldingen). Dat die beelden geen betrekking zouden hebben gehad op "Belgische dossiers", doet daar niets aan af. De geldende wet- en regelgeving is onverkort van toepassing. De FGP heeft politionele gegevens meegedeeld aan een buitenlandse derde private onderneming. In de Belgische wetgeving is nergens een rechtsbasis te vinden voor een dergelijke mededeling van gegevens.

Aangezien uit de rechtspraak blijkt dat de rechtshandhavingsautoriteiten voor de verwerking van biometrische gegevens moeten bogen op solide wettelijke grondslagen, is een specifieke en duidelijke wettelijke basis vereist waarbij de omstandigheden en voorwaarden voor het gebruik van die technologie in een rechtsnorm worden vastgelegd, samen met specifieke en adequate veiligheidswaarborgen. In dat verband werd door het COC reeds gewezen op het ontbreken van een specifieke wettelijke basis voor het gebruik van gezichtsherkenningstechnologie door de luchthavenpolitie van Zaventem, waarna het gebruik ervan werd stopgezet.

In deze context werden politionele gegevens doorgegeven aan een geadresseerde die zich in een derde land (buiten de EU) bevond, zonder dat vaststond dat die een passend beschermingsniveau bood en in weerwil van de bepalingen van de wet van 5 augustus 1992 op het politieambt (WPA), op grond waarvan zulks niet is toegestaan (niet aan een Belgische of Europese instelling of onderneming, en al zeker niet aan een Amerikaanse).

Zodoende komt het de verwerkingsverantwoordelijke, *in casu* de FGP, toe te onderzoeken of het experimenteel gebruik van die technologie wettelijk mogelijk was. De verplichte gegevensbeschermingseffectbeoordeling (GEB), zoals bedoeld in de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens (WGB), had moeten doen uitkomen dat men buiten het wettelijk raamwerk viel. De FGP heeft een dergelijke beoordeling niet uitgevoerd.

Het gebruik van *Clearview* door DJSOC en het gebruik van FRT door de luchtvaartpolitie (LPA) Brussel-Nationaal hebben gemeen dat beide gevallen zich mede in een zogenaamde "testfase" hebben afgespeeld. Maar ook dan moet de wet worden nageleefd. Het wezenlijk onderscheid tussen beide gevallen is vooral gelegen in het achterliggend verwerkingsproces. De *Clearview*-gebruiker heeft geen enkele controle over de verwerking van de

biométriques. Les images sont chargées, de sorte que leur disponibilité est entièrement confiée à l'entreprise américaine *Clearview*, et sont donc envoyées en dehors de l'ordre judiciaire de l'Union européenne. La police n'a plus aucune prise sur la suite du processus de traitement par le destinataire (notamment sur la durée de conservation des images et sur l'usage commercial de ces données policières). Par ailleurs, il est difficile de savoir si, en marge du *template*, *Clearview* a également conservé les données biométriques brutes, voire les exploite ou les a exploitées par la suite à des fins commerciales.

Les traitements ont également lieu durant une phase préalable à l'ouverture d'une information ou d'une instruction et ils se cantonnent au niveau policier. De ce fait, le COC n'a pas non plus pu vérifier matériellement si l'utilisation de la reconnaissance faciale a effectivement conduit à un résultat négatif ou positif. Le COC a dû se baser sur les affirmations des deux enquêteurs. Nulle part, ces traitements de données à caractère personnel ne sont saisis dans les banques de données policières existantes et il ne reste aucune trace des opérations effectuées.

Les enquêteurs concernés ne voyaient aucun problème juridique et considéraient *Clearview* comme une forme d'*open source intelligence,* une sorte de recherche sur Google. Cependant, son utilisation est incontestablement un acte d'information policier, ce qui implique le respect d'obligations telles que la traçabilité.

Il y a donc eu une "expérimentation" libre, avec des photos personnelles des fonctionnaires de police participants, et avec des photos de victimes et/ou d'auteurs provenant de dossiers prétendument américains. Ce qui est surtout inquiétant pour le COC, c'est le fait que la direction de la DGJ ou de la DJSOC ne semble pas avoir pris en considération l'impact et les conséquences du processus de traitement. Elle semble à tout le moins ne pas suffisamment comprendre la portée procédurale et juridique de ce processus. Elle semble ne pas réaliser que non seulement des photos de la police sont transmises à une entreprise commerciale en dehors de l'Union européenne, mais également les données biométriques sont depuis lors conservées par l'entreprise. Le COC émet également de sérieux doutes quant au processus de validation allégué par *Clearview* concernant une utilisation à des fins qui seraient exclusivement policières.

Il est également erroné de penser que seules des photos d'auteurs et/ou de suspects sont conservées. Logiquement, il s'agit de photos qui font partie de dossiers de la police. Donc, des photos non seulement d'auteurs,

biometrische gegevens. De beelden worden opgeladen, waardoor de beschikbaarheid erover volledig wordt overgedragen aan het Amerikaanse *Clearview* en dus buiten de EU-rechtsorde worden gestuurd. De politie heeft geen enkel vat meer op het verdere verwerkingsproces door de ontvanger (het gaat dan onder andere over de bewaartermijn van de beelden en het verdere commerciële gebruik van deze politiegegevens). Het is ook onduidelijk of *Clearview* naast de template ook de ruwe biometrische gegevens heeft bewaard, laat staan verder commercieel (heeft) (ge)exploiteert(d).

De verwerkingen spelen zich ook af in een fase voorafgaand aan de opstart van een opsporingsonderzoek of gerechtelijk onderzoek en blijven "hangen" op politioneel niveau. Daardoor kon het COC ook niet materialiter nagaan of het gebruik van de gezichtsherkenning effectief een negatief dan wel positief opsporingsresultaat heeft opgeleverd. Het COC heeft zich moeten steunen op de beweringen van de twee onderzoekers. Nergens blijken er in de bestaande politionele gegevensbanken logs te gebeuren van deze verwerkingen van persoonsgegevens of is er een spoor terug te vinden van de gestelde handelingen.

Door de betrokken rechercheurs werd er geen juridisch probleem gezien en werd *Clearview* als een vorm van *open source intelligence* gezien, een soort van *Google Search*. Het gebruik ervan is nochtans onmiskenbaar een politionele onderzoekshandeling waardoor aan verplichtingen zoals traceerbaarheid moet worden voldaan.

Er werd dus vrij "geëxperimenteerd" met persoonlijke foto's van deelnemende politieambtenaren en met beelden van slachtoffers en/of daders uit beweerdelijk Amerikaanse dossiers. Verontrustend is voor het COC in hoofdorde dat de leiding DGJ of DJSOC geen oog lijkt te hebben gehad voor de impact en de gevolgen van het verwerkingsproces. Minstens lijken ze de draagwijdte ervan onvoldoende procesmatig en juridisch te begrijpen. Men leek niet te beseffen dat niet enkel politionele foto's aan een commercieel bedrijf buiten de EU werden doorgestuurd, noch dat de biometrische gegevens sindsdien door het bedrijf bijgehouden worden. Het COC heeft ook grote twijfels over het beweerde validatieproces bij *Clearview* omtrent het zogenaamd uitsluitend gebruik door politiediensten.

Het is ook een misvatting te denken dat alleen foto's van daders en/of verdachten worden bijgehouden. Het betreft logischerwijze foto's die deel uitmaken van politionele dossiers. Dus niet enkel daders, maar ook

mais aussi de victimes (des personnes très vulnérables) et même de témoins ou de passants occasionnels se retrouvent aux mains de cette entreprise américaine.

Le COC a émis trois recommandations et pris deux mesures correctrices:

Recommandation 1: l'organisation de formations et la sensibilisation des membres du personnel (et surtout des dirigeants) concernant le recours à l'*open source intelligence* ou à des applications/banques de données particulières en fonction du cadre juridique applicable. Le COC doit régulièrement rappeler à la GPI qu'en matière de gestion de l'information, non seulement les citoyens, mais aussi la police doivent respecter la loi.

Recommandation 2: la mise en place d'un cadre juridique clair pour les traitements d'informations et de données à caractère personnel policières à des fins de test dans une phase expérimentale. Cette recommandation doit se lire conjointement avec l'avis n° DA210029 du 24 janvier 2022 relatif à une proposition de résolution pour la mise en place d'un moratoire de trois ans sur l'utilisation de logiciels et d'algorithmes de reconnaissance faciale sur les caméras de sécurité, fixes ou mobiles, dans les endroits publics et privés (DOC 55 1349/001 du 16 juin 2020).

Recommandation 3**:** dans le cas où l'utilisation de la technologie de reconnaissance faciale serait autorisée par la loi, le COC souhaite que de nombreux aspects soient pris en compte, afin que la loi soit conforme aux exigences des jurisprudences européenne et belge en termes de légalité, de prévisibilité, de clarté, de sécurité de l'information, de transparence, etc.

Après avoir constaté que l'utilisation de la technologie de reconnaissance faciale *Clearview* n'était et n'est pas légale, le COC a ordonné à la police fédérale, comme première mesure correctrice, de prendre les initiatives nécessaires pour respecter ses obligations en tant que responsable du traitement en cas de *databreach,* et notamment l'initiative de sommer *Clearview*:

— de supprimer de sa banque de données les photos transmises par la DJSOC;

— de supprimer le traitement biométrique auprès de *Clearview*, à savoir le *template* et les données biométriques brutes.

Enfin, comme deuxième mesure correctrice, le COC a averti la police fédérale que toute utilisation (future) de la technologie de reconnaissance faciale *Clearview*

slachtoffers (zeer kwetsbare personen) en zelfs getuigen of omstaanders komen zo in handen van dit Amerikaans bedrijf.

Het COC heeft drie aanbevelingen en twee corrigerende maatregelen genomen:

Aanbeveling 1: het organiseren van opleidingen en het stimuleren van *awareness* bij de personeelsleden (en vooral leidinggevenden) bij het gebruik van *open source intelligence* of bijzondere applicaties/gegevensbanken afhankelijk van het toepasselijk juridisch kader; het COC moet de GPI er op het stuk van informatiehuishouding geregeld aan herinneren dat niet alleen de burger, maar ook de politie zich aan de wet moet houden.

Aanbeveling 2: verwerkingen van politionele informatie en persoonsgegevens met het oog op het (uit)testen, in een experimentele fase, moeten een helder juridisch kader krijgt; dit moet samen gelezen worden met het advies DA210029 van 24 januari 2022 betreffende een voorstel van resolutie over een driejarig moratorium op het gebruik van gezichtsherkenningssoftware en -algoritmen in vaste of mobiele beveiligingscamera's in openbare en privéplaatsen (DOC 55 1349/001 van 16 juni 2020).

Aanbeveling 3**:** wanneer het gebruik van gezichtsherkenningstechnologie in de wet zou worden vastgelegd, wenst het COC dat een reeks aspecten worden geregeld die maken dat de wetgeving voldoet aan de vereisten van de Europese en Belgische rechtspraak, die te maken hebben met legaliteit, voorzienbaarheid, duidelijkheid, informatieveiligheid, transparantie en dergelijke meer.

Na te hebben vastgesteld dat het gebruik van de *Clearview*-gezichtsherkenningstechnologie niet wettelijk was noch is, heeft het COC als eerste corrigerende maatregel de federale politie bevolen de nodige initiatieven te nemen teneinde hun verplichtingen als verwerkingsverantwoordelijke bij een *databreach* na te komen en daartoe behoort minstens het initiatief *Clearview* ertoe aan te zetten om:

— de door de DJSOC verstrekte foto's uit haar gegevensbank te verwijderen;

— de biometrische verwerking, met name de template en de ruwe biometrische gegevens, bij *Clearview* te verwijderen.

Tot slot heeft het COC als tweede corrigerende maatregel de federale politie gewaarschuwd dat elk (toekomstig)

ou d'une application/banque de données similaire est illégale.

III. — **DISCUSSION**

A. **Questions et observations des membres**

Mme Yngvild Ingels (N-VA) souhaiterait savoir où en est la mise en œuvre des mesures correctrices et des recommandations du COC. Plus généralement, elle souligne les réticences des services de police à l'égard des nouvelles technologies, de sorte que la législation est souvent en retard. Ne serait-il pas judicieux de créer un cadre légal pour des champs d'expérimentation, afin de permettre l'utilisation de nouveaux moyens techniques sous le contrôle du COC, de manière à donner toutes les garanties de sécurité possibles?

Mme Eva Platteau (Ecolo-Groen) est surtout étonnée par le manque de communication dans ce dossier. En effet, l'information sur l'erreur d'évaluation lors d'une phase de test n'a initialement pas été transmise au Commissaire général et donc pas non plus à l'autorité de contrôle. Quelle en est la raison?

L'intervenante se réfère ensuite à la proposition de résolution qui a été déposée par Mme Chanson (DOC 55 1349/001). Cette proposition demande un moratoire de trois ans sur l'utilisation des logiciels de reconnaissance faciale jusqu'à ce qu'un cadre légal puisse être clairement défini. L'intervenante souhaiterait savoir si les représentants du COC soutiennent cette idée. En effet, les recommandations précisent que le personnel et les dirigeants de la police fédérale doivent être davantage sensibilisés à l'utilisation du logiciel et à ses conséquences au niveau de la protection de la vie privée. Cela signifie-t-il concrètement que davantage de formations consacrées au respect de la vie privée et au RGPD doivent être organisées au sein de la police?

Enfin, l'incident s'est produit dans le cadre d'une *taskforce* d'Europol sur les abus commis sur des enfants. Il est important que les auteurs de tels actes soient recherchés. Serait-il possible qu'à l'avenir, Europol travaille avec sa propre base de données ou son propre logiciel, de manière à ce que la police ne soit plus dépendante d'une société informatique privée américaine sur laquelle les autorités belges n'ont aucun contrôle?

Pour *M. Hervé Rigot (PS)*, les termes utilisés dans le rapport démontrent qu'il s'agit de faits graves. Que l'usage ait été formel ou informel, dans un cadre de test ou d'enquête, ne justifie en aucun cas l'utilisation

gebruik van de *Clearview*-gezichtsherkenningstechnologie of een gelijkaardige applicatie/gegevensbank onwettig is.

III. — **BESPREKING**

A. **Vragen en opmerkingen van de leden**

Mevrouw Yngvild Ingels (N-VA) wil weten hoe het staat met de uitvoering van de corrigerende maatregelen en de aanbevelingen van het COC. Meer in het algemeen stipt de spreekster het spanningsveld aan dat bij de politiediensten bestaat ten aanzien van nieuwe technologieën, waarbij men vaststelt dat de wetgeving vaak iets achterloopt. Zou het geen goede zaak zijn om een wettelijk kader te creëren voor proeftuinen teneinde het gebruik van nieuwe technische middelen onder het toezicht van het COC mogelijk te maken, zodat alle mogelijke veiligheidsgaranties gegeven kunnen worden?

Mevrouw Eva Platteau (Ecolo-Groen) is vooral verbaasd over de manke communicatie in dit dossier. De informatie over de inschattingsfout tijdens een testfase werd aanvankelijk immers niet doorgegeven aan de Commissaris-generaal en derhalve evenmin aan de toezichthouder. Wat is daar de oorzaak van?

Vervolgens verwijst de spreekster naar het voorstel van resolutie dat werd ingediend door mevrouw Chanson (DOC 55 1349/001). Daarin wordt verzocht om een driejarig moratorium op het gebruik van gezichtsherkenningssoftware tot het wettelijk kader duidelijk afgebakend kan worden. De spreekster wil graag van de vertegenwoordigers van het COC vernemen of ze dat idee genegen zijn. In de aanbevelingen wordt immers gesteld dat er meer bewustzijn nodig is bij de personeelsleden en leidinggevenden van de federale politie omtrent het gebruik van de software en de implicaties voor de privacy. Betekent dat concreet dat er bij de politie meer opleidingen georganiseerd moeten worden rond privacy en de GDPR?

Tot slot heeft het voorval zich voorgedaan in het kader van een taskforce van Europol rond kindermisbruik. Het is belangrijk dat daders van dergelijke feiten opgespoord worden. Is het mogelijk dat Europol in de toekomst met een eigen database of eigen software zal werken, zodat de politie niet meer afhankelijk is van een Amerikaans privaat softwarebedrijf waarover Belgische instanties geen controle hebben?

De heer Hervé Rigot (PS) is van oordeel dat de woordkeus in het verslag aangeeft dat de feiten ernstig zijn. Het gebruik van *Clearview* door de politiediensten valt niet te verantwoorden, ongeacht of de technologie

de *Clearview* par les services de police. Cette affaire démontre un problème flagrant de communication au sein de nos entités policières. Il y a une chaîne de commandement qui a failli. La hiérarchie était informée mais n'a pas réagi à temps. L'intervenant s'étonne qu'il n'ait pas été possible d'arrêter plus tôt l'usage de *Clearview*, au vu des illégalités multiples.

Pour M. Rigot, ce n'est pas parce que les choses sont possibles d'un point de vue technologie qu'elles sont autorisées. En ce sens, il convient de procéder à la sensibilisation des policiers: ces derniers doivent faire respecter la loi mais ils doivent aussi respecter eux-mêmes la loi.

Les personnes qui se retrouvent sur ces photos ont-elles été informées? De cette manière, elles pourraient être en mesure de faire valoir leurs droits.

La CNIL a ordonné à *Clearview* de supprimer toutes les photos qu'elle détenait de citoyens français. Le COC a fait de même. Pourquoi cette demande ne concerne-t-elle pas tous les citoyens de l'Union européenne? Une demande en ce sens ne devrait-elle pas émaner de l'*European Data Protection Board*?

Cette affaire démontre que *Big Brother* n'est plus une fiction mais est devenu une réalité.

Il convient d'être prudent sur les dérives que peuvent amener les nouvelles technologies. Le groupe PS a soutenu au niveau européen un moratoire sur les nouvelles technologies.

Si certains souhaitent un cadre légal pour encadrer l'usage de ces technologies, il convient d'en discuter au Parlement.

M. Rigot soutient la proposition de résolution déposée par Ecolo-Groen (DOC 55 1349/001) qui vise à instaurer 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.

Mme Caroline Taquin (MR) considère que le constat émis dans le rapport est clair et interpellant, à savoir que: "Le transfert d'informations et de données à caractère personnel policières à une entreprise privée, et a fortiori à une entreprise établie en dehors de l'Union européenne, n'est pas prévu par la LFP et constitue par conséquent un traitement de données illicite et illégitime. Ce constat n'est pas contesté par la police fédérale".

formeel dan wel informeel werd gebruikt, bij wijze van test of in het raam van een onderzoek. Het onderzoek brengt aan het licht dat de Belgische politiediensten met een flagrant communicatieprobleem kampen. De commandostructuur heeft gefaald. De hiërarchie werd wel op de hoogte gebracht, maar ze heeft niet tijdig ingegrepen. Gezien de vele onwettigheden verbaast het de spreker dat het gebruik van *Clearview* niet eerder kon worden stopgezet.

Volgens de heer Rigot is wat technologisch mogelijk is, daarom nog niet toegestaan. De politieagenten zouden daarvan bewust moeten worden gemaakt: zij moeten de wet handhaven maar zij moeten ook zelf de wet in acht nemen.

Werd wie op die foto's staat daarvan op de hoogte gebracht? Zo zouden zij in de mogelijkheid worden gesteld hun rechten te doen gelden.

De CNIL heeft *Clearview* bevolen alle foto's van Franse staatsburgers waarover het beschikt te wissen. Het COC heeft hetzelfde gedaan. Waarom werd dit verzoek niet voor alle EU-burgers gedaan? Zou een dergelijk verzoek niet van de *European Data Protection Board* moeten uitgaan?

Uit deze zaak blijkt dat *Big Brother* geen fictie meer is, maar werkelijkheid is geworden.

Men moet waakzaam zijn voor de uitwassen waartoe nieuwe technologieën aanleiding kunnen geven. Op het Europese niveau heeft de PS-fractie een moratorium op nieuwe technologieën ondersteund.

Het Parlement is een ideaal forum waarbinnen een wettelijk kader voor het gebruik van die technologieën desgewenst kan worden besproken.

De heer Rigot ondersteunt het door Ecolo-Groen ingediende voorstel van resolutie over een driejarig moratorium op het gebruik van gezichtsherkenningssoftware en -algoritmen in vaste of mobiele beveiligingscamera's in openbare en privéplaatsen (DOC 55 1349/001).

Mevrouw Caroline Taquin (MR) vindt dat de in het rapport geformuleerde vaststelling duidelijk en zorgwekkend is, zoals blijkt uit het volgende tekstfragment: "De doorgifte van politionele informatie en persoonsgegevens (…) naar een privaat bedrijf, laat staan een onderneming buiten de Europese Unie, is niet geregeld in de WPA, bijgevolg onwettig en een onrechtmatige gegevensverwerking. Deze vaststelling wordt evenmin in het raam van de tegenspraak door de federale politie betwist.".

Pour le groupe MR, le respect des règles relatives à la protection des données à caractère personnel est absolument fondamental. La priorité doit être de tout mettre en œuvre pour que des agissements de ce type n'arrivent plus à l'avenir.

À cet égard, le rapport apporte des pistes intéressantes.

L'intervenante retient les trois recommandations formulées par l'Organe de contrôle de l'information policière:

— tout d'abord, miser sur l'organisation de formations et sur la sensibilisation des membres du personnel;

— ensuite, réglementer dans la LPD ou dans la LFP le traitement d'informations et de données à caractère personnel policières à des fins de test et mettre en place pour ce traitement un cadre juridique clair;

Et enfin, tenir compte de certains aspects lors de la réglementation de l'utilisation de la technologie de reconnaissance faciale dans la LPD ou la LFP, et notamment:

— les circonstances particulières dans lesquelles la reconnaissance faciale peut être utilisée;

— l'intervention soit de l'Organe de contrôle soit du magistrat compétent, en motivant et en contrôlant la nécessité, la proportionnalité et la durée de l'utilisation;

— le délai de conservation du traitement des données biométriques distinctes, à savoir le code unique et les données biométriques brutes;

— l'homologation du processus de traitement technique;

— le contrôle périodique de la fiabilité du processus de traitement technique;

— et la transparence du processus de traitement.

En ce qui concerne les mesures correctrices, l'intervenante constate que la première mesure ordonne à la police fédérale de prendre l'initiative de sommer l'entreprise *Clearview* de supprimer de sa banque de données les photos transmises par la DJSOC et de supprimer le traitement biométrique auprès de *Clearview*.

Le délai est clair. La preuve du respect de cette mesure correctrice doit être fournie à l'Organe de contrôle dans les deux mois à compter de la prise de connaissance de cette mesure. Le rapport date de début février, nous

Voor de MR-fractie is de naleving van de regels met betrekking tot de bescherming van de persoonsgegevens een absoluut basisprincipe. Alles moet nu prioritair in het werk worden gesteld opdat dergelijke handelwijzen in de toekomst uitgesloten zijn.

Wat dat betreft, reikt het rapport interessante denksporen aan.

De spreekster onthoudt de drie aanbevelingen van het Controleorgaan op de politionele informatie:

— inzetten op opleiding en sensibilisering van de personeelsleden;

— via de WGB of de WPA de verwerking regelen van politionele informatie en persoonsgegevens met het oog op tests, en er een helder juridisch kader voor creëren;

wanneer het gebruik van gezichtsherkenningstechnologie in de WGB/WPA zou worden vastgelegd, rekening houden met bepaalde aspecten, in het bijzonder:

— de specifieke omstandigheden waarin gezichtsherkenning kan worden gebruikt;

— het optreden van ofwel het Controleorgaan, ofwel de bevoegde magistraat, waarbij de noodzaak, de proportionaliteit en de duur van het gebruik worden gemotiveerd en gecontroleerd;

— de bewaartermijn van de verwerking van de onderscheiden biometrische gegevens, met name de unieke code en de ruwe biometrische gegevens;

— de homologatie van het technisch verwerkingsproces;

— de periodieke controle op de betrouwbaarheid van het technisch verwerkingsproces;

— en de transparantie van het verwerkingsproces.

Wat de corrigerende maatregelen betreft, stelt de spreekster vast dat de eerste maatregel erin bestaat dat de federale politie wordt gelast het initiatief te nemen om *Clearview* ertoe aan te zetten de door de DJSOC verstrekte foto's uit haar gegevensbank te verwijderen en de biometrische verwerking ervan bij *Clearview* te verwijderen.

De deadline hiervoor is duidelijk vastgelegd. Binnen twee maanden na de datum van kennisname van die corrigerende maatregel, moet het bewijs van de naleving ervan aan het Controleorgaan worden bezorgd. Het

sommes début mars. Sauf erreur, il reste donc en théorie un mois à la police fédérale pour appliquer cette mesure correctrice. La presse indique qu'une demande a été transmise par la Police à l'entreprise *Clearview*. Est-il possible d'avoir plus d'informations à ce sujet? La police a-t-elle déjà reçu un retour de l'entreprise *Clearview AI*?

M. Franky Demon (CD&V) rappelle que la réponse de la ministre de l'Intérieur, des Réformes institutionnelles et du Renouveau démocratique au cours de la réunion de la commission du 6 octobre 2021 (CRIV 55 COM 597) laissait déjà clairement entendre que la police fédérale avait utilisé, dans le cadre de la *taskforce* d'identification des victimes d'Europol, une licence de test de *Clearview AI* qui avait une durée de validité limitée. La ministre déclarait à l'époque que le cadre légal belge actuel n'autorisait pas l'utilisation de ce logiciel et que la police fédérale ne continuerait pas à l'utiliser.

L'intervenant a appris dans le rapport que le 7 novembre 2019, la direction de la DJSOC était déjà au courant de l'utilisation de la technologie de reconnaissance faciale. Le Commissaire général de la police fédérale a toutefois démenti cette information en février 2020, dans sa réponse aux questions posées à ce sujet par le COC. Dans son rapport, l'organe critique le manque de circulation de l'information au sein de la hiérarchie de la police fédérale et l'intervenant s'en inquiète également. Bien que le Commissaire général de la police fédérale parle d'un concours de circonstances, l'intervenant estime qu'il y aurait lieu d'approfondir cette question, à la lumière de la transmission des informations au COC, au Parlement et au ministre.

L'intervenant aborde ensuite la question de l'utilisation de la technologie de reconnaissance faciale en soi. Il estime qu'il est important d'engager le plus de moyens possible pour lutter contre la criminalité, mais que cela doit se faire dans un cadre légal et juridique. La LFP n'offre actuellement aucune base juridique pour l'utilisation d'un logiciel de reconnaissance faciale et pour le transfert de données policières à un acteur privé comme *Clearview AI.* Il convient dès lors d'examiner si la législation doit être modifiée dans ce sens. C'est une bonne chose que dans son rapport, le COC formule des recommandations et souligne des points d'attention.

En plus d'un cadre juridique, il faudra également prévoir des formations et des moyens d'information pour le personnel de police. L'intervenant s'étonne en effet, tout comme le COC, que les services de police concernés n'aient pas suffisamment compris quelle était la portée de l'application *Clearview AI*. Dans ce contexte,

rapport dateert van begin februari en we zijn nu begin maart. Als we het goed begrijpen, heeft de federale politie dus in theorie nog een maand om die corrigerende maatregel toe te passen. Volgens de pers heeft de politie een verzoek tot *Clearview* gericht. Is het mogelijk hierover meer informatie te krijgen? Heeft de politie reeds een antwoord van *Clearview AI* gekregen?

De heer Franky Demon (CD&V) wijst erop dat uit het antwoord van de minister van Binnenlandse Zaken, Institutionele Hervormingen en Democratische Vernieuwing in de commissievergadering van 6 oktober 2021 (CRIV 55 COM 597) al duidelijk bleek dat het de federale politie in het kader van de *Victim Identification Taskforce* van Europol gebruikgemaakt had van een proeflicentie van *Clearview AI*, die voor een beperkte periode geldig was. De minister stelde toen dat het huidige wettelijke kader in ons land dergelijk gebruik niet toelaat en dat de federale politie er verder geen gebruik van zou maken.

De spreker heeft uit het rapport vernomen dat de directie van DJSOC op 7 november 2019 al op de hoogte was van het gebruik van gezichtsherkenningstechnologie. Nochtans ontkende de Commissaris-generaal van de federale politie dat in februari 2020 in zijn antwoord op vragen van het COC daaromtrent. Het orgaan laakt in zijn rapport de gebrekkige informatiedoorstroming binnen de hiërarchie van de federale politie en de spreker maakt zich daar ook zorgen over. Hoewel de Commissaris-generaal van de federale politie dit een samenloop van omstandigheden noemde, is de spreker van oordeel dat men hier dieper op moet ingaan in het licht van de informatiedoorstroming naar het COC, het Parlement en de minister.

Vervolgens gaat de spreker in op het gebruik van gezichtsherkenningstechnologie zelf. Hij meent dat het belangrijk is dat er zoveel mogelijk middelen worden ingezet voor de bestrijding van criminaliteit, maar dat dit binnen een wettelijk en juridisch kader moet gebeuren. De WPA biedt momenteel geen rechtsgrond voor het gebruik van gezichtsherkenningssoftware en evenmin voor de overdracht van politionele gegevens aan een derde private actor zoals *Clearview AI*. Er moet dan ook onderzocht worden of de wetgeving in die zin aangepast moet worden. Het is een goede zaak dat het COC in zijn rapport daartoe aanbevelingen formuleert en op aandachtspunten wijst.

Naast een wettelijk kader zal er ook nood zijn aan opleidingen en informatievoorzieningen voor het politiepersoneel. De spreker is immers, net als het COC, verbaasd over het feit dat de betrokken politiediensten niet voldoende inzicht hadden in de draagwijdte van de *Clearview AI*-toepassing. In dat kader vindt de spreker

l'intervenant se félicite que la ministre de l'Intérieur, dans sa réponse au cours de la réunion de la commission du 6 octobre 2021, ait déjà déclaré que la police se dotait actuellement d'une expertise technique afin de mieux pouvoir évaluer l'utilisation de l'intelligence artificielle et plus particulièrement éviter les partis pris pour qu'à l'avenir, la technologie ne puisse être utilisée que dans le respect des droits et libertés de tout un chacun.

Enfin, l'intervenant estime que, compte tenu des divergences de points de vue sur cette question, un débat est encore nécessaire. Il se réjouit que les membres de la commission puissent compter sur l'expertise du COC dans ce domaine.

M. Tim Vandenput (Open Vld) insiste sur le fait que le rapport du COC indique clairement que la police fédérale n'aurait pas dû travailler en dehors d'un cadre légal, mais que cet incident démontre la nécessité d'un tel cadre. Dans ses deuxième et troisième recommandations, le COC déclare dès lors qu'une modification de la LFP s'impose. Le groupe de l'intervenant prépare une telle modification depuis un an et demi.

L'intervenant soutient l'idée de Mme Ingels de mettre en place des champs d'expérimentation. En effet, il est favorable à une utilisation contrôlée de la technologie de reconnaissance faciale. Cette technologie pourrait ainsi être utilisée à certains points d'entrée dans notre pays, pour vérifier si des personnes reprises dans la base de données sur les combattants terroristes de l'Organe de coordination pour l'analyse de la menace (OCAM) entrent en Belgique via ces points, ou pour mettre les personnes concernées sur une liste noire. De tels champs d'expérimentation nécessitent un cadre légal, un contrôle par le COC et une formation pour les utilisateurs.

Le groupe de l'intervenant est plutôt favorable à des champs d'expérimentation qu'à un moratoire, où la technologie est toujours utilisée, mais en dehors d'un cadre légal. L'intervenant rappelle en effet que la technologie de reconnaissance faciale est déjà largement utilisée pour accéder à certaines applications dans un smartphone. Si le smartphone en question est piraté, les données se retrouvent également chez un tiers.

M. Bert Moyaers (Vooruit) demande si le COC dispose d'une capacité et d'une expertise suffisantes pour pouvoir contrôler toutes les formes possibles de traitement de l'information policière et de nouvelles technologies.

L'intervenant constate que la police dispose déjà d'un savoir-faire en matière d'utilisation de ces technologies et demande si dans ce contexte, le COC établit une distinction entre les services de police locaux et fédéraux.

het een goede zaak dat de minister van Binnenlandse Zaken in haar antwoord in de commissievergadering van 6 oktober 2021 al aangaf dat de politie technische expertise aan het opbouwen is om het gebruik van artificiële intelligentie beter in te kunnen schatten en meer bepaald bias te vermijden, zodat de technologie in de toekomst enkel kan worden ingezet met respect voor eenieders rechten en vrijheden.

Tot slot is de spreker van oordeel dat hierover nog een debat gevoerd moet worden, gelet op de verschillende standpunten op dit stuk. Hij verheugt zich over het feit dat de commissieleden hierbij op de expertise van het COC kunnen rekenen.

De heer Tim Vandenput (Open Vld) benadrukt dat het rapport van het COC duidelijk stelt dat de federale politie niet buiten een wettelijk kader had mogen werken, maar dat dit voorval wel de noodzaak van een dergelijk kader aantoont. Het COC stelt in zijn tweede en derde aanbeveling dan ook dat een aanpassing van het WPA zich opdringt. De fractie van de spreker bereidt een dergelijke aanpassing al sinds anderhalf jaar voor.

De spreker schaart zich achter het idee van mevrouw Ingels om proeftuinen te organiseren. Hij is immers voorstander van een gecontroleerd gebruik van gezichtsherkenningstechnologie. Zo zou die technologie op bepaalde ingangspunten in ons land gebruikt kunnen worden gebruikt om na te gaan of personen uit de terroristendatabase van het Coördinatieorgaan voor de dreigingsanalyse (OCAD) via die punten België binnenkomen of om de betrokkenen te blacklisten. Dergelijke proeftuinen behoeven wel een wettelijk kader, toezicht door het COC en opleiding voor de gebruikers.

De fractie van de spreker is eerder voorstander van proeftuinen dan van een moratorium, waarbij de technologie toch nog gebruikt wordt, maar dan buiten een wettelijk kader. De spreker herinnert er immers aan dat gezichtsherkenningstechnologie al veelvuldig gebruikt wordt om op een smartphone toegang te krijgen tot bepaalde apps. Als de smartphone in kwestie gehackt wordt, komen de data ook bij een derde partij terecht.

De heer Bert Moyaers (Vooruit) vraagt of het COC over genoeg capaciteit en expertise beschikt om toezicht te kunnen verzekeren op alle mogelijke vormen van politionele informatieverwerking en nieuwe technologieën.

De spreker stelt vast dat er bij de politie al knowhow bestaat over de omgang met dergelijke technologieën en vraagt of het COC in dat kader een onderscheid vaststelt tussen lokale en federale politiediensten.

Enfin, l'intervenant souhaiterait savoir ce qu'il en est de la sensibilisation de la GPI à la protection des données depuis la création du COC en tant qu'organe de contrôle en 2018. Quels sont les plus grands défis et problèmes actuels?

M. Ortwin Depoortere (VB) signale que son groupe est favorable à l'utilisation de technologies modernes pour lutter adéquatement contre la criminalité. Il constate que sur le terrain, les gens sont également demandeurs de telles technologies. AInsi, la plupart des zones de police utilisent déjà des caméras ANPR. Mais comme cette technologie porte atteinte à la vie privée, les politiques doivent s'interroger sur la manière de trouver un équilibre à ce niveau.

Le rapport du COC montre clairement qu'il manque un cadre juridique. L'intervenant demande au COC si le gouvernement a déjà réagi à ce constat ou s'il faut attendre une initiative parlementaire. En tout état de cause, l'intervenant estime que les modalités proposées par le COC dans sa troisième recommandation constituent déjà un très bon point de départ.

Enfin, l'intervenant s'inquiète du fait que la première mesure correctrice du COC n'oblige pas *Clearview AI* à faire disparaître les images concernées. L'intervenant reconnaît que seul un mois s'est écoulé sur le délai de deux mois accordé à la police fédérale pour l'exécution de cette mesure. Néanmoins, il aimerait savoir si le COC a déjà obtenu des résultats positifs sur ce point.

B. **Réponses**

M. Frank Schuermans aborde tout d'abord la mise en œuvre des mesures correctrices. Eu égard à la capacité limitée du COC, l'organe n'informe pas de la mise en œuvre de ces mesures avant l'expiration du délai de deux mois.

La première mesure correctrice concerne une obligation de moyens envers la police fédérale. Il est possible que *Clearview AI* ne donne pas suite à la demande de la police fédérale, mais le COC ne peut pas prendre des mesures qui vont plus loin.

L'intervenant évoque ensuite les tensions qui existent entre les règles européennes strictes en matière de protection des données et l'explosion des nouvelles technologies. À cet égard, la police fédérale et son autorité de contrôle doivent évidemment procéder à une évaluation. Le COC a suggéré à plusieurs reprises de mettre en place des champs d'expérimentation et de créer

Tot slot wil de spreker weten hoe het gesteld is met het bewustzijn bij de GPI over gegevensbescherming sinds de oprichting van het COC als toezichthouder in 2018. Wat zijn de grootste actuele uitdagingen en problemen?

De heer Ortwin Depoortere (VB) stipt aan dat zijn fractie voorstander is van moderne technologieën om misdaad adequaat te bestrijden. Hij stelt vast dat de mensen in het veld zelf ook vragende partij zijn om dergelijke technologieën in te zetten. Zo gebruiken de meeste politiezones al ANPR-camera's. Gelet op het feit dat men hierbij aan privacy inboet, moet op het politieke niveau wel de vraag gesteld worden hoe men hierin een evenwicht vindt.

Uit het rapport van het COC blijkt duidelijk dat in dit opzicht een wettelijk kader ontbreekt. De spreker vraagt het COC of op die vaststelling al een reactie kwam van de regering of dat men moet wachten op een parlementair initiatief. De spreker is hoe dan ook van oordeel dat de nadere voorwaarden die het COC daarvoor in zijn derde aanbeveling naar voren schuift, al een zeer goed uitgangspunt vormen.

Tot slot maakt de spreker zich zorgen over het feit dat de eerste corrigerende maatregel van het COC geen verplichting ten aanzien van *Clearview AI* inhoudt om de betrokken beelden te verwijderen. De spreker erkent dat er nog maar één maand verstreken is van de termijn van twee maanden die de federale politie gekregen heeft voor de uitvoering van deze maatregel. Toch wil hij graag vernemen of het COC op dit stuk al positieve resultaten heeft ontvangen.

B. **Antwoorden**

De heer Frank Schuermans gaat eerst in op de uitvoering van de corrigerende maatregelen. Gezien de beperkte capaciteit van het COC informeert het orgaan niet vóór het verstrijken van de termijn van twee maanden naar de uitvoering van die maatregelen.

De eerste corrigerende maatregel betreft een inspanningsverbintenis ten aanzien van de federale politie. De mogelijkheid bestaat dat *Clearview AI* niet ingaat op de vraag van de federale politie, maar het COC kan geen maatregelen nemen die verder strekken.

Vervolgens gaat de spreker in op het spanningsveld tussen de strikte Europese gegevensbeschermingsregels en de explosie aan nieuwe technologieën. Op dat stuk moet er zeker bij de federale politie en haar toezichthouder een afweging gemaakt worden. In dat opzicht heeft het COC al meermaals gesuggereerd om proeftuinen te organiseren en om wetgeving te creëren

une législation pour rendre les tests possibles. Selon l'intervenant, c'est la seule façon possible de procéder.

Indépendamment d'un cadre législatif, il est important de prévoir des garanties quant à la qualité des données obtenues. L'intervenant constate en effet que la technologie de reconnaissance faciale comporte une grande marge d'erreur et qu'il existe peu d'études indépendantes sur l'utilisation de cette technologie au Royaume-Uni et aux États-Unis, où cette technologie est plus fréquemment utilisée. L'intervenant ne connaît qu'une seule étude sur ce sujet. Cette étude de l'Université d'Essex était particulièrement négative.

Plus précisément, il faut déterminer ce que l'on fait des résultats opérationnels obtenus lors d'une phase de test. En effet, si l'on intervient sur la base de tels résultats, il ne s'agit plus d'une phase de test. Le COC peut jouer un rôle dans ce débat. On pourrait, par exemple, exiger l'autorisation préalable d'un organe de contrôle conformément à la directive européenne (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données (*Law Enforcement directive*).

L'intervenant aborde ensuite la question du moratoire. Comme cette proposition date déjà d'il y a deux ans, l'intervenant se demande quelle devrait être la durée d'un tel moratoire. Celui-ci pourrait toutefois s'avérer utile pour une période limitée, pour autant que des études soient menées entre-temps sur les systèmes existants, également à l'étranger. À ce jour, le COC n'a pas connaissance d'une quelconque avancée dans ce domaine. Si le Commissaire général de la GPI s'est bien déclaré intéressé par la poursuite de l'utilisation du logiciel de reconnaissance faciale, le COC n'a cependant reçu aucun projet concret dans ce sens. Du reste, l'intervenant fait observer qu'un moratoire n'empêche pas qu'entre-temps, un cadre législatif soit mis en place pour tester la technologie de reconnaissance faciale.

À la question de savoir si la police fédérale a informé les personnes concernées, l'intervenant répond par la négative. Une telle notification est impossible, puisque la police ne connaît pas l'identité des personnes qui figurent sur les images.

En ce qui concerne l'action européenne, il est important de savoir que le Comité européen de la protection des données (CEPD) n'a aucune compétence dans de

teneinde tests mogelijk te maken. Volgens de spreker is dat de enige mogelijke werkwijze.

Nog los van een wetgevend kader is het zaak om garanties in te bouwen over de kwaliteit van de verkregen gegevens. De spreker stelt immers vast dat er een grote foutenmarge bestaat bij gezichtsherkenningstechnologie en dat er weinig onafhankelijke studies bestaan over het gebruik van de technologie in het Verenigd Koninkrijk en de Verenigde Staten, waar die technologie vaker ingezet wordt. De spreker is bekend met slechts één studie op dit stuk. Die studie van de universiteit van Essex was uiterst negatief.

Meer specifiek moet er worden bepaald wat er wordt gedaan met operationele resultaten die tijdens een testfase worden verkregen. Indien men op basis van een dergelijk resultaat optreedt, gaat het immers niet langer over een testfase. Het COC kan een rol spelen in het debat hierover. Het is bijvoorbeeld mogelijk om een voorafgaande machtiging door een toezichthouder te verplichten op grond van de Europese Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens (*Law Enforcement directive*).

Vervolgens stipt de spreker het moratorium aan. Aangezien het voorstel daartoe al van twee jaar geleden dateert, vraagt de spreker zich af wat de termijn van een dergelijk moratorium zou moeten zijn. Voor een beperkte periode zou het evenwel zijn nut kunnen bewijzen, op voorwaarde dat men intussen studies uitvoert naar bestaande systemen, ook in het buitenland. Tot op heden is het COC niet op de hoogte van enige vooruitgang op dat vlak. Zo gaf de Commissaris-generaal van de GPI wel aan interesse te hebben in een voortzetting van het gebruik van gezichtsherkenningssoftware, maar heeft het COC daarover geen concrete plannen over ontvangen. Overigens merkt de spreker op dat een moratorium niet belet dat men intussen aan een wetgevend kader werkt voor het testen van gezichtsherkenningstechnologie.

Met betrekking tot de vraag of de federale politie de betrokkenen op de hoogte heeft gebracht, antwoordt de spreker ontkennend. Een dergelijke kennisgeving is onmogelijk, aangezien de politie de identiteit van de personen op de beelden niet kent.

Wat een Europese actie betreft, is het belangrijk om te beseffen dat het Europees Comité voor gegevensbescherming (*European Data Protection Board*

domaine. Il appartient aux 27 autorités de protection des données des États membres de prendre cette décision. En France, la Commission nationale de l'informatique et des libertés (CNIL) a déjà pris des mesures correctrices à l'égard de *Clearview AI*. En Belgique, c'est l'APD qui doit prendre une telle décision.

L'intervenant revient ensuite sur Europol, qui est un fervent partisan de la technologie de reconnaissance faciale et qui prépare effectivement ses propres fichier et application. Le COC ne sait toutefois pas où en est cette initiative. Le contrôle d'Europol relève en effet de la responsabilité du Contrôleur européen de la protection des données (CEPD).

En ce qui concerne la capacité et l'expertise du COC, l'intervenant souligne que le COC dispose d'un effectif limité à neuf collaborateurs, dont trois membres du comité de direction, trois membres du service d'enquête, deux juristes et un responsable informatique. Depuis sa création en 2018, l'organe n'a pas demandé de moyens supplémentaires, mais a toujours accru son efficacité grâce à la polyvalence de son personnel. L'organe se verra toutefois confier une nouvelle mission dans le cadre de la rétention des données par les opérateurs télécoms. Il devra alors valider les statistiques servant de base pour la rétention des données. L'organe ne dispose toutefois pas de statisticiens. Si l'on devait opter pour une autorisation préalable pour l'utilisation de la technologie de reconnaissance faciale, cela nécessiterait également l'engagement de collaborateurs supplémentaires. Enfin, le COC ne dispose pas non plus de capacités suffisantes dans le domaine informatique pour créer et partager une expertise qui pourrait, par exemple, apporter un soutien aux zones de police. Le responsable informatique doit en effet s'occuper dans une large mesure de la sécurité du COC, qui a un rôle d'exemple à jouer en cette matière.

Le COC doute que la police soit prête pour l'utilisation des nouvelles technologies. Certains corps de police sont plus avancés que d'autres sur ce point, mais le COC constate que la législation actuelle sur le traitement des informations policières n'est souvent pas respectée. Ainsi, des caméras sont souvent mises en service sans l'accord préalable du conseil communal. La Direction de l'information policière et des moyens ICT (DRI) de la police fédérale n'est pas en mesure d'offrir un soutien suffisamment rapide et efficace, de sorte que certaines zones sont amenées à expérimenter elles-mêmes. L'intervenant déplore le manque d'expertise technique

– *EDPB*) geen bevoegdheden op dat stuk heeft. Het is aan de 27 gegevensbeschermingsautoriteiten van de lidstaten om die beslissing te nemen. De Franse nationale commissie voor informatica en vrijheden (*Commission Nationale de l'Informatique et des Libertés – CNIL*) heeft al corrigerende maatregelen genomen ten aanzien van *Clearview AI*. In België komt een dergelijke beslissing toe aan de GBA.

Vervolgens komt de spreker terug op Europol, dat een *believer* is van gezichtsherkenningstechnologie en inderdaad aan een eigen bestand en toepassing werkt. Het COC heeft evenwel geen zicht op de stand van zaken van dat initiatief. Het toezicht op Europol behoort immers tot de bevoegdheden van de Europese Toezichthouder voor gegevensbescherming (*European Data Protection Supervisor – EDPS*).

Wat de capaciteit en de expertise van het COC betreft, benadrukt de spreker dat het COC een beperkt personeelsbestand van negen medewerkers heeft, onder wie drie leden van het directiecomité, drie leden van de dienst Onderzoeken, twee juristen en één IT-verantwoordelijke. Sinds de oprichting van het orgaan in 2018 heeft het geen extra middelen gevraagd, maar heeft het steeds zijn efficiëntie verhoogd dankzij de polyvalentie van zijn personeelsleden. Het orgaan zal evenwel een nieuwe opdracht krijgen in het kader van de dataretentie door telecomoperatoren, waarbij het de statistieken zal moeten valideren die de basis voor de dataretentie. Het orgaan telt echter geen statistici. Indien men zou opteren voor een voorafgaande machtiging voor het gebruik van gezichtsherkenningstechnologie zou ook daar extra mankracht voor nodig zijn. Tot slot beschikt het COC op IT-vlak evenmin over voldoende capaciteit om expertise te creëren en te delen teneinde bijvoorbeeld ondersteuning te bieden aan politiezones. De IT-verantwoordelijke moet zich immers voor een groot deel bezighouden met de beveiliging van het COC, dat ter zake een voorbeeldrol te vervullen heeft.

Het COC twijfelt of de politie klaar is voor nieuwe technologieën. Sommige politiekorpsen staan daarin verder dan andere, maar het COC stelt vast dat de huidige wetgeving inzake politionele informatieverwerking vaak niet nageleefd wordt. Zo worden camera's vaak in gebruik genomen zonder voorafgaande goedkeuring van de gemeenteraad. De Directie van de politionele informatie en ICT-middelen (DRI) bij de federale politie kan niet genoeg snelle en efficiënte ondersteuning bieden, waardoor bepaalde zones zelf aan het experimenteren zijn geslagen. De spreker noemt het gebrek aan technische expertise op het vlak van informatiehuishouding

dans le domaine de la gestion de l'information, notamment chez les chefs de corps, pour qui la gestion de l'information devrait pourtant relever de leurs activités principales.

En ce qui concerne la sensibilisation à la protection des données, beaucoup de choses dépendent également du chef de corps et du délégué à la protection des données (*data protection officer* ou *DPO*) qu'il désigne. L'intervenant regrette, par exemple, que l'arrondissement judiciaire du Limbourg ne compte qu'un seul DPO, qui est responsable de toutes les zones de police. Dans d'autres cas, le DPO s'avère être un "pigeon" qui ne connaît pas ses dossiers. Le COC peut toutefois faire pression en imposant des mesures correctrices pour obliger les zones de police à apporter des améliorations, comme l'élaboration d'un plan de sécurité de l'information. C'est ce que le COC a fait il y a deux ans dans la zone de police de Sint-Niklaas, qui est devenue une zone modèle sur le plan de la sécurité de l'information. Au niveau de la police fédérale également, l'intervenant constate que l'on n'accorde pas suffisamment d'attention à la protection des données et à la sécurité de l'information, pas même dans la formation des commissaires divisionnaires.

Il y a donc une résistance qui, selon l'intervenant, est liée à la volonté de la police de pouvoir traiter un maximum d'informations. À cet égard, il constate, par exemple, que certains fonctionnaires de police cherchent des moyens pour contourner l'archivage automatique de la Banque de données nationale générale (BNG), qui entrera bientôt en vigueur.

M. Ronny Saelens revient sur la base légale du traitement des données biométriques. Depuis 2016, une législation existe sur le sujet au niveau européen, mais ces dispositions n'ont pas été transposées en droit belge de manière satisfaisante. En ce qui concerne les données biométriques, la LFP mentionne uniquement les empreintes digitales, sans en préciser le traitement. Cela diffère du traitement de la reconnaissance faciale, qui inclut les émotions et les caractéristiques comportementales et peut être utilisé pour différentes finalités. Pour l'intervenant, il est nécessaire que cette loi aborde le traitement de toutes les sortes de données biométriques.

M. Saelens insiste sur le fait que le législateur devrait réfléchir à la manière dont la technologie de reconnaissance faciale pourrait être utilisée. Pourrait-elle être ciblée ou non ciblée? La fiabilité du logiciel utilisé et les valeurs seuils appliquées doivent également être prises en compte. Se pose en outre la question de savoir si et pendant combien de temps les données biométriques

schrijnend, met name bij de korpschefs, voor wie het toch tot hun kernactiviteiten zou moeten behoren.

Ook het bewustzijn over gegevensbescherming hangt sterk af van de korpschef en de functionaris voor gegevensbescherming (*Data Protection Officer* of DPO) die hij aanstelt. Zo betreurt de spreker dat het gerechtelijk arrondissement Limburg maar één DPO telt, die voor alle politiezones instaat. In andere gevallen blijkt de DPO een Chinese vrijwilliger die niet op de hoogte is van zijn dossiers. Het COC kan wel druk uitoefenen met corrigerende maatregelen om politiezones ertoe te verplichten verbeteringen aan te brengen zoals het opstellen van een informatieveiligheidsplan. Dat deed het COC twee jaar geleden in de politiezone Sint-Niklaas, dat intussen een modelzone is geworden op het stuk van informatieveiligheid. Ook bij de federale politie merkt de spreker dat er niet genoeg aandacht is voor gegevensbescherming en informatieveiligheid, zelfs niet in de opleiding tot hoofdcommissaris.

Er is dus een weerstand die volgens de spreker gelinkt is aan de politionele drang om zoveel mogelijk informatie te kunnen verwerken. Op dat vlak stelt hij bijvoorbeeld vast dat bepaalde politieambtenaren manieren zoeken om de automatische archivering van de Algemene Nationale Gegevensbank (ANG), die binnenkort in werking zal treden, te omzeilen.

De heer Ronny Saelens komt terug op de wettelijke basis voor de verwerking van biometrische gegevens. De wetgeving daarrond bestaat op Europees vlak al sinds 2016, maar die bepalingen werden niet voldoende in de Belgische wetgeving omgezet. In de WPA worden wat biometrische gegevens betreft enkel vingerafdrukken vermeld, zonder dat de verwerking ervan gespecificeerd wordt. Deze verschilt van de verwerking van gezichtsherkenning, waaronder ook emoties en gedragskenmerken vallen, en die voor onderscheiden finaliteiten kan worden toegepast. Voor de spreker is het noodzakelijk dat de verwerking van alle soorten biometrische gegevens in die wet behandeld wordt.

De heer Saelens benadrukt dat de wetgever zou moeten nadenken over de manier waarop gezichtsherkenningstechnologie gebruikt zou mogen worden. Zou dat gericht of ongericht zijn? Daarbij moet ook gekeken worden naar de betrouwbaarheid van de gebruikte software en de gehanteerde drempelwaardes. Bovendien rijst ook de vraag of en hoelang biometrische gegevens

d'une surveillance non ciblée par caméra peuvent être conservées.

Il convient en outre de réfléchir à l'utilisation des données publiques. Le rapport indique que les policiers concernés estimaient que sur les plateformes publiques, les informations sont communiquées par l'utilisateur. L'intervenant souligne toutefois que ce n'est pas toujours le cas, par exemple dans le cadre de la consultation d'un registre de condoléances numérique. Bien que le registre soit public, il a un but précis, à savoir exprimer sa sympathie et son respect à la famille du défunt. Dans un tel cas, la famille doit-elle vraiment s'attendre à ce que la reconnaissance faciale puisse être appliquée à la photographie du défunt simplement parce que le registre est public? Il s'agit dans ce cas de trouver un équilibre entre le respect de la vie privée et le travail de la police, et cet équilibre exige des garanties pouvant être contrôlées. La résolution pour la mise en place d'un moratoire vise à explorer cette piste.

La rapporteure, *Le président,*

Julie CHANSON Ortwin DEPOORTERE

van ongerichte camerabewaking bijgehouden mogen worden.

Daarnaast moet men nadenken over het gebruik van openbare gegevens. In het rapport wordt aangegeven dat de betrokken politieagenten van mening waren dat informatie op openbare platformen vrijgegeven wordt door de gebruiker. De spreker wijst erop dat dat echter niet altijd het geval is, bijvoorbeeld in het kader van de raadpleging van een digitaal rouwregister. Hoewel het register openbaar is, heeft deze een specifieke finaliteit, met name het betuigen van het medeleven en respect aan de familie van de overledene. Moet de familie in dat geval werkelijk in redelijkheid verwachten dat gezichtsherkenning op de foto van de overledene kan worden toegepast louter vanwege het gegeven dat het register openbaar is? Het gaat hier over een evenwicht tussen privacy en politiewerk, waarbij er waarborgen nodig zijn die gecontroleerd kunnen worden. De resolutie voor een moratorium strekt ertoe dat te onderzoeken.

De rapportrice, *De voorzitter,*

Julie CHANSON Ortwin DEPOORTERE

Imprimerie centrale – Centrale drukkerij