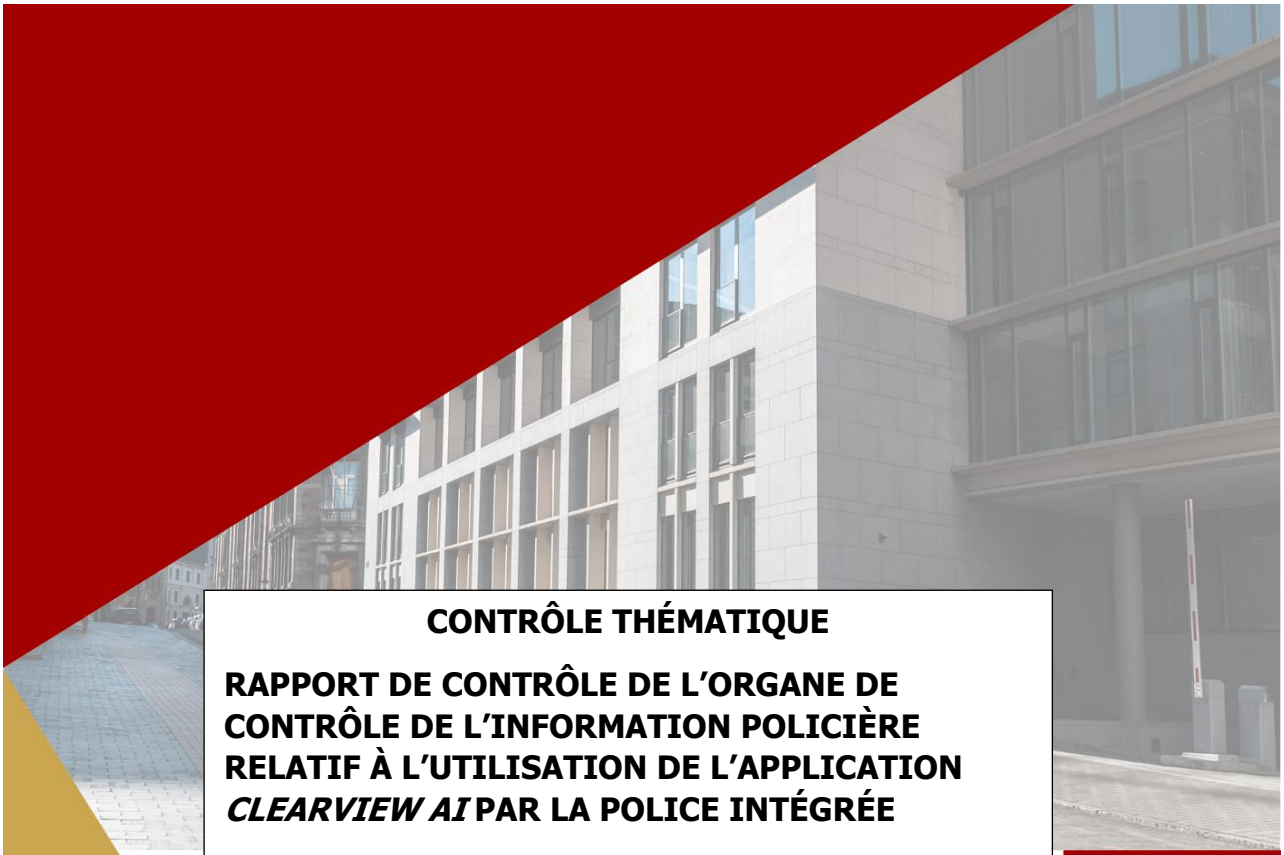


CONTRÔLE THÉMATIQUE

RAPPORT DE CONTRÔLE DE L'ORGANE DE CONTRÔLE DE L'INFORMATION POLICIÈRE RELATIF À L'UTILISATION DE L'APPLICATION *CLEARVIEW AI* PAR LA POLICE INTÉGRÉE

Référence : DIO21006

RAPPORT

RAPPORT

TABLE DES MATIÈRES

Les compétences de l'Organe de contrôle de l'information policière

La loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel (LPD)[1] a réformé l'Organe de contrôle de l'information policière ('Organe de contrôle' ou 'COC') en notamment une autorité de surveillance à part entière en plus des compétences de contrôle en matière de gestion de l'information policière prévues par la loi du 5 août 1992 sur la fonction de police (LFP). L'article 71 §1er et les Titres II et VII de la LPD décrivent les missions et les compétences du COC. Il est dans ce contexte fait référence par ailleurs aux missions de contrôle visées aux articles 44/1 à 44/11/14 inclus de la LFP, relatifs à la gestion de l'information par les services de police. L'Organe de contrôle est ainsi investi d'une mission de surveillance et de contrôle, ce qui signifie qu'en marge de la protection de la vie privée et des données, le COC prête également attention à des éléments comme l'efficacité de la gestion de l'information et de l'intervention policière. Sur la base de la réglementation susmentionnée, le COC dispose donc d'une compétence de surveillance générale à l'égard de tous les traitements opérationnels et non opérationnels de données (à caractère personnel) effectués par la GPI[2].

[1] M.B. 5 septembre 2018. Elle contient également des dispositions d'application du Règlement (UE) n° 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données et abrogeant la directive 95/46/CE (règlement général sur la protection des données), ci-après 'le RGPD', et de la Directive (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 aux fins de l'exécution de sanctions pénales, et de libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil (ci-après la 'directive Police-Justice' ou *LED* (***L**aw **E**nforcement **D**irective*)).

[2] Le COC fait la distinction entre plusieurs formes de contrôle ou de supervision :

- **Contrôle global** : il s'agit d'une enquête de surveillance qui s'accompagne d'une ou plusieurs visite(s) approfondie(s) sur le terrain ou de visites où la portée de la surveillance est très large.
- **Contrôle thématique** : comme son nom l'indique, une enquête est menée sur un thème spécifique, ce qui permet à la fois une recherche documentaire et/ou des visites sur place.

L'Organe de contrôle est compétent pour les services de police[3], pour l'inspection générale de la police fédérale et de la police locale (AIG)[4] et pour l'unité d'information des passagers (BEL-PIU)[5]. La compétence de surveillance de l'Organe de contrôle à l'égard des services de police couvre comme nous le disions à la fois les activités de traitement opérationnelles et non opérationnelles[6].

Pour ce qui est de la mission de contrôle, l'Organe de contrôle est chargé du contrôle du traitement des informations et des données visées à l'article 44/1 de la LFP, y compris celles introduites dans les banques de données visées à l'article 44/2, ainsi que de toute autre mission qui lui est confiée par ou en vertu d'autres lois.

Dans ce cadre, le COC procède à des constatations et peut avoir recours à des demandes, des recommandations, des avertissements et/ou des mesures correctrices (des injonctions contraignantes) comme «*ultimum remedium* » si le COC constate des infractions à la réglementation applicable.

L'Organe de contrôle est en particulier chargé du contrôle du respect des règles relatives à l'accès direct à la Banque de données nationale générale (BNG) et à sa consultation directe, ainsi que du respect de l'obligation visée à l'article 44/7, 3e alinéa de la LFP, qui oblige tous les membres des services de police à alimenter cette banque de données.

À travers un contrôle du fonctionnement, l'Organe de contrôle vérifie si le contenu de la BNG et la procédure de traitement des données et informations qui y sont conservées sont conformes aux dispositions des articles 44/1 à 44/11/14 de la LFP et à leurs mesures d'exécution.

Dans le cadre de l'utilisation de caméras non visibles, l'Organe de contrôle fonctionne en quelque sorte comme une commission « MAP »[7]. Conformément à l'article 46/6 de la LFP, toute autorisation et prolongation d'utilisation non visible de caméras dans les cas visés à l'article 46/4 doit être notifiée à l'Organe de contrôle sauf lorsque l'utilisation des caméras est réalisée sous le contrôle d'un magistrat. L'Organe de contrôle doit alors examiner si les conditions pour la décision, la prolongation ou l'exécution de cette mesure sont remplies. L'Organe de contrôle prend en outre connaissance des plaintes et statue sur leur bien-fondé[8].

Les membres et les membres du personnel de l'Organe de contrôle et notamment de son service d'enquête (DOSE)[9] disposent à cet égard de compétences d'investigation sur la base desquelles l'Organe de contrôle, et plus spécifiquement son comité de direction (DIRCOM) peut prendre des mesures correctrices[10].

Un recours juridictionnel peut être introduit dans les trente jours contre certaines décisions de l'Organe de contrôle devant la Cour d'appel du domicile ou du siège du demandeur qui traite l'affaire selon les formes du référé conformément aux articles 1038, 1040 et 1041 du Code judiciaire[11].

1. OBJET DU CONTRÔLE

- **Contrôle technique** : ces contrôles se limitent principalement à vérifier la légalité, l'exhaustivité et l'exactitude des saisies et des traitements dans les banques de données policières.
- **Contrôle restreint** : ces contrôles portent sur un ou seulement quelques (sous-)aspect(s) d'un traitement de données policières ou non policières.
- **Contrôle international** : il s'agit des éventuelles enquêtes internationales auxquelles le COC collabore.
- **Contrôle particulier** : il s'agit d'enquêtes et de contrôles dans des domaines particuliers, tels que les contrôles annuels des banques de données communes sur le terrorisme et l'extrémisme.

[3] Tels que définis à l'article 2, 2° de la loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux (la 'loi sur la police intégrée') et à l'article 26, 7°, a de la LPD.
[4] Telle que définie à l'article 2 de la loi du 15 mai 2007 sur l'Inspection générale et portant des dispositions diverses relatives au statut de certains membres des services de police et à l'article 27, 7°, d de la LPD.
[5] Telle que visée au chapitre 7 de la loi du 25 décembre 2016 relative au traitement des données des passagers et à l'article 26, 7°, f de la LPD. BEL-PIU est l'acronyme de la dénomination anglaise '*Belgian Passenger Information Unit*'.
[6] Art. 4 §2, quatrième alinéa de la loi du 3 décembre 2017 portant création de l'Autorité de protection des données (LAPD).
[7] MAP signifie « méthodes administratives particulières ».
[8] Art. 240, 4° de la LPD.
[9] **D**ienst **O**nderzoeken / **S**ervice d'**E**nquête.
[10] Art. 244 et 247 de la LPD.
[11] Art. 248 de la LPD.

RAPPORT

1. Le contrôle a trait au recours potentiel à l'application de reconnaissance faciale *Clearview AI*[12] par la police intégrée (GPI[13]). *Clearview AI* est une application commerciale qui doit son nom à l'entreprise américaine qui l'a développée, et qui permet au client de comparer au moyen d'un logiciel de reconnaissance faciale des photos avec des photos conservées dans la banque de données de *Clearview*. L'entreprise *Clearview* a été mise en cause en Belgique en février 2020 pour sa pratique consistant à récupérer massivement des photos de sources numériques accessibles au public, comme les réseaux sociaux, pour les mettre à des fins commerciales à la disposition des autorités répressives[14]. Selon les médias, les services de police belges recourraient également ou auraient également recouru à l'application *Clearview*. Le 25 août 2021, le site d'information en ligne *Buzzfeed* indiquait que la police fédérale aurait réalisé entre 100 et 500 recherches au moyen de l'application *Clearwiew*[15]. L'Organe de contrôle constate que la police fédérale n'a pas souhaité réagir à cette dépêche.

2. ANTÉCÉDENTS

2. Après le premier communiqué de presse du 28 février 2020, l'Organe de contrôle a adressé en date du **2 mars 2020** un courrier au nouveau 'Comité stratégique Information et ICT'[16] de la GPI pour l'informer que l'Organe de contrôle avait été consulté au sujet de l'utilisation de l'application *Clearview* par la GPI. L'Organe de contrôle posait dans ce courrier la question suivante :
« La GPI belge ou l'une de ses composantes (la police fédérale ou une police locale) utilise-t-elle ou expérimente-t-elle actuellement avec la technologie de reconnaissance faciale (FRT) ? Dans l'affirmative, pourrait-on indiquer au COC dans quelle entité c'est le cas ? Je vous saurais gré de bien vouloir soumettre cette question aux services de police et de formuler une réponse à l'intention du COC. »

3. Le **19 mai 2020**, le COC a reçu du Comité stratégique Information et ICT la réponse suivante, manifestement transmise à ce Comité par la police fédérale et la Commission Permanente de la Police Locale : ***« Sur la base des informations disponibles actuellement, 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***[17]***.*** *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 pour pouvoir recourir à cette technologie. »*. Compte tenu de ce message, l'Organe de contrôle a donc conclu que les services de police belges n'utilisaient pas la technologie de reconnaissance faciale *Clearview*. Pour cette raison, l'Organe de contrôle a toujours formellement répondu par la négative aux questions formulées par la presse à ce sujet.

Le **25 août 2021**, cependant, un nouvel article a été publié sur le site *Buzzfeednews* au sujet de la *Facial Recognition Technologie* (*FRT*) de *Clearview*. Cette fois, l'article indiquait explicitement que la police fédérale belge aurait utilisé cette technologie entre 100 et 500 fois. Il y était aussi question d'une réunion d'Europol qui se serait tenue en octobre 2019, à laquelle la Belgique aurait participé et lors de laquelle le recours à cette technologie aurait été abordé par Europol, Interpol et 21 représentants des États membres. Le porte-parole d'Europol aurait à cette occasion confirmé certains éléments. Pour toute clarté, la GPI n'avait fait aucune mention de tout ceci dans sa réponse au COC en 2020.

Pour cette raison, le COC a une nouvelle fois interrogé par courrier du **27 août 2021** le commissaire général de la police fédérale au sujet de l'utilisation prétendue de la technologie de reconnaissance faciale *Clearview* par la GPI en général ou par la police fédérale en particulier. Le COC soulignait que certains éléments semblaient ne pas correspondre à la réponse (susmentionnée) du 19 mai 2020 que le COC avait reçu de la police fédérale au nom de toute la GPI. Le COC priait donc le commissaire général d'examiner la véracité des articles parus et de faire la clarté à ce sujet pour le 27 septembre 2021.

Le **22 septembre 2021**, le COC a reçu une réponse du commissaire général formulée après une enquête interne et des renseignements pris auprès de l'entreprise *Clearview* elle-même, et faisant en détail le point sur l'utilisation ou non de la technologie de reconnaissance faciale. Il ressort de cette réponse que la réalité est tout de même bien différente du message transmis en mai 2020 par la GPI au COC, sur lequel l'Organe de contrôle s'était basé jusqu'alors. L'enquête

---

[12] *Artificial Intelligence.*
[13] L'acronyme GPI signifie **G**eïntegreerde **P**olitie – **P**olice **I**ntégrée.
[14] Service d'actualité de la VRT, 28 février 2020, https://www.vrt.be/vrtnws/nl/2020/02/28/clearview (avec une référence à la publication du 27 février 2020 du site d'information en ligne *Buzzfeed*).
[15] https://www.buzzfeednews.com/article/ryanmac/clearview-ai-international-search-table.
[16] Le 'Comité d'avis en charge de la stratégie en matière d'information et d'ICT' visé à l'article 8*sexies* de la loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux ('la LPI').
[17] Soulignement de l'Organe de contrôle.

interne a ainsi révélé que des membres de la DGJ/DJSOC[18], et plus précisément du service *Child Abuse*, prennent part deux fois par an à une taskforce opérationnelle d'Europol, la *Victim Identification Taskforce*. La taskforce s'est réunie physiquement en 2019 et sous forme virtuelle en 2020 (en présence du FBI américain). C'est dans ce cadre que des licences de test ont été mises par Europol à la disposition des participants (et donc également de deux membres de la DJSOC). Selon le commissaire général, ces membres du personnel ont à plusieurs reprises testé/utilisé l'application sur des dossiers non belges durant la taskforce d'Europol et (à leur retour en Belgique) également sur des dossiers du *NCMEC* américain (le *National Center for Missing and Exploited Children*). Ils ont également effectué des tests avec des photos d'eux-mêmes et de collègues/connaissances. Selon le courrier du 22 septembre 2021, ces tests n'ont jamais débouché sur des *« résultats opérationnels »* (opérationnels au sens de « pertinents dans le cadre d'une information »). Selon *Clearview*, il aurait au total été procédé à 78 consultations et la dernière utilisation remonterait au 10 février 2020. Le commissaire général confirmait dans ce courrier que l'application ne serait pas utilisée par la police fédérale aussi longtemps que le cadre légal ne le permet pas et que, afin d'éviter tout incident similaire à l'avenir, il serait rappelé à tous les membres du personnel qu'une utilisation d'applications ou un traitement de données à caractère personnel à des fins professionnelles n'est possible que moyennant le respect rigoureux des conditions prévues par la loi.

Dans son courrier du **1er octobre 2021**, le COC épingle quelques incohérences dans la réponse formulée en date du 22 septembre 2021 par le commissaire général, qui ont amené l'Organe de contrôle à initier une enquête d'office plus active. En effet, alors que la réponse formulée le 19 mai 2020 par le Comité stratégique Information et ICT stipulait que l'application *Clearview* n'était pas utilisée par la police (fédérale), on pouvait lire ce qui suit dans le courrier susmentionné du 22 septembre 2021 : *« À leur retour, l'un des deux participants a utilisé l'outil à quelques jours qui restaient de la licence d'essai, mais toujours sans résultat. »*, et par ailleurs *« Le Chef de service confirme donc bien que la solution n'a pas été utilisée dans des analyses par la DGJ. »*. Afin d'obtenir davantage de clarté à ce sujet, le COC a posé dans ce même courrier du 1er octobre 2021 neuf (9) questions au commissaire général (voir plus loin).
Dans ce courrier, l'Organe de contrôle soulignait également que ces informations auraient déjà dû être reprises dans l'analyse d'impact relative à la protection des données (AIPD)[19] qui aurait dû être effectuée avant de recourir à cette technologie, et que l'Organe de contrôle n'a jamais reçue.

Dans le cadre des questions parlementaires posées le **6 octobre 2021** au sujet du logiciel *Clearview* au sein de la Commission de l'Intérieur, de la Sécurité, de la Migration et des Matières administratives, le ministre de l'Intérieur a répondu que la police fédérale n'utilisait pas de manière structurelle l'outil *Clearview*, mais qu'une enquête interne avait révélé que 2 enquêteurs de la police judiciaire avait eu, lors d'une réunion de la taskforce d'identification des victimes d'Europol en octobre 2019, accès à une licence de test qui avait une durée de validité limitée. Et le ministre d'ajouter : *« Étant donné que le cadre légal belge n'autorise pas l'exploitation de ce logiciel, celui-ci ne sera pas utilisé par la police fédérale. »*[20]. Le ministre précisait également que les informations requises seraient transmises au COC.

Enfin, le commissaire général a formulé dans son courrier du **18 octobre 2021** une réponse au courrier du COC du 6 octobre 2021 dans lequel l'enquête d'office était annoncée, en transmettant au COC un dossier ayant trait à l'enquête interne menée par le commissaire général dans le sillage des courriers du 22 septembre 2021 et du 1er octobre 2021. Il ressort en outre de la réponse du commissaire général qu'au total 3 membres de la police judiciaire fédérale ont créé un compte temporaire auprès de l'entreprise *Clearview* en vue d'utiliser la technologie de reconnaissance faciale de l'entreprise.

À l'occasion d'une concertation bilatérale qui s'est tenue le 3 novembre 2021 entre l'Organe de contrôle et l'autorité de contrôle d'Europol, l'*European Data Protection Supervisor* (EDPS)[21], ce dernier a annoncé qu'il avait émis un avis dans le sillage de son enquête sur l'utilisation de l'application *Clearview* par Europol. Cet avis du 29 mars 2021 a dans l'intervalle été publié, certes moyennant l'omission de quelques éléments, et sa lecture nous apprend que les constatations effectuées par l'EDPS sont dans une large mesure parallèles à celles formulées dans le présent rapport[22].

3. MÉTHODOLOGIE

[18] La Direction centrale de la lutte contre la criminalité grave et organisée de la Direction générale de la police judiciaire.
[19] En anglais *'Data Protection Impact Assessment'* (DPIA).
[20] Doc. Parl. *Chambre*, 2020-2021, CRIV 55 COM 597, 3-4.
[21] L'EDPS est l'autorité de protection des données pour Europol ; voir aussi www.edps.europa.eu.
[22] https://edps.europa.eu/system/files/2022-01/21-03-29_edps_opinion_2020-0372.pdf.

4. L'enquête peut globalement être subdivisée en trois parties. La première partie consistait à obtenir des réponses claires aux 9 questions posées par le COC dans son courrier du 1er octobre 2021, à savoir :

Partie 1

1) une copie de l'enquête interne menée par le service de police au sujet de l'utilisation de cette technologie, qui a conduit au courrier du 22 septembre 2021 ;
2) les conventions éventuelles passées avec l'entreprise *Clearview* concernant le recours à cette technologie ;
3) la date à laquelle le recours à cette technologie a effectivement débuté ;
4) s'il a dans l'intervalle été mis un terme à l'utilisation de cette technologie, la date à laquelle cette utilisation a pris fin ;
5) tout le processus de traitement de l'utilisation de cette technologie (les modalités d'utilisation, l'enregistrement local du logiciel et/ou le traitement sur la plateforme de *Clearview*, etc.) ;
6) le nombre, la nature et les numéros de PV des dossiers dans le cadre desquels la technologie a été appliquée ;
7) une présentation (impression) d'un « résultat » de l'utilisation de la technologie (même si le résultat est négatif dans le cadre de l'information) ;
8) l'endroit où le résultat de l'application de cette technologie est conservé au sein de la police ;
9) le nombre de personnes qui sont/étaient autorisées à utiliser cette technologie, l'entité de police dont ces personnes faisaient partie et l'identité de la personne qui a donné son autorisation à cette fin ;

Partie 2

Sur la base des réponses et des constatations, deux membres de la Direction centrale de la lutte contre la criminalité grave et organisée (*DJSOC*) ont été entendus au sujet de l'utilisation effective de l'application *Clearview*.

Partie 3

Cette partie a trait à l'évaluation juridique de l'utilisation de la technologie de reconnaissance faciale *Clearview*.

Pour la bonne compréhension, nous commençons par présenter ci-après un exposé général et concis concernant l'application de la technologie de reconnaissance faciale (chapitre 4). Nous présentons ensuite les conclusions de l'enquête en expliquant d'abord le fonctionnement de l'application *Clearview* et ensuite son utilisation par la police judiciaire fédérale (chapitre 5). Nous évaluons alors l'utilisation de cette application en fonction du cadre légal actuel (chapitre 6), pour terminer ce rapport par quelques réflexions, la conclusion, et enfin les recommandations et les mesures correctrices (chapitres 7 et 8).

Le 10-01-2022, le projet de rapport a été approuvé par le Comité de direction du COC en vue de sa transmission en prélecture.
Le 10-01-2022, le projet de rapport a été transmis en prélecture au commissaire général dans le cadre du droit de réponse.
Le 28-01-2022, le COC a reçu les remarques et demandes de modifications du commissaire général au sujet du projet de rapport, les a traitées et a apporté les précisions nécessaires. Le commissaire général transmettait par la même occasion une nouvelle note temporaire du 28.01.2022 portant la référence CG/2022-16 et intitulée *« Rappel des principes en matière de traitement de données à caractère personnel »*, qui était adressée à toutes les entités de la police fédérale.

Le 4 février 2022, le rapport définitif a été approuvé par le Comité de direction du COC.

4. L'APPLICATION DE LA RECONNAISSANCE FACIALE

5. L'utilisation de la technologie de reconnaissance faciale implique également un traitement de données à caractère personnel biométriques. Ces données à caractère personnel relèvent des 'catégories particulières' de données à caractère personnel parce qu'elles comportent des aspects incontestables touchant à (l'essence de) la vie privée du fait qu'elles contiennent des caractéristiques uniques de la personne. Outre les représentations du visage, les empreintes

digitales[23] et la voix de la personne physique relèvent également de cette catégorie particulière de données à caractère personnel. La reconnaissance faciale nécessite toutefois un traitement technique complémentaire de la représentation du visage (la photo ou l'image)[24].

6. En résumé, le processus de traitement peut en l'occurrence être subdivisé en trois phases. Après l'enregistrement ou la mise à disposition de la photo ou de l'image (première phase), il est recouru à un logiciel spécialement conçu pour reconnaître les caractéristiques uniques de la personne sur la photo (l'image) (deuxième phase). Cette opération peut être considérée comme l'enregistrement – et donc le traitement – de données biométriques à travers la conversion des données 'brutes' (l'enregistrement des caractéristiques du visage) en un code chiffré unique et sa conservation sur un support (ce que l'on appelle un '*template*'). Ces données (le *template* biométrique : le code chiffré unique) permettent d'identifier la personne de manière unique parmi un groupe (in)déterminé de personnes. Bien que des données biométriques soient donc déjà traitées durant cette phase, le résultat ne pourra être effectivement atteint qu'en comparant ce *template* (traitement de données à caractère personnel) à d'autres photos ou images (troisième phase)[25]. En cas de résultat positif ('*hit*' : correspondance des caractéristiques du visage), ce résultat doit être validé ('*match*')[26]. La reconnaissance faciale proprement dite est donc la résultante d'une application technologique spécifique visant l'identification unique de la personne au moyen de la mise en relation (comparaison) d'au moins deux photos ou images.

7. Dans le contexte policier, l'utilisation de la technologie de reconnaissance faciale poursuit *grosso modo* deux objectifs génériques, à savoir l'**identification** à partir d'une recherche non ciblée ou ciblée de personnes[27].

8. Dans le cas d'une reconnaissance faciale non ciblée réalisée en public (en temps réel ou non), une quantité très importante de photos ou d'images (données à caractère personnel) est comparée à une liste de personnes recherchées ou disparues. L'application de la reconnaissance faciale fonctionne à distance (*remote*), par exemple au moyen du réseau de caméras de police installées dans des lieux publics qui est suivi et géré à partir du bâtiment de police. La reconnaissance faciale est en principe 'non ciblée' parce que les images ou photos d'un nombre indéterminé de passants (fortuits) – et donc d'un groupe non différencié de personnes – sont captées. Il s'agit par essence d'une situation 'non-suspect versus suspect/personne disparue' (N:1). La reconnaissance faciale peut être appliquée au traitement d'images dont le service de police est le responsable du traitement ou d'images auxquelles la police a accès (en temps réel ou non) auprès d'une tierce partie, comme les images des caméras des sociétés de transport en commun ou les images enregistrées lors d'un événement d'envergure (organisé par un acteur privé ou public) auxquelles la police a ou peut avoir accès pendant la durée de l'événement[28].

9. La reconnaissance faciale ciblée réalisée en public consiste à comparer les photos ou images d'un ou plusieurs suspects ou d'une ou plusieurs personnes disparues (victimes) avec des photos ou images collectées et conservées par des caméras installées dans des lieux accessibles au public. Il s'agit donc de l'opération inverse : au lieu de comparer les photos ou images d'un groupe indéterminé et non différencié de personnes avec une liste bien définie, il est procédé ici sur la base de photos ou images sélectionnées au préalable par la police à une recherche 'ciblée' (et réactive) de photos ou images correspondantes gérées par des tiers[29] ou par la police (sur une plateforme numérique). Il est donc

[23] Article 26, 13° de la LPD et considérant 51 de la *LED*. Il est en outre également question de reconnaissance du comportement de la personne (caractéristiques comportementales).
[24] Article 34 §1er de la LPD.
[25] Sur la base de la détection des caractéristiques uniques correspondantes sur les photos auxquelles la comparaison est appliquée.
[26] Voir l'article 35, 1er alinéa de la LPD. Le résultat positif ('*match*') ne peut pas découler d'une décision fondée exclusivement sur un traitement automatisé, à moins que la loi ne réglemente explicitement cette possibilité et offre les garanties requises. Dans l'état actuel de la législation (LPD), la décision doit se fonder sur une évaluation humaine.
[27] Nous faisons ici abstraction de l'« authentification », dont le processus de traitement peut être subdivisé en quatre phases du fait que les données biométriques sont traitées deux fois : la première fois lors de la collecte et une seconde fois lorsque la personne concernée s'authentifie. L'« authentification » est une vérification reposant sur une comparaison un-à-un (1:1) destinée à déterminer si l'image de la personne correspond à la personne dont les données à caractère personnel ont été enregistrées dans une banque de données (et s'y identifiant). L'identification est par contre une comparaison entre une personne et un groupe (1:N) sans que la personne ne revendique une identité déterminée (vérification). Pour dire les choses autrement, l'identification répond à la question 'Qui est cette personne ?'. La personne est individualisée de manière unique. L'authentification, en revanche, répond à la question 'Cette personne est-elle qui elle est ou prétend être ?'. Dans ce cas, la personne n'est donc pas individualisée de manière unique parmi un groupe indéterminé de personnes. Cf. WENDEHORST, Y. DULLER, *Biometric Recognition and Behavioral Detection. Assessing the ethical aspects of biometric recognition en behavioural techniques with a focus on their current and future use in public spaces*. European Union 2021, 20, http://www.europarl.europa.eu/supporting-analyses.
[28] Voir à ce sujet l'article 9, 3e alinéa, 3°, a) et b) de la loi du 21 mars 2007.
[29] Comme les gares ferroviaires et routières et d'autres lieux accessibles au public dont le service de police n'est pas le gestionnaire, comme prévu à l'article 9, 3e alinéa, 3° de la loi du 21 mars 2007 *« réglant l'installation et l'utilisation de caméras de surveillance »* et à l'article 25/1 §2 de la LFP.

alors question d'un acte d'information ou d'instruction ciblé qui consiste à comparer l'image de (plusieurs) suspects ou victimes avec des photos ou images (mises à disposition) en vue de l'identification du suspect ou de la victime (1:N)[30].

Dans les applications abordées ci-avant, chaque *hit* est validé par un fonctionnaire de police compétent (pour aboutir ou non à une *match*).

10. Il ressort de l'exposé qui suit que la présente enquête se concentre sur l'utilisation de la reconnaissance faciale ciblée en vue de l'identification (réactive) de victimes et d'auteurs. On recherche une ou des personnes spécifiques (auteurs ou victimes) parmi un nombre (in)déterminé de personnes (1:N).

5. CONCLUSIONS DE L'ENQUÊTE

5.1. L'application *Clearview*

11. Selon ses propres dires, l'entreprise *Clearview* n'est accessible que pour les *'law enforcement agencies'*, autrement dit les autorités répressives. L'entreprise présente son produit comme étant *« a revolutionary, web-based intelligence platform for law enforcement to use as a tool to help generate high-quality investigative leads. Our platform, powered by facial recognition technology, includes the largest known database of 10+ billion facial images sourced from public-only web sources, including news media, mugshot websites, public social media, and other open sources »*[31]. *Clearview* gère, optimalise et exploite donc une banque de données géante de représentations de visages (photos et images) de personnes qui sont accessibles sur Internet, sur les réseaux sociaux et sur les sites de presse en particulier, et qui sont donc accessibles au public, et met à des fins commerciales ces images à la disposition des services de police.

12. L'entreprise propose une version *trial* (période de test gratuite) pour 30 jours afin de permettre à l'utilisateur de se familiariser avec le traitement de l'application *Clearview*. Une fois cette période de test écoulée, l'utilisation de l'application *Clearview* est payante. Le site Internet de *Clearview* comporte un lien dénommé '*request trial*'. Lorsque l'utilisateur potentiel clique sur ce lien, il voit s'afficher un écran mentionnant clairement que cette application est uniquement accessible aux services de police (*'law enforcement personnel'*[32]) 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 *Clearview*. Une fois le processus d'enregistrement terminé, l'utilisateur reçoit un lien pour activer son compte *Cleaview*. Lorsque l'utilisateur s'identifie avec son compte *Clearview*, il reçoit un lien (URL[33]) qui lui permet de charger une photo. Une photo peut contenir plusieurs représentations de personnes. Dans ce dernier cas, l'application sélectionnera automatiquement chaque photo séparément pour les comparer avec la banque de données de *Clearview*. Si la comparaison aboutit à un résultat positif, l'utilisateur reçoit un lien (URL) de la source dans laquelle *Clearview* a recueilli (*'scrapted'*) les photos (un site Internet, Facebook ou autre).

Étape par étape, l'utilisation de l'application *Clearview* peut être décrite comme suit :

1) l'utilisateur charge une photo ou une image (représentant une ou plusieurs personnes) ;
2) sans aucune intervention de la part de l'utilisateur, le système recherche dans la banque de données *Clearview* des représentations correspondantes (visages) ;
3) si le système trouve une *match* et/ou un visage similaire (*'similar'*), l'utilisateur obtient le résultat de cette correspondance ;

[30] Une autre possibilité est la reconnaissance faciale interne. Dans le cadre de la reconnaissance faciale interne (privée), le système ne fonctionne pas à distance ni en temps réel. La technologie de reconnaissance faciale est ici appliquée par la police à des photos et images qui ont déjà été enregistrées dans des banques de données et qui sont comparées entre elles. Nous pensons par exemple aux images de caméras de la police qui sont enregistrées en application de l'utilisation générique des caméras et/ou aux photos enregistrées dans une banque de données opérationnelle. Il s'agit ici aussi d'un acte d'information ciblé, mais la reconnaissance faciale est appliquée à des données existantes internes à la police. Il s'agit d'une comparaison automatisée de photos et images qui ont été enregistrées dans les banques de données policières en vue d'une identification ou vérification correcte de la personne suspecte et/ou condamnée. La raison de ce choix est surtout pratique et organisationnelle : une comparaison manuelle ('hit') nécessiterait une affectation déraisonnable de main-d'œuvre et prendrait aussi beaucoup de temps. Dans ce scénario, la comparaison peut être organisée en vue de l'identification (auteur d'une autre infraction pénale) ou de la vérification (s'agit-il de la même personne ?).
[31] https://www.clearview.ai.
[32] Un concept qui est d'ailleurs dans le contexte américain plus vaste qu'au sens de la législation belge.
[33] *Uniform Resource Locator*, en l'occurrence l'adresse de la banque de données de *Clearview.*

4) en cas de *match* et de *similar*, l'utilisateur obtient également le lien vers l'endroit où la photo est disponible (par exemple sur Facebook ou Instagram, dans la presse numérique, etc.) ;
5) enfin, le lien vers l'endroit où se trouve(nt) la ou les photos peut être ouvert ; le cas échéant, cet emplacement renvoie lui-même à une ou plusieurs autres sources numériques (dans laquelle (lesquelles) d'autres photos sont éventuellement disponibles).

L'application *Clearview* est très conviviale, de sorte que son utilisation à partir de n'importe quel ordinateur ou appareil (*'device'*) ne nécessite que peu d'efforts.

Dans l'intervalle, nous savons que *Clearview* est mise en cause par plusieurs autorités de contrôle nationales[34] à travers le monde. En France, la *CNIL*[35] a par exemple ordonné le 21 décembre 2021 à *Clearview* de cesser toute activité de *scraping* sur le territoire français[36] en raison de diverses infractions au RGPD. La décision de la CNIL contient d'ailleurs une bonne description de la technique et de la technologie utilisées par *Clearview*.

5.2. L'utilisation de l'application *Clearview* par la police judiciaire fédérale

13. Il ressort de l'enquête menée par le COC que la technologie de reconnaissance faciale de *Clearview* a été utilisée par la police judiciaire fédérale, et ce pour la première fois durant la taskforce d'Europol à La Haye qui s'est tenue du 14 au 25 octobre 2019 inclus[37]. Cette taskforce était organisée dans le cadre d'un dossier coordonné à l'échelle internationale, à savoir le *National Center of Missing and Exploited Children* (NCMEC)[38]. Le NCMEC est en réalité un service répressif américain auquel participe le *Federal Bureau of Investigation* (FBI)[39]. La police judiciaire fédérale belge apporte également son concours aux dossiers du NCMEC[40]. Le NCMEC rassemble (et reçoit aussi des services Internet, dont les réseaux sociaux) des photos et images d'auteurs et victimes potentiels de violences sexuelles à l'encontre de mineurs d'âge (pédopornographie). Il s'agit en l'occurrence d'auteurs et victimes potentiels qui n'ont pas encore été localisés (identité et résidence ou espace/temps).

14. Lors de cette taskforce, les possibilités de la reconnaissance faciale de *Clearview* ont été démontrées aux services de police participants de 24 pays et appliquées à des données du NCMEC. Selon les conclusions de l'enquête, c'est dans ce contexte qu'un membre présent de la police judiciaire fédérale a utilisé pour la première fois la technologie de reconnaissance faciale, durant la taskforce en octobre 2019. Il apparaît en outre que la police judiciaire fédérale a également utilisé la technologie de reconnaissance faciale de *Clearview* après la taskforce d'Europol sur des photos et images dans le cadre d'enquêtes portant sur des abus sexuels potentiels à l'encontre de mineurs d'âge[41]. Selon *Clearview*, la dernière activité recourant à la technologie de reconnaissance faciale remonterait comme nous le disions au 10 février 2020, après quoi les comptes ont été clôturés à l'initiative de *Clearview*[42].

15. La reconnaissance faciale de *Clearview* a été utilisée pour constater l'identité (et éventuellement la résidence) d'auteurs d'abus sexuels à l'encontre de mineurs d'âge (pédopornographie) dans le cadre de dossiers du NCMEC afin de pouvoir ensuite ouvrir un dossier d'information[43]. Il ressort de l'enquête que la police judiciaire fédérale aurait effectué au total 78 recherches dans la banque de données de *Clearview*[44], et a donc effectivement utilisé la reconnaissance faciale de *Clearview*. L'utilisation de l'application *Clearview* par la police judiciaire fédérale n'aurait jamais

[34] Voir e.a. Audibert, L., « Les technologies de reconnaissance faciale menacent la notion de vie privée en ligne et hors ligne », Le Monde, 6 janvier 2022, https://journal.lemonde.fr/data/1838/reader/reader.html?xtor=EPR-32.
[35] Commission Nationale de l'Informatique et des Libertés, www.cnil.fr.
[36] www.cnil.fr, Decision n° MED 2021-134 of 1st November 2021 issuing an order to comply to the company CLEARVIEW AI (cnil.fr).
[37] Courrier du commissaire général de la police fédérale du 18 octobre 2021, confirmé par une interview avec un membre de la police judicaire fédérale.
[38] Courrier du commissaire général de la police fédérale du 18 octobre 2021, p. 1.
[39] Ibid, p. 3.
[40] Courrier du commissaire général de la police fédérale du 18 octobre 2021, p. 1.
[41] C'est ce qui ressort de la réponse de *Clearview*, qui stipule que l'application a encore été utilisée le 10 février 2020. La DGJ le confirme d'ailleurs dans son e-mail du 19 septembre 2021. Il est important dans ce contexte de garder à l'esprit que le COC n'a pas examiné la véracité des informations fournies par *Clearview* et n'est en réalité pas en mesure de le faire étant donné que cette entreprise ne relève pas de la compétence du COC.
[42] Ibid. Parce que la période d'essai était terminée.
[43] Pour toute clarté, il s'agit de la constatation de l'identité de personnes dont l'identité n'était pas encore connue de la police judiciaire fédérale. Si l'identité de ces personnes avait été connue, la reconnaissance faciale aurait plutôt été utilisée pour vérifier l'identité (pour répondre à la question 'est-ce la même personne que celle qui est connue de la police pour une telle infraction ?').
[44] E-mail de *Clearview AI* du 16 septembre 2021. L'application *Clearview* a d'abord été testée par les utilisateurs sur leurs photos personnelles et sur celles de connaissances/collègues afin de tester l'efficacité de la technologie de reconnaissance faciale.

abouti à un résultat positif dans le cadre d'une information, ni pendant la taskforce d'Europol ni lors d'enquêtes menées en Belgique après la taskforce[45]. En dépit du fait que les photos et les images ne faisaient à ce stade pas nécessairement partie d'une instruction 'belge', ces photos et images doivent bel et bien être considérées comme des données à caractère personnel policières au sens du Titre II de la LPD et de la LFP[46].

L'exposé qui précède soulève deux questions dans le cadre de l'enquête :

1) Le commissariat général de la police fédérale en général et la Direction générale de la police judiciaire (DGJ) en particulier étaient-ils au courant – ou auraient-ils raisonnablement dû l'être – de l'utilisation de la technologie de reconnaissance faciale de *Clearview* par des membres de la police (judiciaire) fédérale, à savoir la DJSOC ?
2) Le recours à la reconnaissance faciale de *Clearview* est-il (et était-il) conforme au cadre légal ? Une réponse à cette question est formulée au point 5.4.

5.3. Autorisation et connaissance du recours à la technologie de reconnaissance faciale

16. Il ressort de l'enquête et du rapport de synthèse du membre de la police judiciaire fédérale qui a pris part à la taskforce d'Europol (du 14 au 25 octobre 2019 inclus) que la Direction centrale de la lutte contre la criminalité grave et organisée (DJSOC) a été informée de l'utilisation de l'application *Clearview* immédiatement après la taskforce (verbalement), et **au moins le 7 novembre 2019** de manière formelle par écrit[47]. Cela signifie que la hiérarchie de la police judiciaire fédérale était au courant de l'utilisation de la technologie de reconnaissance faciale de *Clearview* immédiatement après la taskforce d'Europol – et donc pour des dossiers auxquels les membres de la police judiciaire fédérale travaillaient, et a également toléré cette utilisation. Ce dernier constat ressort aussi du fait que l'utilisation payante de l'application *Clearview* par la police judiciaire fédérale a par la suite été envisagée mais n'est finalement pas devenue réalité.

17. Il est dès lors frappant de constater que le commissaire général répond dans son courrier du 19 mai 2020 au COC que *« sur la base des informations disponibles actuellement, 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[48]. 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 pour pouvoir recourir à cette technologie. »*.[49]. Ce n'est que sur l'insistance du cabinet du commissaire général lors d'une seconde enquête interne (qui faisait suite à la nouvelle demande du COC du 27 août 2021, elle-même formulée en réaction à des articles parus dans la presse) – sur la base de la confirmation, par *Clearview* en date du 16 septembre 2021, de l'utilisation de la reconnaissance faciale par des membres de la police fédérale – que la Direction générale de la police judiciaire (DGJ) a formellement confirmé le 19 septembre 2021 que l'application *Clearview* était effectivement utilisée par des membres de la police judiciaire fédérale dans le cadre de (quelques) dossiers du NCMEC.

18. Il ressort donc clairement des éléments de l'enquête que la réponse adressée le 19 mai 2020 par le commissaire général à l'Organe de contrôle ne correspondait pas à la réalité étant donné que la police judiciaire fédérale était bel et bien au courant depuis au moins le 7 novembre 2019 de l'utilisation de l'application *Clearwiew* par des membres de la DJSOC, tolérait cette utilisation et a par la suite pris en toute connaissance de cause la décision de ne pas acheter de licences de l'application.

En dépit de l'utilisation illicite, d'un point de vue légal, de la technologie de reconnaissance faciale de *Clearview* (voir le point 5.4 ci-dessous) par un ou plusieurs enquêteurs individuels de la DJSOC – par ailleurs très zélés –, l'Organe de contrôle reproche surtout à (la hiérarchie de) la Direction générale de la police judiciaire de ne pas avoir fait part de l'utilisation de l'application *Clearview*, ni au COC ni manifestement au commissaire général. Il va de soi que ce constat est incompatible avec le devoir de coopération que la loi impose aux services de police se trouvant sous tutelle[50], et

[45] Courrier du commissaire général de la police fédérale du 18 octobre 2021, p. 3, confirmé par la DGJ dans son e-mail du 19 septembre 2021. Le COC n'a pas pu vérifier la véracité de cette affirmation. Comme nous le disions dans la note de bas de page précédente, la coopération de *Clearview* est à cet égard essentielle.
[46] Articles 26, 1° et 2° de la LPD et 44/1 §1er de la LFP.
[47] Rapport de synthèse de la mission à l'étranger dans le cadre de la *Victim Identification Taskforce* en charge des abus sexuels à l'encontre de mineurs d'âge (daté par l'e-mail du 7 novembre 2019 du membre de la DJSOC ayant pris part à la taskforce).
[48] Soulignement de l'Organe de contrôle.
[49] Comme indiqué plus haut dans la rubrique 2.
[50] Voir l'article 57 de la LPD : *« Le responsable du traitement et le sous-traitant coopèrent avec l'autorité de contrôle compétente, à la demande de celle-ci, dans l'exécution de ses missions. »*. Cette non-communication est d'ailleurs répréhensible au titre d'obstacle aux missions légales de vérification et de contrôle conformément à l'article 222, 7° de la LPD.

d'une manière générale néfaste pour le contrôle, qui doit pouvoir se fier à la véracité des réponses de la GPI. Dans le cadre de son droit de réponse, le commissaire général indique ne pas percevoir de la part de la DGJ une véritable volonté de dissimulation, mais plutôt un concours de circonstances qui a fait que l'échange d'informations ne s'est pas déroulé comme souhaité. Le COC en prend acte.

Vu la sensibilité de la matière et le constat (à juste titre) du commissaire général que le public et les décideurs politiques – et évidemment l'autorité de contrôle – attachent de plus en plus d'importance à la légalité et à la proportionnalité des traitements de données policiers[51], il convient de partir du principe que la prise de conscience de la part de la GPI est actuellement telle que les erreurs de communication de ce genre appartiennent désormais au passé.

Pour le reste, il ne relève pas de la mission du COC d'évaluer plus en détail les canaux de communication internes de la police fédérale, et encore moins de se mettre en quête de responsables individuels.

5.4. L'absence d'une base légale

19. Il ressort incontestablement de ce qui précède que la police judiciaire fédérale a réellement appliqué la technologie de reconnaissance faciale de *Clearview* à des données à caractère personnel policières (photos et images). Le fait que les photos qui ont été utilisées dans ce contexte n'auraient pas eu[52]trait à des 'dossiers' belges n'y change rien. Ni la nationalité des personnes concernées ni le fait qu'il s'agisse ou non de personnes faisant l'objet d'un dossier d'information 'belge' ne sont pertinents en l'occurrence. Le COC souligne que ce traitement de données à caractère personnel relève de la responsabilité d'un service de police belge. Or, le cadre juridique de l'Union européenne en matière de protection des données à caractère personnel (transposé au Titre II de la LPD) et les dispositions de la LFP en matière de gestion de l'information s'appliquent sans restriction aux données à caractère personnel traitées par les services de police belges.

20. Cela signifie que la police judiciaire fédérale a par ailleurs communiqué des données policières à une entreprise tierce privée (étrangère) (et donc pas à un service de police ou une autorité). Comme nous l'exposons ci-après, cette communication de données policières ne trouve nullement appui dans la LFP et est dès lors illicite. Le COC constate que la police fédérale n'a émis à ce sujet aucune remarque ni réserve dans le cadre du droit de réponse, et se rallie dès lors au point de vue du COC.

21. Tout comme le ministre de l'Intérieur[53], nous constatons que l'utilisation de la technologie de reconnaissance faciale n'est pas concrètement réglementée dans la loi sur la fonction de police (LFP). Et force est de constater que la transmission de données policières à une tierce partie privée comme *Clearview* ne l'est pas non plus.

L'article 44/1 §2, 1° de la LFP prévoit dans des termes très généraux une base légale pour le traitement de 'données biométriques' en vue de l'identification univoque notamment de suspects d'un fait répréhensible et de personnes disparues. Il convient par exemple de faire remarquer que dans les dossiers du NCMEC, les victimes sont des enfants. Or, la loi exige en principe pour l'utilisation de leurs données biométriques l'obtention du consentement des parents ou du tuteur aussi longtemps qu'aucun dossier pénal belge (ou éventuellement une enquête étrangère soumise aux règles de l'entraide judiciaire) n'a été ouvert, ce qui est en l'occurrence toujours le cas. Il est donc très peu probable – pour ne pas dire impensable – que le législateur ait également tenu compte, lors de l'introduction de la compétence de traitement pour les données biométriques en 2019, de l'éventualité que ces données puissent être traitées dans le cadre d'abus sexuels à l'encontre d'enfants tels que visés en l'occurrence par la taskforce d'Europol.

De plus, la notion de 'données biométriques' est plus large que la seule reconnaissance faciale, de sorte que leur traitement, en fonction des circonstances du traitement et de la technologie utilisée, induit un risque particulièrement élevé pour la protection des droits et libertés fondamentaux. À la lumière de la qualité de la base légale imposée par la jurisprudence (européenne) 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

[51] Voir aussi la note temporaire du 28.01.2022 portant la référence CG/2022-16 et intitulée *« Rappel des directives concernant le traitement de données à caractère personnel »*, qui était adressée à toutes les entités de la police fédérale.
[52] *« auraient »*, parce qu'il n'est plus possible de déterminer sur quelles photos ou images (ni a fortiori sur quels « dossiers ») l'application a été utilisée par les membres de la DJSOC.
[53] Doc. Parl. *Chambre*, 2020-2021, Commission de l'Intérieur, de la Sécurité, de la Migration et des Matières administratives, 6 octobre 2021, CRIV 55 COM 597, p. 4.

être définies dans une norme de droit et accompagnées de garanties (de sécurité) spécifiques et adéquates[54]. À cet égard, le COC a déjà souligné précédemment l'absence d'une base légale spécifique pour l'utilisation de la technologie de reconnaissance faciale par la police de l'aéroport de Zaventem[55], pour laquelle le COC a dû formuler des mesures correctrices.

Dans le cadre de son droit de réponse, le commissaire général a prié le COC d'adopter un point de vue concernant la conformité aux dispositions actuelles de la LFP de l'application de la reconnaissance faciale aux données policières internes existantes. Le COC souligne que la police fédérale fait à cet égard référence aux notes de bas de page 27 et 30 du projet de rapport contradictoire, qui ont été reprises telles quelles dans le présent rapport définitif. Pour toute clarté, la demande visant à adopter un point de vue n'a donc **pas** trait à la recherche ciblée telle que visée par l'utilisation de l'application *Clearview* par la DJSOC, mais bien à l'application de la technologie de reconnaissance faciale à des données policières internes existantes (comparaison de photos enregistrées dans les banques de données policières). Il convient de souligner que cette demande doit être ignorée *hic et nunc* et dans le présent rapport dès lors que l'utilisation de la reconnaissance faciale qui est visée par la police fédérale dans sa réaction du 28 janvier 2022 est tout à fait différente de l'utilisation de *Clearview*, et que seule cette dernière fait l'objet du contrôle et du présent rapport définitif. De plus, et purement par souci d'exhaustivité, les situations envisagées par le COC dans le rapport, dans lesquelles la police pourrait recourir à la reconnaissance faciale, sont purement hypothétiques et ne s'appliquent au surplus que pour autant que cette utilisation soit réglementée de manière claire et précise dans la LFP, ce qui n'est pas le cas actuellement. Comme nous le faisions remarquer plus haut, la notion de 'données biométriques' est interprétée au sens très large (empreintes digitales, caractéristiques faciales et comportementales, iris de l'œil, empreinte d'oreille, voix, émotions, …), de sorte que la nature très spécifique des données et des processus de traitement (sous-jacents) diffère fortement notamment en fonction de l'intelligence artificielle spécifique à laquelle il est recouru dans ce cas précis et du (degré de) risque pour les droits et libertés fondamentaux de la personne concernée, de sorte qu'un cadre légal spécifique et précis, accompagné de garanties, est requis. Or, ce cadre n'existe pas à l'heure actuelle.

Au surplus, le COC fait référence à son 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)[56], dans lequel il approfondit en détail le cadre législatif *de lege lata* et *de lege ferenda*.

22. Il convient, par souci d'exhaustivité, de tenir compte également du fait que l'utilisation de l'application *Clearview* diffère en certains points (essentiels) de l'usage que la police de l'aéroport de Zaventem fait de la technologie de reconnaissance faciale.

Pour commencer, la reconnaissance faciale de *Clearview* n'est en l'occurrence pas appliquée aux images de caméras installées dans des lieux publics. Au lieu de cela, elle utilise des photos ou des images dont la police dispose déjà dans le cadre de dossiers du NCMEC. Il est donc question d'un recours ciblé à la reconnaissance faciale. Ensuite, la police judiciaire fédérale fait appel pour l'utilisation de la technologie de reconnaissance faciale à une tierce partie, en l'occurrence une entreprise commerciale privée (américaine). La police transmet en effet les photos de police (données à caractère personnel) à *Clearview* par le biais d'une URL de cette dernière, ou du moins les met à sa disposition, *Clearview* devant être considérée comme une 'tierce partie' à la lumière du Titre II de la LPD, de sorte qu'il est par essence procédé à un transfert d'informations et de données à caractère personnel policières (photos de personnes), ou du moins qu'il est accordé un accès à ces données[57]. De ce fait, des **données à caractère personnel policières sont transmises à un destinataire se trouvant dans un pays tiers sans qu'il ne soit établi que ce dernier garantit un niveau de protection adéquat ou offre les garanties appropriées**[58]. Le médiateur finlandais en charge de la protection des données en arrive à la même conclusion en ce qui concerne l'utilisation expérimentale de

[54] Non seulement sur le plan juridique, mais aussi sur le plan de la fiabilité (objectivité, homologation, …) et de la transparence des aspects techniques de cette technologie. Le recours à cette technologie (processus de traitement et de décision) n'est en effet pas performant en soi.
[55] 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 (DIO19005), https://www.organedecontrole.be/publications/rapports.
[56] Voir www.organedecontrole.be, sous la rubrique Publications/Avis réglementation.
[57] Cf. *European Data Protection Board*, *« Guidelines 05/2021 on the interplay between the application of Article 3 and the provisions on the international transfers as per Chapter V on the GDPR »*, adoptées le 18 novembre 2021 et disponibles sur le site edpb.europa.eu/our-work-tools/general-guidance/guidelines-recommendations-best-pratices_en.
[58] Articles 66 à 70 de la LPD.

l'application *Clearview* par la police finlandaise[59]. Troisièmement, **les services de police belges transmettent dans ce contexte des informations et des données à caractère personnel policières à un destinataire tiers privé (une entreprise qui n'a pas non plus la qualité de sous-traitant), ou du moins les mettent à sa disposition, ce qui n'est pas prévu dans la LFP et n'est donc pas autorisé (ni à une instance ou entreprise belge ou européenne, ni a fortiori à une entreprise américaine)**. Les destinataires ne faisant pas partie de la police sont en effet strictement délimités dans la LFP[60]. Le COC constate que ces trois points ne sont pas contestés par la police fédérale dans le cadre de son droit de réponse, et que cette dernière n'émet aucune réserve à ce sujet.

23. Par souci d'exhaustivité, le COC rappelle et souligne que le fait que l'application *Clearview* soit utilisée sur des personnes (auteurs ou victimes) qui ne sont pas de nationalité belge ne change **rien** à l'absence d'une base légale suffisante dans la LFP. Si le traitement relève du champ d'action de l'Union européenne, la protection offerte par la *LED* (transposée au Titre II de la LPD et dans la LFP) s'applique aux personnes physiques indépendamment de leur nationalité ou résidence[61]. Il en découle que même si la reconnaissance faciale de *Clearview* a été appliquée par la police judiciaire fédérale à des citoyens non belges (ce qui n'est pas établi) ou à des citoyens ayant la nationalité d'un autre État membre ou d'un pays tiers, une base légale est requise pour l'application de la technologie de reconnaissance faciale[62].

24. Il relève de la responsabilité du responsable du traitement – en l'occurrence la police judiciaire fédérale – d'examiner si l'utilisation expérimentale de cette technologie de reconnaissance faciale était (est) possible selon la loi.

Concrètement, cela revient donc à dire que la police judiciaire fédérale aurait globalement dû se poser les questions suivantes et y répondre :

1) Quelles données à caractère personnel sont traitées ?
2) La police est-elle compétente pour ce traitement ?
3) Quel traitement est effectué (traitement biométrique, transfert à un pays tiers, …) ?
4) Ce traitement est-il autorisé d'un point de vue juridique ?
5) Où les données à caractère personnel sont-elles conservées et pour combien de temps ?
6) Le traitement des données biométriques s'accompagne-t-il des garanties appropriées ?

Ces questions et risques auraient dû être identifiés et résolus dans une analyse d'impact relative à la protection des données (AIPD[63]).

Le COC n'a reçu aucune information indiquant que la DJSOC ait procédé à une telle analyse.

On peut donc raisonnablement partir du principe que cette obligation imposée par la LPD n'a pas non plus été respectée par la police judiciaire fédérale, comme le confirme le fait que ce constat n'ait pas été contesté dans le cadre du droit de réponse.

6. RÉFLEXIONS

25. L'utilisation de la technologie de reconnaissance faciale de *Clearview* par la Direction générale de la police judiciaire (concrètement par la DJSOC) et l'utilisation de la technologie de reconnaissance faciale par la Direction générale de la police administrative (concrètement par la police de l'aéroport de Bruxelles-National) ont en commun qu'elles cadraient dans les deux cas dans une 'phase de test'. Cela dit, même dans cette phase de test – ou, pour dire les choses

[59] Disponible sur le site edpb.europa.eu/news/national-news/2021/finnish-sa-police-reprimanded-illegal-processing-personal-data-facial_en.
[60] Article 44/11/9 §1er de la LFP. En vertu du 2e paragraphe du même article, les données à caractère personnel et les informations peuvent également être communiquées aux autorités publiques **belges**, organes ou organismes publics ou d'intérêt public chargés par la loi de l'application de la loi pénale ou qui ont des missions légales de sécurité publique lorsque ceux-ci en ont besoin pour l'exécution de leurs missions légales. Cette possibilité n'est ici mentionnée qu'au surplus étant donné que *Clearview* n'est non seulement pas un organisme belge, mais n'est pas non plus une autorité, ni un organe ou un organisme public, et est encore moins chargée par la loi de l'application de la loi pénale.
[61] Article 2 de la *LED* lu conjointement avec les considérants 2 et 17. Article 2 du RGPD lu conjointement avec le considérant 2 du RGPD.
[62] Dans sa réponse du 19 septembre 2021, la DGJ souligne que l'utilisation de la technologie de reconnaissance faciale n'avait pas trait à des dossiers belges, ce qui contredit le courrier du commissaire général du 18 octobre 2021, dans lequel il est stipulé *« (…) nous avons bien mentionné que des utilisations avaient eu lieu 'à quelques reprises dans les dossiers du National Center for Missing and Exploited Children en Belgique' »* (soulignement du COC).
[63] En anglais *'Data Protection Impact Assessment'* (DPIA).

autrement, lorsque le traitement des données à caractère personnel est purement ou notamment effectué à des fins de test –, la LPD et la LFP doivent être respectées. *De lege ferenda*, il n'est prévu aucune dérogation au cadre légal, même s'il s'agit purement d'une phase de test ou d'un projet pilote.

26. La différence essentielle entre les deux cas se situe en revanche dans le processus de traitement sous-jacent de l'application *Clearview*. Contrairement au cas de l'utilisation de la reconnaissance faciale par la police de l'aéroport de Zaventem, l'utilisateur de l'application *Clearview* n'exerce aucun contrôle sur le traitement des données biométriques. Les photos et les images sont en effet chargées par le biais d'une URL, de sorte que la disponibilité des photos et des images est entièrement confiée à l'entreprise américaine *Clearview*. Les photos et les images, y compris le traitement biométrique (le template qui contient les données à caractère personnel uniques), sont envoyées en dehors de l'environnement policier (et en dehors de l'ordre judiciaire de l'UE) et sont ensuite traitées. **L'entité de police qui transmet les photos et les images n'a donc (plus) aucune emprise sur le traitement des données biométriques, ni sur la suite du processus de traitement appliqué par le destinataire.** Il est donc clair, et dès lors hautement problématique, que le service de police qui transmet les photos et les images n'a aucune influence notamment sur le délai de conservation des photos et images, ni sur l'usage commercial qui pourrait potentiellement en être fait par *Clearview*. Par ailleurs, il n'est pas clairement établi si *Clearview* a, en marge du template (ce code unique des caractéristiques biométriques), également conservé les données biométriques brutes (les caractéristiques uniques du visage sur la base desquelles le code unique est créé), ni si elle les a par la suite exploitées à des fins commerciales. Enfin, il est clair qu'il est pour ainsi dire impossible pour les personnes concernées de savoir que leur photo a été chargée dans l'application *Clearview*, et il est de surcroît très difficile – pour ne pas dire impossible – pour la personne concernée d'exercer ses droits à l'égard de *Clearview* (voir notamment l'enquête de la CNIL que nous évoquions plus haut au point 12).

27. On peut également conclure de l'enquête menée par le COC que la police judiciaire fédérale ne considère pas (nécessairement) l'utilisation de la reconnaissance faciale de *Clearview* comme un acte d'information ou d'instruction, de sorte que l'attente légitime qu'il doive également être satisfait aux obligations d'enregistrement s'appliquant au traitement d'informations et de données à caractère personnel policières en vertu de la LFP et de la directive MFO-3[64] ne peut pas non plus être rencontrée. Les traitements ont manifestement lieu durant la phase préalable à l'ouverture d'une information ou d'une instruction (belge), et ils se cantonnent (éventuellement même exclusivement) au niveau policier. De ce fait, le COC n'a pas non plus pu vérifier objectivement ni matériellement si l'utilisation de la reconnaissance faciale a effectivement conduit à un résultat négatif ou positif (l'Organe de contrôle peut ici uniquement se baser sur les affirmations des deux enquêteurs interrogés). Ces traitements de données à caractère personnel ne sont nulle part saisis ni journalisés dans les banques de données policières existantes.

L'application est donc plutôt considérée comme une forme de 'moteur de recherche Internet'. Les enquêteurs concernés sont en l'occurrence partis du principe que les personnes qui s'aventurent dans l'univers numérique accessible au public « s'exposent » sciemment au contrôle de la police, par analogie aux personnes qui fréquentent des lieux publics dans le monde réel. Cette perception qu'ont les membres de la police judiciaire fédérale – ou du moins certains d'entre eux – repose notamment sur l'hypothèse que ce qui est accessible au public dans l'univers numérique est aussi effectivement disponible pour la police et peut être utilisé par cette dernière (*'open source intelligence'*). Dans cette optique, *Clearview* n'est qu'un moyen facilitant l'accès à ces photos accessibles au public. Cette vision n'a cependant rien d'une évidence et est en tout état de cause dans une certaine mesure contraire au cadre en vigueur en matière de protection des données.

L'utilisation de la reconnaissance faciale de *Clearview* par la police judiciaire fédérale doit incontestablement être considérée comme un acte d'information ou d'instruction policier (car tel en est le seul objectif), de sorte que, comme nous le faisions remarquer plus haut, les obligations découlant des dispositions de la LFP et de la MFO-3 restent d'application sans restriction, ce qui signifie que ces traitements sont également traçables ou devraient l'être, ce qui n'est en l'occurrence pas le cas.

28. Avant que cette technologie de reconnaissance faciale ne soit utilisée par la police judiciaire fédérale, elle a fait l'objet d'« expérimentations » libres avec des photos personnelles des fonctionnaires de police participants. C'était également le cas lors de l'utilisation de photos de victimes et d'auteurs provenant de dossiers du NCMEC. Les membres de la DJSOC n'y voyaient manifestement aucun problème, d'autant que la hiérarchie ne s'est jamais opposée à

[64] La Directive commune MFO-3 du 14 juin 2002 des Ministres de la Justice et de l'Intérieur *'relative à la gestion de l'information de police judiciaire et de police administrative'*.

l'utilisation de la technologie de reconnaissance faciale. Un constat à la fois frappant et interpellant réside dans le fait que ni la DJSOC ni la DGJ – en particulier la hiérarchie – ne semblent avoir pensé à l'impact et aux conséquences du processus de traitement de l'application *Clearview*. Elles semblent à tout le moins ne pas comprendre – ou pas suffisamment – la portée procédurale et juridique de l'application *Clearview*, et ne pas être en mesure de l'évaluer en connaissance de cause.

La police judiciaire fédérale ne semble pas réaliser que l'utilisation de cette application implique le transfert de photos de la police à une entreprise commerciale (qui plus est établie en dehors de l'Union européenne), ni que les données biométriques – en l'occurrence des caractéristiques faciales – sont depuis lors conservées par l'entreprise *Clearview*[65].

Manifestement, il n'a pas été et il n'est toujours pas tenu compte du fait que le traitement de ces photos et images (et données biométriques) constitue le modèle d'activité de cette entreprise. L'optimalisation de la banque de données de *Clearview* est l'activité principale sur laquelle repose son modèle de rentabilité et donc sa subsistance. Ce n'est naturellement pas sans raison que *Clearview* incite dans sa correspondance par e-mail les utilisateurs du compte *Clearview* à effectuer un maximum de recherches (et donc à partager des photos et des images avec *Clearview*).

29. Il serait une erreur de penser que seules des images d'auteurs et/ou de suspects sont conservées. Logiquement, il s'agit de photos qui font partie de dossiers de la police. De cette manière, des photos non seulement d'auteurs, mais aussi de victimes (et même de témoins ou de passants occasionnels) se retrouvent aux mains d'une entreprise qui assure sa subsistance et qui génère et optimalise ses bénéfices au moyen d'informations et de données à caractère personnel très sensibles, dont celles de personnes particulièrement vulnérables. Or, l'utilisateur de l'application *Clearview* n'a aucun contrôle sur ce traitement.

Dans le cadre du droit de réponse, la police fédérale a invoqué des circonstances[66] qui ont trait d'une part à l'utilisation très restreinte et temporaire de *Clearview* par la DGJ, et d'autre part à la lourde charge de travail de cette direction générale. Bien que le COC comprenne que le service de police a exclusivement utilisé l'application *Clearview* par souci d'efficacité, cela ne change rien au constat fait par le COC, à savoir que des données policières (photos d'auteurs, de victimes et de tiers) se sont retrouvées aux mains d'une entreprise privée américaine. Le fait que la DGJ ne l'ait manifestement pas compris constitue un point d'attention et d'action important, de sorte que la charge de travail invoquée n'est à cet égard d'aucune pertinence.

7. CONCLUSION

29. Il ressort de l'enquête menée par l'Organe de contrôle que des membres de la police judiciaire fédérale ont expérimenté avec la technologie de reconnaissance faciale de l'entreprise américaine *Clearview* en utilisant des photos de victimes et d'auteurs provenant d'une enquête de pédopornographie.

L'expérimentation avec la technologie de reconnaissance faciale dans le cadre de laquelle il est recouru à des photos de victimes et de suspects constitue un traitement de données à caractère personnel soumis à la LPD et à la LFP.

L'application de la technologie de reconnaissance faciale constitue un traitement spécifique de données à caractère personnel biométriques du visage de la personne lors duquel des caractéristiques faciales uniques de la personne sont enregistrées. L'application de la technologie de reconnaissance faciale constitue à ce titre une ingérence très grave dans le respect de la vie privée et la protection des données à caractère personnel.

[65] Il convient de faire remarquer que l'Organe de contrôle n'a pas obtenu de preuve de l'existence d'une validation par les fonctionnaires de police (ni, a fortiori, par le responsable hiérarchique de la police) lors de la création d'un compte auprès de *Clearview*. Il n'est pas exclu que *Clearview* n'applique aucun processus de validation effectif lors de la création d'un compte. Le fait de disposer d'une adresse e-mail ayant comme nom de domaine '@police.belgium.eu' semble en effet déjà suffisant pour que *Clearview* considère l'utilisateur comme un membre du personnel d'un service de police belge et lui donne par conséquent accès à sa banque de données. Cette méthode est évidemment très problématique étant donné que le personnel non opérationnel de la police et même des personnes ne faisant aucunement partie d'un service de police peuvent également disposer d'une adresse e-mail @police.belgium.eu (notamment certains consultants externes).

[66] La police fédérale renvoie notamment au point 27 du projet de rapport contradictoire, qui a été repris tel quel sous la même numérotation dans le présent rapport définitif. Le COC part par conséquent du principe que les circonstances invoquées par le commissaire général sont également invoquées dans le cadre de ce point.

Bien que la loi sur la fonction de police prévoie d'une manière générale le traitement de données biométriques[67], elle n'offre pas une base légale suffisante pour l'application de cette forme de technologie de reconnaissance faciale. Ce point est d'ailleurs également confirmé au surplus par le ministre de l'Intérieur et par la police fédérale elle-même.

La hiérarchie de la police (judiciaire) fédérale était au courant de l'utilisation expérimentale de la technologie de reconnaissance faciale de *Clearview*, tandis que la DGJ n'a pas mis un terme – ou n'a mis que tardivement un terme – à l'utilisation de cette technologie.

La police judiciaire fédérale a utilisé cette technologie de reconnaissance faciale pendant une courte période, mais sans s'être renseignée sur l'impact et les retombées du processus de traitement sur les données à caractère personnel policières.

L'utilisation de l'application *Clearview* a donné lieu à un transfert d'informations et de données à caractère personnel policières (photos) à une instance non policière au sens de la LPD. De plus, il s'agit d'un transfert de données policières à un destinataire établi dans un pays tiers, sans que la police judiciaire fédérale n'ait examiné si ce destinataire offre et maintient un niveau de protection adéquat comme l'exige la LPD[68]. Ce constat n'a pas été contesté par la police fédérale dans le cadre de son droit de réponse.

Le transfert d'informations et de données à caractère personnel policières (photos provenant de dossiers du NCMEC) 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 non plus contesté par la police fédérale dans le cadre de son droit de réponse.

8. RECOMMANDATIONS ET MESURES CORRECTRICES

29. À la lumière de ce qui précède, le COC émet trois (3) recommandations et prend deux (2) mesures correctrices.

30. Pour le reste, il appartient à la police fédérale elle-même ou à son autorité de tutelle de tirer les enseignements à la fois de cette enquête et de celle menée en 2019 sur l'utilisation de la technologie de reconnaissance faciale par la police de l'aéroport de Bruxelles-National.

POUR CES RAISONS,

l'Organe de contrôle,

Recommandation n° 1

1) recommande de miser sur l'organisation de formations et sur la sensibilisation des membres du personnel (et des dirigeants) concernant le recours à l'*open source intelligence* en fonction de l'application du cadre juridique en vigueur en général et du droit à la protection des données en particulier ;

Recommandation n° 2

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

Recommandation n° 3

[67] Le commissaire général fait à ce sujet référence à juste titre aux articles 34 de la LPD et 44/1 §2, 2e alinéa, 1° et §2, 3e alinéa de la LFP.
[68] Étant entendu qu'il convient de faire remarquer par souci d'exhaustivité que le transfert ne constitue pas non plus une circonstance exceptionnelle au sens de l'article 69 ou 70 de la LPD. De plus, la DJSOC aurait, dans l'hypothèse où le transfert aurait pu être basé sur les dispositions des articles 69 et 70 de la LPD (transfert à une autorité non compétente d'un pays tiers dans des cas exceptionnels) – quod non –, dû effectuer, documenter et mettre à la disposition du COC l'évaluation prévue à l'article 70, ce qu'elle n'a pas fait.

3) insiste pour qu'il soit au moins tenu compte des aspects suivants lors de la réglementation de l'utilisation de la technologie de reconnaissance faciale dans la LPD/la LFP – le cas échéant après un moratoire[69] et éventuellement dans un cadre de test :
- les circonstances particulières dans lesquelles la reconnaissance faciale peut être utilisée ;
- en fonction de la finalité de police administrative ou judiciaire, prévoir 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 (par analogie aux règles relatives à l'utilisation de caméras non visibles) ;
- 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 (dont le seuil minimum) ;
- le contrôle périodique de la fiabilité du processus de traitement technique ;
- la transparence du processus de traitement ;

constate que l'utilisation de la technologie de reconnaissance faciale de *Clearview* n'est pas légale et n'était et n'est par conséquent pas autorisée ;

constate que l'utilisation de la technologie de reconnaissance faciale de *Clearview* constituait un transfert de données policières à un pays tiers au sens de la LPD, sans que la Commission européenne n'ait pris une décision d'adéquation au sens de l'article 67 de la LPD, et sans qu'il ne soit possible d'invoquer les exceptions spécifiques prévues aux articles 68 à 70 inclus de la LPD ;

constate par conséquent que le transfert à *Clearview* doit être considéré comme un *databreach* au sens de la LPD et ordonne à la police fédérale de respecter les règles applicables en cas d'atteinte à la sécurité de l'information, en recourant le cas échéant au modèle de déclaration disponible sur le site Internet de l'Organe de contrôle (www.organedecontrole.be).

impose, en application de l'article 247, 2° et 4° de la LPD, les deux mesures correctrices suivantes :

Mesure correctrice n° 1

ordonne à la police fédérale de prendre les mesures et initiatives nécessaires au respect des obligations du responsable du traitement en cas d'atteinte à la sécurité de l'information conformément aux articles 61 et 62 de la LPD ;

en fait notamment partie, l'initiative de sommer l'entreprise *Clearview* :

a) de supprimer de sa banque de données les photos transmises par la DJSOC ;
b) de supprimer le traitement biométrique auprès de *Clearview*, à savoir le template et les données biométriques brutes ;

la preuve du respect de cette mesure correctrice sera fournie à l'Organe de contrôle dans les deux mois à compter de la prise en connaissance de cette mesure ;

Mesure correctrice n° 2

avertit la police fédérale que toute (potentielle) utilisation future de la technologie de reconnaissance faciale de *Clearview* ou d'une application similaire ou toute utilisation d'une banque de données similaire est illicite et qu'un éventuel traitement projeté de données à caractère personnel peut dès lors constituer ou constituera *de lege lata* une infraction à la réglementation relative au traitement de données à caractère personnel.

[69] Voir la proposition de résolution du 16 juin 2020 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 Parl. *Chambre*, 2019-2020, DOC 1349/001, 22 p. L'Organe de contrôle a émis au sujet de cette proposition son avis n° DA210029 du 24 janvier 2022, voir aussi le point 19, *in fine*.

RAPPORT

Dit pour droit que la date d'entrée en vigueur des mesures correctrices et la date de prise de connaissance desdites mesures telles que visées aux points 1.a) et 1.b) doivent être comprises comme étant la date de la transmission du présent rapport définitif de l'Organe de contrôle augmentée de deux jours.

L'Organe de contrôle rappelle la possibilité, pour les parties, d'introduire un recours auprès de la Cour d'appel du ressort du domicile ou du siège du demandeur dans les 30 jours de la décision définitive de l'Organe de contrôle (article 248 §1er, premier alinéa, et §2 de la LPD).

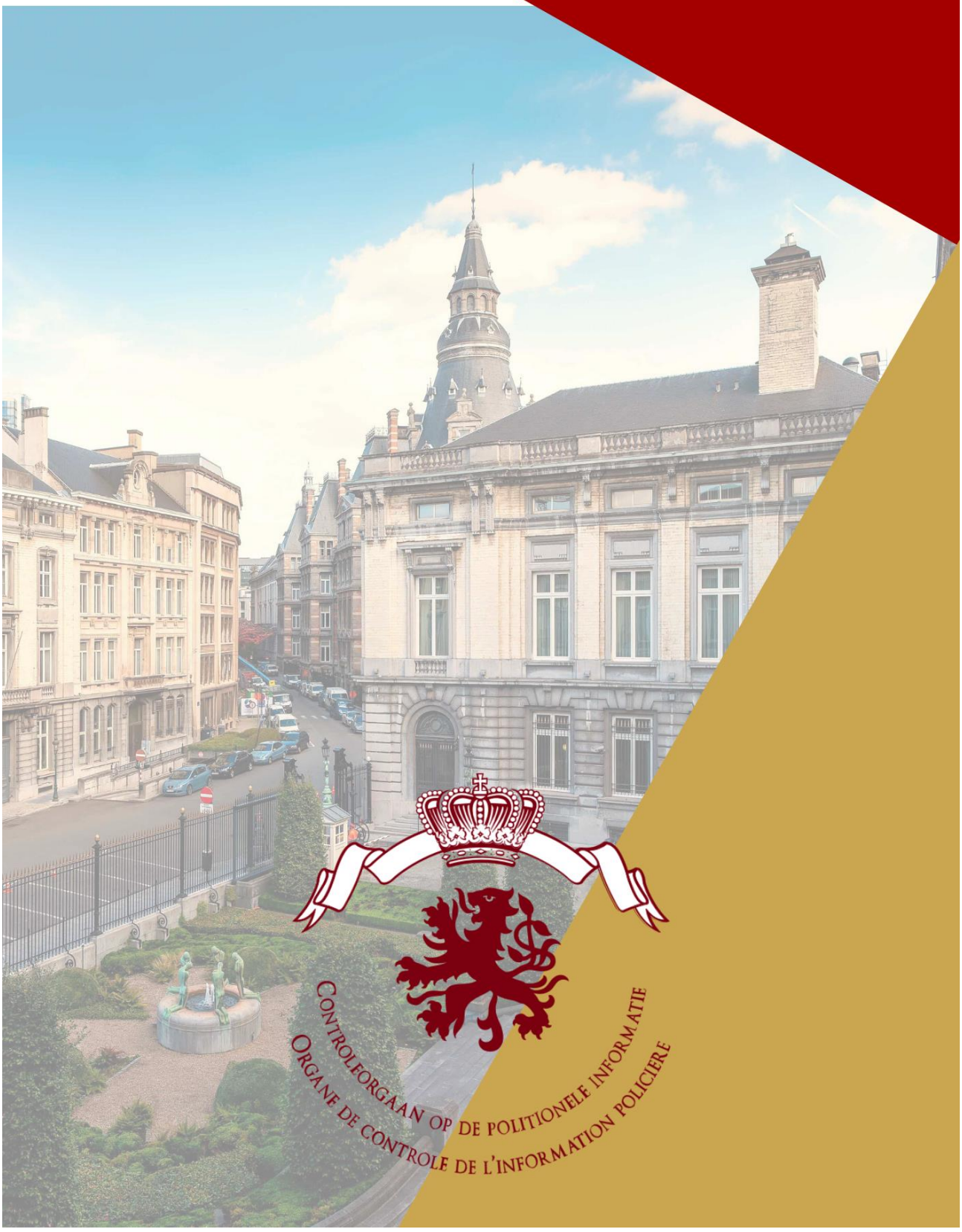
Ainsi décidé par l'Organe de contrôle de l'information policière le 4 février 2022.

Pour l'Organe de contrôle,

Koen Gorissen	Frank Schuermans	Philippe Arnould
Membre-conseiller	Membre-conseiller	Président

Copie électronique :

- à la présidente de la Chambre des Représentants
- au président de la Commission de l'Intérieur, de la Sécurité, de la Migration et des Matières administratives de la Chambre des Représentants
- au ministre de la Justice
- au ministre de l'Intérieur
- au président du Collège des procureurs généraux
- au président de la Commission Permanente de la Police Locale



Controleorgaan op de politionele informatie

Organe de contrôle de l'information policière