ORGANE DE CONTRÔLE DE L'INFORMATION POLICIÈRE

Votre référence	Notre référence	Annexe(s)	Date
	DA210029		24/01/2022

<u>Objet :</u> Avis relatif à une proposition de résolution pour la mise en place d'un moratoire de trois ans sur l'utilisation de logiciels et d'algorithmes de reconnaissance faciale sur les caméras de sécurité, fixes ou mobiles, dans les endroits publics et privés (DOC 55 1349/001 du 16 juin 2020)

L'Organe de contrôle de l'information policière (ci-après le 'COC' ou 'l'Organe de contrôle').

Vu la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel (M.B. du 5 septembre 2018, ci-après 'la LPD'), en particulier l'article 71 et le Titre VII, en particulier l'article 236 §2, 1er alinéa.

Vu la loi du 3 décembre 2017 portant création de l'Autorité de protection des données (ci-après 'la LAPD').

Vu la loi du 5 août 1992 sur la fonction de police (ci-après 'la LFP').

Vu la loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux (ci-après 'la LPI').

Vu la *Law Enforcement Directive* 2016/680 du 27 avril 2016 (ci-après 'la *LED*').

Vu la demande adressée par e-mail par le président de la Commission de l'Intérieur de la Chambre des Représentants en date du 25 novembre 2021.

Vu le rapport de Monsieur Frank Schuermans, membre-conseiller de l'Organe de contrôle.

Émet, le 24 janvier 2022, l'avis suivant.

I. Remarque préalable concernant la compétence de l'Organe de contrôle

1. À la lumière respectivement de l'application et de la transposition du Règlement 2016/679[1] et de la Directive 2016/680[2], le législateur a remanié en profondeur les tâches et missions de l'Organe de contrôle. L'article 4 §2, quatrième alinéa de la LAPD dispose qu'à l'égard des services de police au sens de l'article 2, 2°, de la loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux, les compétences, missions et pouvoirs d'autorité de contrôle tels que prévus par le Règlement 2016/679 sont exercés par l'Organe de contrôle.

2. L'Organe de contrôle doit être consulté lors de la préparation de la législation ou d'une mesure réglementaire ayant trait au traitement de données à caractère personnel par les services de police de la police intégrée (voir les articles 59 §1er, 2e alinéa et 236 §2 de la LPD, l'article 36.4 du RGPD et l'article 28.2 de la directive Police-Justice ou *LED*). L'Organe de contrôle a dans ce contexte pour mission d'examiner si l'activité de traitement projetée par les services de police est conforme aux dispositions du Titre 1er (pour les traitements non opérationnels)[3] et du Titre 2 (pour les traitements opérationnels) de la LPD[4]. En ce qui concerne en particulier les activités de traitement dans le cadre des missions de police administrative et/ou judiciaire, l'Organe de contrôle émet dès lors des avis soit d'initiative, soit à la demande du Gouvernement ou de la Chambre des Représentants, d'une autorité administrative ou judiciaire ou d'un service de police, concernant toute matière ayant trait à la gestion de l'information policière telle que régie par la Section 12 du Chapitre 4 de la loi sur la fonction de police[5].

3. Par ailleurs, l'Organe de contrôle est également chargé, à l'égard des services de police, de l'inspection générale de la police fédérale et de la police locale (en abrégé 'AIG'), telle que visée dans la loi du 15 mai 2007 sur l'Inspection générale, et de l'Unité d'information des passagers (ci-après dénommée en abrégé 'BELPIU') visée au Chapitre 7 de la loi du 25 décembre 2016, de la surveillance de l'application du Titre 2 de la LPD et/ou du traitement de données à caractère personnel tel que visé aux articles 44/1 à 44/11/13 de la loi sur la fonction de police, et/ou de toute autre mission qui lui est confiée en vertu ou par d'autres lois[6].

---

[1] Règlement (UE) 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 ou « RGPD »).
[2] 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 d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil (ci-après dénommée « directive Police-Justice » ou *Law Enforcement Directive* (*LED*)).
[3] Article 4 §2, 4e alinéa de la LAPD.
[4] Article 71 §1er, 3e alinéa de la LPD.
[5] Articles 59 §1er, 2e alinéa et 236 §2 de la LPD.
[6] Article 71 §1er, troisième alinéa juncto article 236 §3 de la LPD.

4. Enfin, l'Organe de contrôle est compétent à l'égard du Service Contentieux de l'Administration générale des Douanes et Accises en ce qui concerne les réquisitions adressées par ce service à la BELPIU dans des matières fiscales, et ce en vertu de l'article 281 §4 de la loi générale sur les douanes et accises du 18 juillet 1977, telle que modifiée par la loi du 2 mai 2019 modifiant diverses dispositions relatives au traitement des données des passagers.

II. Objet de la demande

5. Le demandeur soumet 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 »* (ci-après 'la résolution'), introduite par Messieurs Vanden Burre et Smet et Madame Soors.

6. L'intention des auteurs du texte soumis consiste à :

1) mettre en place un moratoire de trois ans sur l'utilisation de logiciels et d'algorithmes de reconnaissance faciale sur les caméras de sécurité, fixes ou mobiles, dans les endroits publics et privés ;

2) veiller à mettre en place au sein de la Chambre des Représentants un débat sur ce sujet sensible, afin que cette technologie intrusive ne puisse être implémentée qu'accompagnée des garanties strictes concernant les droits humains.

Par essence, les auteurs de la résolution souhaitent dès lors le gel de tout **recours** à la technologie de reconnaissance faciale (ci-après également désignée sous l'acronyme *'FRT'* correspondant au terme anglais *Facial Recognition Technology*). Les auteurs de la résolution n'ont manifestement pas l'intention de faire porter le moratoire sur quelque initiative législative que ce soit concernant la *FRT*.

7. L'Organe de contrôle n'est pas uniquement une autorité de protection des données mais est aussi chargé du contrôle et de la surveillance des banques de données policières[7] et de tous les traitements policiers, également en termes de légalité, d'efficacité et d'effectivité. Cet élément (par exemple de la faisabilité et de la capacité opérationnelles pour la GPI) est également toujours pris en compte lors de la formulation d'un avis.

III. Analyse de la demande

A. Remarques générales

[7] Voir aussi le rapport d'activité 2020 du COC, https://www.organedecontrole.be/files/Rapport-dactivit%C3%A9_COC_2020_F.pdf, points 7 et 8.

8. En ce qui concerne le contenu général et la portée de la résolution, le COC fait référence au texte intégral de cette dernière. Cela dit, la proposition de résolution remonte déjà au 20 mai 2020. La situation a connu dans l'intervalle toute une évolution que nous retracerons ci-après dans les grandes lignes. Il n'est évidemment pas possible dans le cadre du présent avis de détailler de manière exhaustive les nombreuses évolutions, publications et initiatives qui sont intervenues ces dernières années dans le cadre de cette thématique. Il est en tout état de cause établi que ce thème fait l'objet de beaucoup d'intérêt au sein de la société et connaît une perpétuelle évolution, mais que le fonctionnement de l'intelligence artificielle et de la *FRT* n'est pas véritablement compris – et encore moins dans le contexte de la répression (le maintien de l'ordre ou *law enforcement* en anglais), tout comme lorsque l'on se met en quête d'évaluations indépendantes dans les pays où la *FRT* est déjà utilisée dans le contexte de la répression (s'agissant essentiellement d'ordres juridiques anglo-saxons et asiatiques).

9. Comme nous le disions, la proposition de résolution est motivée en détail. Globalement, l'Organe de contrôle n'a aucune remarque particulière à formuler à ce sujet, sous réserve de l'exposé qui suit.

L'exposé des motifs motive en effet de manière convaincante la proposition de moratoire sur toute utilisation de la *FRT* en faisant référence à plusieurs sources (de droit). En ce qui concerne par contre les traitements policiers et donc les finalités de maintien de l'ordre ou répressives (ou, plus généralement, les finalités de police administrative et judiciaire ou de *law enforcement*), la proposition de résolution est d'une certaine manière superflue d'un point de vue juridique étant donné que le cadre légal actuel n'offre de toute manière aucun fondement juridique (suffisant) permettant à la police intégrée (ci-après 'la GPI') – et donc également au parquet et au juge d'instruction – de recourir à une telle technologie de reconnaissance faciale. De fait, ni la loi sur la fonction de police, ni le Code d'instruction criminelle ni une quelconque autre loi (pénale) spéciale n'offre *de lege lata* un fondement juridique (suffisant) pour l'utilisation de la *FRT* dans le cadre de missions de police administrative ou judiciaire. Ce qui n'est dès lors pas possible légalement à l'heure actuelle ne nécessite donc pas – du moins d'un point de vue strictement juridique – une résolution pour confirmer cette impossibilité. La résolution prévoit toutefois un moratoire sur toute utilisation de la *FRT* jusqu'en mai 2023.

La résolution n'empêche cependant pas le législateur d'œuvrer dans l'intervalle à la mise en place d'un cadre législatif pour l'utilisation de la *FRT* en général ou de la *FRT* à des fins de *law enforcement* en particulier, pour autant que l'utilisation effective de cette technologie ne puisse débuter qu'en mai 2023. On peut toutefois se demander si les auteurs de la proposition visent toujours cette date étant donné qu'il ne reste désormais plus que moins d'un an et demi d'ici là. Reste à voir aussi si les auteurs de la résolution s'opposent à ce que le Parlement élabore dans l'intervalle un cadre législatif. Cela ne semble pas être le cas dès lors qu'ils plaident en faveur de la mise en place d'un débat parlementaire afin que cette technologie intrusive ne puisse être implémentée qu'accompagnée des garanties strictes concernant les droits humains.

10. Le fait qu'il n'existe pas à l'heure actuelle de fondement juridique suffisant pour les finalités de *law enforcement* ne nécessite pas d'explications additionnelles. Il semble qu'il existe un consensus sur ce point. Nous pouvons notamment faire référence à ce sujet à la note de politique du ministre de l'Intérieur relative au budget 2022, qui stipule :

« *L'utilisation de caméras et l'échange de données augmentent l'efficacité et la qualité des opérations et des services fournis par la police, l'administration – service Population – et tous les autres services qui veillent à notre sécurité. Toutefois, les évolutions technologiques se heurtent parfois aux préoccupations et à la réglementation en matière de protection de la vie privée, par exemple. En 2022, nous mettrons donc en place une commission consultative éthique « sécurité » pour évaluer l'utilisation éthique et efficace des technologies et des méthodes d'enquête et d'intervention. Les résultats des travaux peuvent également contribuer à améliorer la loi caméras*. »[8]. Et plus loin :

« L'importance d'une utilisation efficace de ces technologies est déjà ancrée dans la législation, dans la loi sur la fonction de police (LFP). Outre les directives élaborées en 2021 dans le cadre de la LFP, d'autres ajustements auront lieu dès 2022 afin de consolider dans la LFP les défis mentionnés au point 11. L'article 44 de la LFP s'appuie en effet sur l'ancienne approche du traitement des données et donc sur des technologies du siècle dernier. Ces ajustements seront effectués en étroite concertation avec l'organe de contrôle (COC) et sous les auspices de l'UE, afin que les nouvelles technologies ne puissent être utilisées que dans des conditions et sous une surveillance strictes, tout en protégeant au maximum le stockage des données. … Les résolutions et la législation européennes relatives à l'intelligence artificielle font l'objet d'un étroit suivi, afin que nous continuions à œuvrer pour une utilisation efficace des nouvelles technologies dans un cadre légal et réglementaire strict, avec l'incorporation nécessaire de mesures de sécurité à plusieurs niveaux, y compris celui des organes de surveillance.[9] »

Dans le cadre de l'utilisation illicite, par la police fédérale, de la technologie de reconnaissance faciale *Clearview*, le ministre a à juste titre déclaré le 6 octobre 2021 au sein de la Commission de l'Intérieur de la Chambre des Représentants[10] : *« Aangezien het Belgisch wettelijk kader de exploitatie van deze software niet toelaat, zal ze niet door de federale politie worden gebruikt, conform mijn eerdere antwoorden met betrekking tot dit thema. … Gezichtsherkenning is zeker een interessante piste om op termijn te gebruiken ter ondersteuning van de werking van de politie in uitvoering van de opdrachten van de bestuurlijke en gerechtelijke politie. Dat kan uiteraard enkel met een correcte wettelijke basis zodat de verkregen informatie rechtsgeldig bestuurlijk en gerechtelijk aangewend kan worden. »*[11] [traduction libre : *Attendu que le cadre légal belge ne permet pas l'exploitation de ce logiciel, celui-ci ne sera pas utilisé par la police fédérale, conformément aux réponses que j'ai formulées précédemment sur ce thème. … La reconnaissance faciale est une piste intéressante à utiliser à l'avenir en appui du fonctionnement de la police dans le cadre de la réalisation des missions*

[8] Doc. Parl. *Chambre*, 2021-2022, n° 2294/18, p. 6 ; soulignement propre de l'Organe de contrôle.
[9] Doc. Parl. *Chambre*, 2021-2022, n° 2294/18, p. 59-60 ; soulignement propre de l'Organe de contrôle.
[10] 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.
[11] Soulignement propre de l'Organe de contrôle.

de police administrative et judiciaire. Ce n'est évidemment possible que moyennant une base légale correcte, de manière à ce que les informations obtenues puissent être utilisées valablement sur le plan administratif et judiciaire.]

11. 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[12] 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)[13].

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*'[14]). 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). En cas de résultat positif ('*hit*' : correspondance des caractéristiques du visage), ce résultat doit être validé ('*match*')[15]. 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.

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[16].

---

[12] 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).

[13] Article 34 §1er de la LPD.

[14] Un *template* peut être défini comme suit : *« A biometric template is a digital representation of the unique features that have been extracted from a biometric sample and is stored in a biometric database. »*, voir *Guidelines on facial recognition, Consultative Committee of Convention 108 the Convention for the protection of individuals with regard to automatic processing of personal data, Council of Europe, June 2021*.

[15] 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.

[16] 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

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[17].

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' de photos ou images correspondantes gérées par des tiers[18] ou par la police (sur une plateforme numérique). Il est donc 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)[19].

(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.

[17] Voir à ce sujet l'article 9, 3e alinéa, 3°, a) et b) de la loi du 21 mars 2007.

[18] 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.

[19] 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 ?).

12. Tout comme le ministre de l'Intérieur[20], 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). 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. 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 et nationale) 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[21]. 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[22], pour laquelle le COC a dû formuler des mesures correctrices. Une intervention similaire de la part du COC se profile dans le cadre du dossier *Clearview*, pour lequel le COC a initié une enquête d'office qui se trouve dans sa phase finale.

B. Contexte plus large et rétroactes

13. Depuis mai 2020, nombre d'autres initiatives notables ont été prises qui toutes peuvent et/ou doivent être mises en relation avec la réflexion au sujet de l'intelligence artificielle en général et de la technologie de reconnaissance faciale en particulier ainsi qu'avec l'élaboration d'une politique et d'une éventuelle législation interne en la matière.

B.1. Au niveau international et européen

14. Le 21 avril 2021, la Commission européenne a publié sa proposition de règlement relatif à l'intelligence artificielle (également dénommé *Artificial Intelligence Act* ou *AIA*)[23]. Sept mois plus tard, le Conseil de l'Union européenne a présenté un texte consensuel contenant quelques modifications

[20] 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.
[21] 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.
[22] 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.
[23] Proposition de règlement établissant des règles harmonisées concernant l'intelligence artificielle (législation sur l'intelligence artificielle) et modifiant certains actes législatifs de l'Union, https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:52021PC0206&from=EN.

substantielles qui donneront sans aucun doute encore matière à discussion. Dans l'intervalle, un avis conjoint de l'*EDPB*[24] et de l'*EDPS*[25] a également été publié sur proposition de la Commission[26].

15. Les points de discussion ont notamment trait, mais pas exclusivement :

- à la définition des systèmes d'intelligence artificielle, pour laquelle le Conseil juge la proposition de la Commission européenne trop large. Le Conseil propose d'exclure de la définition tous les *« logiciels plus traditionnels »*. De plus, la version du Conseil exclut tous les *« systèmes d'intelligence artificielle destinés à des finalités génériques »* du champ d'application de l'*AIA*. Autrement dit, si un système d'intelligence artificielle générique (tels qu'ils sont souvent développés par les grandes entreprises technologiques) renferme seulement le 'potentiel' de mettre en œuvre des pratiques à risque, mais n'a pas (encore) été déployé dans ces contextes à risque, il ne serait pas nécessairement soumis à l'*AIA* ;
- l'une des dispositions les plus controversées est l'article 5 de l'*AIA*, qui énonce une 'liste noire' (les 'pratiques interdites en matière d'intelligence artificielle'), à savoir les applications dont le risque est considéré comme inacceptable, sous réserve de quelques exceptions. Le Conseil a apporté sur ce plan quelques modifications qui ont également leur importance dans le contexte de la répression. En ce qui concerne la reconnaissance biométrique en temps réel, la proposition de la Commission prône l'interdiction générale de son utilisation dans des espaces publics par les autorités répressives, moyennant il est vrai des exceptions importantes. Le Conseil de l'Union européenne a à son tour apporté plusieurs modifications à la proposition de la Commission, dont :
    - une modification du champ d'application, qui ferait que :
        - la finalité de la sécurité nationale (et donc les activités des services de renseignement) ne relèverait pas de l'*AIA* ;
        - les systèmes d'intelligence artificielle dont l'objectif est la recherche scientifique ou le développement (donc aussi la recherche scientifique/le développement par les services de police ?) ne relèveraient pas de l'*AIA* ;
        - le champ d'application aurait trait non seulement aux autorités répressives qui utilisent les systèmes d'intelligence artificielle, mais aussi à leurs éventuels sous-traitants (*« on their behalf »*) ;
    - la caractéristique *« remote »* a été supprimée, de sorte que la portée de l'interdiction de principe est élargie ;

[24] L'*EDPB* (*European Data Protection Board*) ou Comité européen de la protection des données est le comité qui réunit en sa qualité d'organe indépendant de l'Union toutes les autorités de protection des données nationales, tandis que l'*EDPS* (le Contrôleur européen de la protection des données et le successeur de l'ancien groupe de travail « Article 29 », voir la note de bas de page suivante) contrôle l'application correcte et cohérente du droit de la protection des données au sein de l'UE ; voir aussi www.edpb.europa.eu.
[25] L'*EDPS* est l'autorité de protection des données d'Europol ; voir aussi www.edps.europa.eu.
[26] EDPB-EDPS Joint Opinion 5/2021 on the proposal for a regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (Artificial Intelligence Act), 18 June 2021, https://edps.europa.eu/Opinions | European Data Protection Supervisor (europa.eu).

- les menaces pour les infrastructures critiques et la santé ont été introduites en tant qu'exceptions à l'interdiction, et la circonstance selon laquelle la menace doit être imminente a été supprimée, de sorte que la portée de l'utilisation légitime de l'intelligence artificielle est élargie (article 5.1.d.ii).

Pour résumer, la proposition du Conseil prévoit donc à présent une interdiction de principe de l'utilisation en temps réel (*« live »*) de systèmes d'identification biométrique (donc notamment de la *FRT*) à des fins répressives, sauf si l'objectif poursuivi est l'un des suivants :

- la recherche ciblée de victimes (potentielles) (article 5.1.d.i) ;
- la prévention d'une menace spécifique et substantielle pour les infrastructures critiques, la vie, la santé ou la sécurité physique des personnes physiques ou la prévention d'une attaque terroriste (les critères *« infrastructures critiques »* et *« santé »* ont, comme nous le disions, été introduits en tant qu'exceptions additionnelles, tandis que la circonstance selon laquelle la menace doit être *« imminente »* a été supprimée (article 5.1.d.ii) ;
- la détection, la localisation, l'identification ou les poursuites à l'encontre de l'auteur ou du suspect d'une – ou de la personne condamnée pour une – infraction pénale reprise dans la liste prévue par la décision-cadre 2002/584/JAI relative au mandat d'arrêt européen et punissable dans l'État membre concerné d'une peine d'emprisonnement d'une durée maximale d'au moins trois ans, déterminée par le droit de cet État membre.

Le projet d'*AIA* de la Commission, tel qu'amendé par le Conseil, prévoit en outre que les éléments suivants doivent être pris en compte dans le contexte d'une telle utilisation à des fins répressives (article 5.2) :

- la nature de la situation, en particulier la gravité, la probabilité et l'ampleur du préjudice causé en l'absence d'utilisation du système ;
- les conséquences de l'utilisation du système sur les droits et libertés de toutes les personnes concernées, notamment la gravité, la probabilité et l'ampleur de ces conséquences.

Des limitations temporelles, géographiques et relatives aux personnes doivent également être prévues pour toute utilisation à des fins répressives (article 5.2). En vertu du projet d'article 5.3, cette utilisation d'un système d'identification biométrique en temps réel dans des espaces accessibles au public est subordonnée à une autorisation préalable octroyée par une autorité judiciaire ou une autorité administrative indépendante délivrée sur demande motivée et conformément aux règles du droit national. Dans une situation d'urgence, il est possible de commencer à utiliser le système sans autorisation à condition de demander l'autorisation sans retard et de mettre immédiatement un terme à l'utilisation si l'autorisation n'est pas octroyée.

Enfin, l'article 5.4 prévoit que le droit national de l'État membre peut prévoir la possibilité d'autoriser totalement ou partiellement l'utilisation susmentionnée de systèmes biométriques (ce qui signifie que

la Belgique pourrait prévoir des dispositions plus restrictives ou plus strictes dans son propre droit national). Ce droit national devra en tout état de cause fixer des règles détaillées pour la demande, la délivrance et l'exercice des autorisations ainsi que pour la surveillance et le compte rendu y afférents. Ces règles devront également préciser pour quels objectifs énumérés à l'article 5.1.d et notamment pour quelles infractions pénales (figurant dans la liste des infractions pénales visées par le mandat d'arrêt européen) le droit national prévoira la possibilité d'utiliser des systèmes d'identification biométrique en temps réel dans des espaces publics.

De toute évidence, même si l'*AIA* est adoptée, le législateur national aura encore du pain sur la planche et devra faire des choix.

16. Sont notamment considérés comme des systèmes d'intelligence artificielle à haut risque conformément à l'annexe III de l'*AIA* :

- les systèmes d'intelligence artificielle destinés à être utilisés pour l'identification biométrique en temps réel ou a posteriori de personnes physiques à leur insu. Cette définition inclut donc les systèmes d'identification biométrique comme la *FRT* qui seraient utilisés exclusivement de manière réactive dans le cadre d'informations ou d'instructions ;
- dans le contexte de la répression : tous les systèmes utilisés à des fins de *« predictive policing »* et de *« predictive justice »*, les détecteurs de mensonges ou systèmes similaires destinés à détecter les émotions, les systèmes destinés à détecter les hypertrucages (*« deep fake »*), les systèmes destinés à évaluer la fiabilité des preuves et les systèmes destinés à être utilisés pour le profilage dans le contexte de la police ou de la justice. Le Conseil supprime toutefois la proposition de la Commission visant à considérer également comme systèmes à haut risque les systèmes destinés à être utilisés pour l'analyse de la criminalité des personnes physiques, permettant aux autorités répressives d'effectuer des recherches dans de vastes jeux de données complexes liés et non liés disponibles dans différentes sources de données ou dans différents formats de données afin de mettre au jour des schémas inconnus ou de découvrir des relations cachées dans les données.

La qualification des systèmes considérés comme à haut risque est essentielle étant donné que leur utilisation est soumise à de nombreuses conditions et obligations qui sans cela ne sont pas d'application.

17. Il convient également d'évoquer l'interdiction générale, demandée conjointement par l'*EDPB* et l'*EDPS*, de toute forme d'utilisation de l'intelligence artificielle à des fins de reconnaissance automatique de caractéristiques humaines (et donc pas uniquement la reconnaissance faciale) dans des lieux accessibles au public : *« The EDPB and the EDPS call for a general ban on any use of AI for an automated recognition of human features in publicly accessible spaces - such as of faces but also of gait, fingerprints, DNA, voice, keystrokes and other biometric or behavioural signals - in any*

context. »[27]. Le COC est d'ores et déjà d'un avis plus nuancé concernant cet aspect lorsqu'il est question de finalités répressives.

Quoi qu'il en soit, il est clair que le débat de société en général et le trialogue en particulier concernant le règlement sur l'intelligence artificielle sont loin d'être clos. Selon la doctrine, il faudra attendre 2025 pour qu'il soit question d'une entrée en vigueur effective de l'*AIA*, au terme d'un *« long combat qui mènera à une version finale du règlement sur l'intelligence artificielle »*, et nous n'en sommes encore qu'au début d'un processus laborieux[28]. La question qui se pose est dès lors évidemment de savoir s'il est judicieux de ne pas attendre cette initiative législative européenne et de déjà légiférer à ce sujet en tant qu'État membre individuel (voir plus loin).

18. D'autre part, la Commission européenne veut apparemment accélérer la manœuvre pour permettre l'utilisation de la *FRT*, comme en témoigne une proposition très récente visant la création au sein d'Europol d'un *hub* qui mettrait en relation les banques de données policières des 27 États membres et permettrait aussi d'échanger des données biométriques et des informations et données à caractère personnel obtenues par le recours à la *FRT*. La presse a notamment relayé à ce sujet l'information suivante :
« Face à l'activité croissante des réseaux criminels internationaux, la Commission européenne a proposé, ce mercredi, un paquet législatif visant à accroître la coopération entre les forces de police des 27 États membres de l'Union européenne (UE). L'initiative comporte une proposition de directive sur les échanges d'informations entre les services de police. … La Commission propose de revoir les règles du traité de Prüm sur la coopération policière dans l'espace Schengen, afin de créer d'ici à 2027 un hub central pour accélérer l'échange d'informations. Ce point de contact unique, géré par Europol, sera accessible de manière permanente par les services de police des États européens. L'information demandée devrait être mise à disposition dans les 8 heures pour les cas urgents jusqu'à un maximum de 7 jours. L'exécutif européen propose aussi d'inclure dans les informations à partager les images de reconnaissance faciale de suspects et de criminels condamnés[29] *ainsi que les casiers judiciaires*[30]*. »*

Cette dépêche fait référence à la proposition du 8 décembre 2021 de la Commission européenne[31] visant à créer un *code de coopération policière* qui comprendrait (1) une proposition de directive relative à l'échange d'informations entre les services répressifs et abrogeant la décision-cadre 2006/960/JHA[32], (2) une proposition de règlement relatif à l'échange automatisé de données à des

[27] EDPB-EDPS Joint Opinion 5/2021 on the proposal for a regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (Artificial Intelligence Act), 18 June 2021, https://edps.europa.eu/Opinions | European Data Protection Supervisor (europa.eu), voir les points 30 et suivants.
[28] Traduction libre, S. De Schrijver, Een kijk op het strijdtoneel van de Verordening inzake artificiële intelligentie, Computerrecht, 2021, 247. L'auteur ajoute : « Il est clair que l'élaboration du règlement sur l'intelligence artificielle nécessitera encore beaucoup de travail. » (traduction libre).
[29] Soulignement propre.
[30] L'Écho, *Vers une coopération policière plus musclée entre les 27 États membres*, 9 décembre 2021, p. 8.
[31] https://ec.europa.eu/commission/presscorner/detail/fr/ip_21_6645.
[32] *Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on information exchange between law enforcement authorities of Member States, repealing Council Framework Decision 2006/960/JHA, COM(2021) 782 final*

fins de coopération policière (Prüm II)[33] et (3) une recommandation relative à la coopération policière opérationnelle[34]. L'objectif du règlement est *« d'ajouter des images faciales de suspects et de criminels condamnés ainsi que des dossiers de police à l'échange automatisé de données »*[35], et donc de permettre l'échange et la recherche automatisés d'images faciales entre les États membres. Les modalités techniques devront encore être élaborées plus en détail par des actes d'exécution de la Commission et par le droit national (qui devra notamment réglementer l'accès et les modalités de recherche pour la banque de données nationale d'images faciales à créer). Bien que la proposition de règlement ne le précise pas – les *facial images* sont néanmoins définies comme étant des données biométriques[36] –, il est clair que cette recherche et cet échange automatisés de photos/d'images de visages de personnes physiques n'est pas possible sans de véritables traitements biométriques, ce qui sous-entend un système de reconnaissance faciale à part entière.

19. L'*EDPB* (le Comité européen de la protection des données) planche en ce moment de son côté (comme il l'a d'ailleurs fait pendant la totalité de 2021) sur des directives relatives à l'utilisation de la technologie de reconnaissance faciale à des fins répressives[37]. Le COC représente pour ce thème la Belgique en qualité d'autorité de protection des données. Le temps nécessité par l'élaboration d'une directive et le nombre de réunions qui ont été organisées jusqu'ici à ce sujet illustrent bien la complexité de la thématique.

Ces directives seront cruciales, notamment parce qu'elles décrivent bien les différentes applications possibles de la *FRT*, qui n'impliquent pas toutes le même degré de violation de la vie privée. L'aspect suivant est en effet important également : dans quels cas et pour quelles finalités veut-on utiliser la *FRT* ? Le projet attire à juste titre l'attention sur la multitude d'objectifs, d'applications et de contextes de la *FRT*.

20. Dans la phase de projet de la directive, les exemples suivants sont d'ores et déjà évoqués lorsqu'il est question de la reconnaissance faciale à des fins d'identification[38] :

- la recherche de photos/d'images dans un fichier afin d'établir l'identité d'une personne inconnue (par exemple un auteur/suspect ou une victime) ;
- la surveillance du comportement d'une personne dans un lieu public. Le visage de cette personne est comparé avec les *templates* de toutes les personnes se trouvant en ce lieu

2021/0411(COD).

[33] *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on automated data exchange for police cooperation ("Prüm II"), amending Council Decisions 2008/615/JHA and 2008/616/JHA and Regulations (EU) 2018/1726, 2019/817 and 2019/818 of the European Parliament and of the Council, COM(2021) 784 final 2021/0410(COD).*

[34] Proposition de RECOMMANDATION DU CONSEIL relative à la coopération policière opérationnelle, COM(2021) 780 final 2021/0415(CNS).

[35] Reinforcing police cooperation across Europe, Factsheet_Police cooperation package_Reinforcing police cooperation across Europe, https://ec.europa.eu/commission/presscorner/detail/en/fs_21_6647 ; voir aussi les considérants 5, 7, 10 et 11 et les projets d'articles 1, 3, 4, 10° et 11°, et en particulier le chapitre 4.

[36] Projets d'articles 4, 11°, 37, 39 et 50 de la proposition de règlement Prüm II.

[37] À l'heure actuelle, le document s'intitule donc toujours *« Draft guidelines x/202x on the use of facial recognition technology in the area of law enforcement »*, non publié.

[38] Nous ne parlons donc pas des applications à des fins d'authentification.

pendant une période déterminée (par ex. après qu'une infraction pénale a été commise en ce lieu) ;

- la reconstitution du trajet parcouru par une personne et des contacts qu'elle a eus avec d'autres personnes durant ce trajet ;
- l'identification biométrique à distance (*remote*), dans des lieux publics, de personnes recherchées par la police/la justice, ce qui implique une comparaison du *template* des personnes recherchées avec les *templates* de tous les visages de toutes les personnes présentes pendant une période donnée en ce lieu public ;
- la reconnaissance automatisée dans le but de détecter des relations sur les réseaux sociaux ;
- etc.

L'attention est à juste titre attirée sur les aspects de la fiabilité et de l'exactitude de la technique : *« Like every technology, facial recognition may also be subject to challenges when it comes to its implementation, in particular when it comes to its reliability and efficiency in terms of authentication or identification, as well as the overall issue of quality and accuracy of the "source" data and the result of facial recognition technology processing.*
Such technological challenges entail particular risks for data subjects concerned which are all the more significant or serious in the area of law enforcement considering the possible legal effects for data subjects or other effects similarly affecting them in a significant manner.
As pointed out by the EU Fundamental Rights Agency in its 2019 report[39], "determining the necessary level of accuracy of facial recognition software is challenging": there are many different ways to evaluate and assess accuracy, also depending on the task, purpose and context of its use. When applying the technology in places visited by millions of people – such as train stations or airports – a relatively small proportion of errors (e.g. 0.01 %) still means that hundreds of people are wrongly flagged. In addition, certain categories of people may be more likely to be wrongly matched than others, as described in Section 3. There are different ways to calculate and interpret error rates, so caution is required. In addition, when it comes to accuracy and errors, questions in relation to how easily a system can be tricked by, for example, fake face images (called 'spoofing') are important particularly for law enforcement purposes. ».

Le projet de directive décrit en outre différents scénarios possibles (applications hypothétiques) ou *use cases*, qui montrent aussi que les risques pour la protection de la vie privée peuvent fortement différer selon le scénario ou *use case*, compte tenu d'une AIPD à réaliser qui devra évaluer la nécessité, la proportionnalité, les finalités et le cadre juridique national ou européen applicable. Pour simplifier, il s'agit des possibilités suivantes :

- systèmes de contrôle aux frontières consistant en une comparaison un-à-un ; il s'agit donc d'une vérification et d'une identification 1 – 1 ;

[39] *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, EU Fundamental Right Agency, 21st November 2019.

- un système visant à identifier les victimes de pédophilie sera mis au point, consistant en une comparaison de reconnaissance faciale entre la photo d'une victime potentielle avec une banque de données policière de photos de victimes de pédophilie ; ce système serait alors utilisé au cas par cas dans des enquêtes spécifiques, suivi à chaque fois d'une vérification sur la base de tous les éléments du dossier ; il s'agit donc d'une identification 1 – N ;
- un système permettant d'identifier des auteurs sélectionnés de vandalisme et de violence lors d'une manifestation en comparant leur image avec les images ou photos de caméras fixes ou mobiles (privées et publiques) installées sur les lieux des faits et aux abords, les images publiées par les médias, les images publiées sur les réseaux sociaux, etc. (les images/photos servant de base à la comparaison ne sont donc a priori pas une banque de données policière ; la police crée une banque de données ponctuelle en rassemblant les images/photos 'privées' évoquées plus haut de toutes les personnes qui étaient présentes au moment des faits) ; il s'agit donc d'une identification 1 – N ;
- un scénario identique au précédent, mais cette fois en effectuant une comparaison avec la banque de données policière nationale de photos de suspects telle qu'elle est tenue à jour par la police judiciaire ; il s'agit donc d'une identification 1 – N ;
- un système d'identification biométrique à distance en temps réel dans des lieux publics procédant à une comparaison continue de toutes les personnes présentes en ce lieu avec une liste de personnes recherchées sans qu'il ne soit question d'une présomption (ou, le cas échéant, seulement d'une présomption très vague) quant à la présence potentielle de ces personnes recherchées dans les lieux publics placés sous surveillance ; il s'agit donc d'une identification N – 1 ;
- un système privé et une banque de données privée (du type *Clearview*) sont utilisés par la police à des fins de reconnaissance faciale ; il s'agit d'une identification 1 – N, mais elle peut avoir trait à des suspects, à des victimes voire à des témoins.

Ces exemples d'utilisations potentielles de la *FRT* montrent à eux seuls l'énorme complexité, ne serait-ce que pour élaborer une législation adéquate indépendamment de l'usage qui est effectivement fait de la technologie.

21. Un autre document important en la matière est la *Recommendation CM/Rec(2021)8* du Comité des Ministres du Conseil de l'Europe *« on the protection of individuals with regard to automatic processing of personal data in the context of profiling »*, adoptée le 3 novembre 2021 et abordant notamment la problématique du profilage, la qualité requise des algorithmes utilisés ainsi que les dispositions et mesures spécifiques à prendre lorsque le profilage repose sur des systèmes d'intelligence artificielle incluant des processus d'apprentissage automatique (*« machine learning »*).

B.2. Au niveau belge

22. Outre la proposition de résolution qui fait l'objet du présent avis, nous pouvons également faire référence à la proposition de loi n° 55 1904/001 du 6 avril 2021 modifiant la loi relative à la publicité de l'administration[40], au sujet de laquelle l'IFDH[41] a émis son avis 5/2021 du 5 octobre 2021. Dans cet avis, l'IFDH attire également l'attention sur les dangers et les enjeux de l'utilisation de l'intelligence artificielle, même si la proposition ne s'applique pas aux services répressifs comme la police et les instances judiciaires. La proposition a en tout cas le mérite d'être la première à vouloir définir un cadre pour l'utilisation, par les administrations belges, de certaines technologies algorithmiques et de l'intelligence artificielle.

C. Arguments plaidant en faveur d'un moratoire

C.1. Légitimité de la police et application de la fonction de police orientée vers la communauté

23. Comme le montre l'énumération d'initiatives (législatives) en tous genres, le sujet est tout sauf cristallisé.

Michael O'Flaherty, le directeur de l'Agence des droits fondamentaux de l'Union européenne (la FRA), a déclaré ce qui suit lors de la conférence de l'*EDEN*[42] le 18 octobre 2018[43], soulignant à juste titre l'importance pour la police, avant tout pour sa propre légitimité, de respecter comme il se doit les droits fondamentaux notamment lors du recours à l'intelligence artificielle : *« … when policing itself shows a deep respect for human rights, it delivers better outcomes. Such approaches do, and will, help build public trust in policing, which is so essential for secure societies. We need to invest in the strengthening, the building of that trust right now, for instance, in the context of the use of biometric data applications in public settings. »*. Sans cette confiance de la population à l'égard de la police et des technologies qu'elle utilise, il ne saurait être question d'une fonction de police orientée vers la communauté alors qu'il s'agit là toujours par excellence du modèle auquel la Belgique aspire. Ce modèle est, soit dit en passant, déjà fortement hypothéqué par la pandémie de coronavirus, qui force la GPI à endosser un rôle par définition répressif. La police doit éviter à tout prix de recourir à une technologie dont la fiabilité, l'exactitude, la pertinence et la qualité sont mises en doute par la population, voire par les autorités, a fortiori parce que cela porterait également préjudice à la chaîne répressive dans son ensemble.

---

[40] Proposition de loi du 6 avril 2021 modifiant la loi relative à la publicité de l'administration du 11 avril 1994 afin d'introduire une plus grande transparence dans l'usage des algorithmes par les administrations, Doc. Parl. *Chambre*, 2020-2021, n° 55.1904/001.

[41] Institut Fédéral pour la protection et la promotion des Droits Humains, https://institutfederaldroitshumains.be, Publications/Avis.

[42] *EDEN* est le réseau d'experts en protection des données d'Europol (***E****uropol* ***D****ata Protection* ***E****xperts* ***N****etwork*).

[43] https://fra.europa.eu/en/speech/2021/data-protection-policing.

Un autre aspect important réside dans les connaissances et le savoir-faire dont dispose la GPI elle-même. Le COC n'est à ce stade nullement rassuré à ce sujet. Il existe au sein de la GPI en général un réel problème d'expertise (connaissances juridiques élémentaires, expertise en technologies de l'information, aptitude numérique, etc.). Il ne serait pas judicieux de s'étendre dans cet avis sur la formation de la police belge, que ce soit pour la fonction de police de base ou pour toutes les formes de formation complémentaire, mais force est d'admettre que la formation qui est dispensée en Belgique est minimale et ne souffre souvent pas la comparaison avec ce qui se fait à l'étranger (la durée limitée de la formation de base permettant d'accéder à la fonction d'inspecteur de police reste à elle seule un problème majeur, alors que l'on pourrait et devrait au fond attendre de chaque membre du cadre de base qu'il ait suivi une formation de bachelier). La FRA insiste elle aussi à juste titre sur ce point : *« We need high degrees of digital literacy, not only in the security communities … »*[44].

24. À cela s'ajoutent en outre les aspects de la sécurité de l'information, qui prennent encore plus d'importance à partir du moment où la police se mettrait massivement à conserver et à traiter des données biométriques. Il serait illusoire de penser que la police ou les services répressifs en général pourraient rester épargnés d'attaques cybernétiques, voire de bévues informatiques involontaires (pensons par exemple à l'attaque cybernétique d'envergure dont a fait l'objet la Défense le 16 décembre 2021[45]). De plus en plus d'administrations sont victimes d'attaques de ce type, comme ce fut le cas encore récemment en France. Là aussi, le constat est que *« les administrations ne cessent d'être ciblées par les cybercriminels pour les informations personnelles qu'elles possèdent »*. Pas moins de 1.964 services publics français ont été en 2021 confrontés à des attaques cybernétiques ou vols de données. L'autorité française de protection des données, la CNIL, a dû sanctionner le ministère de l'Intérieur pour sa gestion automatisée déficiente des empreintes digitales[46].

À cela s'ajoute le fait que la GPI belge utilise de plus en plus des produits de Microsoft, pour lesquels il n'existe de toute manière jamais aucune certitude que les autorités américaines n'ont pas accès aux données susmentionnées. Ces risques existants n'en deviennent que plus grands dès lors que des données à caractère personnel obtenues par la reconnaissance faciale sont massivement enregistrées, données qui – faut-il le répéter ? – comportent des données biométriques non modifiables.

Chaque année, la GPI déclare au COC quelque 30 violations de données, certaines relativement substantielles. Ce fut encore dernièrement le cas en raison de la perte de deux smartphones 'FOCUS' au sein d'une zone de police. Un tel smartphone permet d'accéder à un vaste ensemble de banques de données policières et non policières. Il va dès lors de soi que les conséquences d'atteintes à la sécurité s'en trouvent considérablement aggravées dès lors que des données biométriques comme

---

[44] Ibid., https://fra.europa.eu/en/speech/2021/data-protection-policing.
[45] *« Na 26 dagen kan het leger weer mailen »*, De Standaard, 13 janvier 2022, p. 9 ; *« Cyberaanval op defensie erger dan gedacht », De Morgen*, 13 janvier 2022, p. 7.
[46] Le Monde du 27.12.2021, *Les failles de la protection des données des Français par les pouvoirs publics*, https://journal.lemonde.fr/data/reader.html?xtor=EPR-32.

des photos et des *templates* de personnes physiques se perdent ou sont volées. Les risques augmentent alors dans des proportions exponentielles. Par ailleurs, le vol d'identité est dès à présent un phénomène particulièrement grave et difficile à enrayer qui s'assortit très rapidement de conséquences très lourdes pour les victimes (qui peuvent par exemple soudain être suspectées de faits répréhensibles commis par les voleurs d'identité, avec toutes les retombées que cela implique). On peut sans peine imaginer ce qu'il adviendrait si des données biométriques venaient à être volées également, en grandes quantités ou non…

25. Cette légitimité de la police ne peut être atteinte que si la GPI s'acquitte scrupuleusement de ses obligations en matière d'analyses d'impact relatives à la protection des données (AIPD) et réfléchit bien avant de procéder à des traitements impliquant un risque ; une telle AIPD devra aussi tenir compte spécifiquement du contexte et de l'application, et devra être effectuée avant de procéder concrètement à une application de la technologie de reconnaissance faciale. Cela dit, cette obligation ne peut pas être oubliée non plus au stade de l'élaboration de la réglementation, en particulier lorsqu'il est question de reconnaissance faciale. Toutefois, la réalisation d'une AIPD préalablement à un traitement impliquant un risque est encore loin d'être une évidence au sein de la GPI. Il est au contraire fréquent qu'il n'y soit pas procédé, également lors de la mise en service d'applications informatiques d'envergure. Nous citerons comme exemples frappants le cas des applications/banques de données INFOTHÈQUE et FOCUS. Lors du déploiement actuellement en cours de l'application *police search* également – une sorte de moteur de recherche *Google* propre à la police –, il est apparu que la Direction de l'information policière et des moyens ICT (DRI) de la police fédérale n'avait initialement pas l'intention de procéder à une AIPD.

C.2. Surface portante auprès de la population pour le recours à l'intelligence artificielle et à la technologie de reconnaissance faciale

26. En 2019, la FRA a mené à l'échelle de l'Union européenne une enquête auprès de la population sur la mesure dans laquelle le citoyen serait prêt à accepter le recours à la reconnaissance faciale à des fins d'identification. À peine 17 % des personnes interrogées se sont déclarées ouvertes à cette idée.

La commission consultative éthique « sécurité » annoncée par le ministre pourra sans aucun doute jouer ici un rôle important[47] étant donné qu'elle définira *« … le cadre juridique et opérationnel d'une utilisation responsable, éthique et efficace des technologies et de certaines méthodes de recherche et d'intervention dans le domaine de la sécurité »*[48]. Cette commission devra donc être créée et être opérationnelle avant que la GPI ne puisse ne serait-ce qu'envisager de commencer à utiliser un système de reconnaissance faciale.

[47] Doc. Parl. *Chambre*, 2021-2022, n° 2294/18, p. 6 et 9.
[48] Ibid., p. 16.

C.3. Les problèmes de qualité inhérents de la technologie de reconnaissance faciale

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

C.4. Les droits fondamentaux concernés par le recours à la technologie de reconnaissance faciale

28. Il est clair que le droit au respect de la vie privée et à la protection des données n'est pas la seule dimension qui intervient dans le cadre du recours à la technologie de reconnaissance faciale à des fins répressives. Le thème touche aussi à l'interdiction de la discrimination, à des droits fondamentaux comme la liberté de réunion, la liberté d'expression, la liberté de recevoir et de diffuser des informations, la liberté de religion, etc.[49] ; le *chilling effect* a dans l'intervalle été largement décrit et reconnu.

D. Principes devant encadrer le recours à l'intelligence artificielle et à la technologie de reconnaissance faciale

29. Considérés dans le contexte et appliqués concrètement à l'utilisation de l'intelligence artificielle et de la technologie de reconnaissance faciale par la GPI, les principes suivants doivent absolument être respectés et concrétisés, tant dans la réglementation que dans la pratique :

Licéité

29. La protection des données à caractère personnel qui découle de l'obligation explicite visée à l'article 8, alinéa 1er de la Charte des droits fondamentaux de l'Union européenne revêt notamment une importance pour le droit au respect de la vie privée (lors du traitement de données à caractère personnel, dont les données biométriques) qui est prévu à l'article 7 de ladite Charte[50]. La législation doit définir des règles claires et précises concernant la portée et l'application de la mesure en question

[49] Ibid., https://fra.europa.eu/en/speech/2021/data-protection-policing.
[50] CJUE n° C-594/12, §53.

et offrir des garanties afin que les personnes dont les données sont traitées disposent de suffisamment de garanties protégeant effectivement leurs données à caractère personnel contre le risque d'abus et contre tout accès ou utilisation illicite de ces données[51]. De telles garanties sont encore plus nécessaires lorsque les données à caractère personnel font l'objet d'un traitement automatisé et qu'il existe un risque considérable d'accès illicite aux données, a fortiori lorsqu'il s'agit de données biométriques[52]. Aucune autorité ne peut interférer avec l'exercice de ce droit, sauf si cette ingérence est conforme à la loi et nécessaire, dans une société démocratique, dans l'intérêt de la sécurité nationale, de la sûreté publique et du bien-être économique du pays, pour la défense de l'ordre et la prévention des infractions pénales, pour la protection de la santé ou de la morale, ou encore pour la protection des droits et libertés d'autrui. La Convention européenne des droits de l'homme fixe également des normes quant à la manière dont des restrictions peuvent être imposées. Une exigence de base, en marge de la primauté de la loi (*« rule of law »*), est la **prévisibilité**. Pour répondre à l'exigence de prévisibilité, la loi doit être suffisamment claire que pour fournir aux individus une indication adéquate des circonstances et des conditions dans lesquelles les autorités ont le pouvoir de prendre de telles mesures[53]. Les exigences de qualité que la Cour européenne des droits de l'homme (CEDH) impose à la base légale sont proportionnelles à la gravité de la violation de la vie privée[54].

L'Organe de contrôle rejoint l'*EDPB* et l'*EDPS* dans leur avis de juin 2020 lorsqu'ils déclarent : *« The use of AI in the area of police and law enforcement requires area-specific, precise, foreseeable and proportionate rules that need to consider the interests of the persons concerned and the effects on the functioning of a democratic society. »*[55].

Lorsqu'elle a trait à l'utilisation de la *FRT* par les services de police, la législation devra également tenir compte des différentes finalités et applications poursuivies :

- pour la GPI, cela signifie qu'elle ne devra pas uniquement tenir compte des traitements de données opérationnels au sens de la *LED*, mais devra par exemple réglementer également l'utilisation de la *FRT* à des fins internes de la GPI et dans le cadre du RGPD (contrôle interne, finalités disciplinaires, contrôle d'accès interne pour les collaborateurs, etc.). *De lege lata*, l'utilisation de données biométriques comme la reconnaissance faciale ou les empreintes digitales n'est en effet pas autorisée dans le contexte du RGPD.

[51] CJUE n° C-594/12, §54 ; concernant l'article 8 de la Convention européenne des droits de l'homme, voir aussi CEDH, Liberty and Others contre le Royaume-Uni, 1er juillet 2008, n° 58243/00, §§ 62 et 63 ; Rotaru contre la Roumanie, §§ 57 à 59 inclus et S. and Marper contre le Royaume-Uni, §99.
[52] CJUE n° C-594/12, §55 ; concernant l'article 8 de la Convention européenne des droits de l'homme, voir aussi CEDH, S. and Marper contre le Royaume-Uni, §103 et M. K. contre la France, 18 avril 2013, n° 19522/09, §35.
[53] CEDH, Copland contre le Royaume-Uni, 3 avril 2007, n° 62617/00, §46.
[54] CEDH, Gaughran contre le Royaume-Uni, 13 février 2020, n° 45245/15 ; CEDH, P.N contre l'Allemagne, 11 juin 2020, n° 74440/17 ; CEDH, S. and Marper contre le Royaume-Uni, 2 décembre 2008, n° 30562/04 et 30566/04.
[55] EDPB-EDPS Joint Opinion 5/2021 on the proposal for a regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (Artificial Intelligence Act), 18 June 2021, https://edps.europa.eu/Opinions | European Data Protection Supervisor (europa.eu), p. 10, n° 27.

- Un autre point d'attention a trait à la problématique de la 'catégorisation' (sexe, couleur de peau, émotions, …) qui découle de la *FRT*. Bien que le but premier de la *FRT* soit dans le contexte de la GPI l'« identification », il peut aussi être question d'une catégorisation. Bien que le but de la catégorisation ne soit pas en soi axé sur l'identification en tant que telle, il sera généralement au moins question d'une possibilité d'identification indirecte. Or, le COC est d'avis que le recours à la *FRT* en vue de la reconnaissance d'émotions uniques peut revêtir un intérêt par exemple dans le cadre de l'enregistrement d'une audition (cf. utilisation du détecteur de mensonges). Une lecture stricte de l'article 44/1 §2, 1° de la LFP semble *de lege lata* exclure ce type de catégorisation étant donné que les données biométriques ne peuvent en principe être utilisées actuellement que dans le but « *d'assurer l'identification certaine* » de la personne concernée. Vu sous cet angle, le recours à la *FRT* à des fins de catégorisation (par exemple pour détecter des émotions) est *de lege lata* exclu à l'heure actuelle, ou du moins tel semble être le cas (en tout cas dans la LFP). Il va donc falloir évaluer si l'on veut permettre une telle application de la *FRT*, auquel cas le cadre légal actuel devra être modifié. D'un autre côté, l'article 44/1 §2, 1° de la LFP ne semble pas exclure le recours à la *FRT* en vue de la reconnaissance de caractéristiques comportementales uniques si cet aspect est réglementé plus concrètement dans la LFP. Bien que ce type de traitement biométrique puisse être considéré comme une forme de catégorisation, il s'agit cependant bel et bien d'une 'identification'. Prenons un exemple pour illustrer ce propos. Une attaque de banque ou un cambriolage à main armée est commis(e). Les victimes n'ont pas eu l'occasion de voir – ni a fortiori de reconnaître – le visage des auteurs, mais ont par contre remarqué quelques caractéristiques physiques ou comportementales frappantes, comme une certaine corpulence de la personne ou sa démarche. La police pourrait envisager de recourir à la *FRT* pour retrouver les auteurs… Le COC estime que de telles applications devraient être autorisées dans le contexte d'une information à condition, comme nous le disions, d'être prévues dans une base légale claire et spécifique et accompagnées des garanties requises. À moins que l'objectif des auteurs de la résolution ne soit de soumettre également cette forme de recherche 'ciblée' à un moratoire, voire de l'interdire complètement ?

Il s'agit là d'exemples de recours à la *FRT* impliquant un traitement de (types de) données biométriques spécifiques pour lequel 1) les circonstances et les conditions dans lesquelles les données biométriques spécifiques sont traitées et 2) les exigences technologiques spécifiques auxquelles le système d'intelligence artificielle doit répondre soulèvent de nombreuses questions et ne peuvent pas être dûment réglementées par une seule disposition légale générale (comme le fait actuellement l'article 44/1 §2, 1° de la LFP, s'agissant là d'un problème auquel les auteurs du nouvel article 44/1 §2, 1° de la LFP n'ont peut-être pas pensé en 2019[56]).

[56] La base juridique permettant à la GPI de traiter des données biométriques a été introduite par la loi du 22 mai 2019 modifiant diverses dispositions en ce qui concerne la gestion de l'information policière.

Nécessité et proportionnalité

30. Toute technologie de reconnaissance faciale ou tout système de reconnaissance biométrique devra passer avec succès le test de la nécessité et de la proportionnalité. Un traitement ne peut être considéré comme 'strictement nécessaire' que si les dérogations à la protection des données à caractère personnel et les limitations de celle-ci s'opèrent dans les limites du strict nécessaire[57]. L'ajout du terme 'strict' signifie que le législateur n'autorise le traitement de catégories particulières de données (comme les données biométriques) que dans des conditions encore plus strictes que celles imposées pour la nécessité 'ordinaire'. C'est encore plus vrai dans le cas de traitements automatisés.

Pour faciliter et mettre en œuvre l'évaluation de la nécessité et de la proportionnalité de mesures législatives régissant la reconnaissance faciale à des fins répressives, le législateur national et le législateur européen peuvent d'ores et déjà recourir aux instruments pratiques disponibles qui ont été conçus spécialement à cet effet, comme la *toolkit* et les directives de l'*EDPS*[58].

Transparence technologique

31. L'actuel manque de transparence technologique des systèmes d'intelligence artificielle et des algorithmes utilisés est sans aucun doute l'un des principaux obstacles.

Le directeur de la FRA formule cela en ces termes : *« It means we need to know what is in the algorithms. We need to know the content of machine training data. And again, the point needs to be made repeatedly and loudly, because, there is a pushback from parts of the industry. We are hearing voices, for instance, saying it is too difficult, it is too complicated, it is too hard to understand and therefore we cannot deliver on transparency. »*. L'Organe de contrôle se rallie à ce point de vue, à

---

[57] Jurisprudence établie relative au droit fondamental au respect de la vie privée ; voir e.a. CJUE n° C73/07, Satakunnan Markkinapörssi and Satamedia, §56 ; CJUE n° C92/09 et C93/09, Schecke and Eifert, §§ 74, 77 et 86 ; CJUE n° C/293/12 et C/594/12, Digital Rights, §§ 46, 52, 56, 62, 64 et 65 ; CJUE n° C/362/14, Schrems, §§ 92 et 93 ; CJUE n° C/311/18, Schrems, §§ 167 et 176. Voir par exemple, dans ce dernier arrêt n° C/311/18 : *« Enfin, pour satisfaire à l'exigence de proportionnalité selon laquelle les dérogations à la protection des données à caractère personnel et les limitations de celle-ci doivent s'opérer dans les limites du strict nécessaire, la réglementation en cause comportant l'ingérence doit prévoir des règles claires et précises régissant la portée et l'application de la mesure en cause et imposant des exigences minimales, de telle sorte que les personnes dont les données ont été transférées disposent de garanties suffisantes permettant de protéger efficacement leurs données à caractère personnel contre les risques d'abus. Elle doit en particulier indiquer en quelles circonstances et sous quelles conditions une mesure prévoyant le traitement de telles données peut être prise, garantissant ainsi que l'ingérence soit limitée au strict nécessaire. La nécessité de disposer de telles garanties est d'autant plus importante lorsque les données à caractère personnel sont soumises à un traitement automatisé. ».*

[58] *« Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A toolkit »* (11.4.2017) ; voir aussi « *EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data »* (19.12.2019), www.edps.europa.eu.

l'instar de l'IFDH qui souligne l'importance de la transparence, en particulier au regard de la capacité d'apprentissage autonome des traitements algorithmiques[59].

32. Le COC constate d'ailleurs trop souvent dans la pratique que les collaborateurs de terrain de la GPI ne sont pas suffisamment, voire pas du tout en mesure d'expliquer le fonctionnement des moyens technologiques qu'ils utilisent, voire ne le comprennent pas vraiment eux-mêmes. C'est déjà le cas pour les traitements actuels 'ordinaires' des caméras, et ce problème ne fera que s'aggraver avec l'introduction de systèmes de reconnaissance faciale complexes recourant à des algorithmes. Les enquêtes que le COC a déjà menées au cours de ses trois années d'existence (depuis qu'il est également une autorité de protection des données spécialisée) dans des matières dans lesquelles il est recouru – *contra legem* – à la technologie de reconnaissance faciale, à savoir l'enquête menée auprès de la police de l'aéroport de Bruxelles-National (DGA/LPA) et l'enquête menée au sujet de l'utilisation de la technologie *Clearview* par la Direction centrale de la lutte contre la criminalité grave et organisée (DJSOC) de la Direction Générale Judiciaire de la police fédérale, le montrent de manière éclatante.

Dans le contexte de l'intelligence artificielle et de la technologie de reconnaissance faciale, cette transparence à l'égard du sujet de droit signifie également *« the dimension of making people aware that they have been subject to the application of technology that has impacted their life »*[60]. Cet aspect devra d'une manière ou d'une autre être lui aussi concrétisé dans la réglementation et dans la pratique.

D. Rôle et importance de l'autorité de contrôle

33. L'efficacité des autorités de protection des données gagnera encore en importance dans le contexte du déploiement de toutes sortes de systèmes de reconnaissance biométrique de personnes physiques (reconnaissance faciale), a fortiori dans un contexte de répression. Le COC fait référence au surplus au rôle futur de ces autorités de protection des données, dont l'Organe de contrôle lui-même, dans le cadre du contrôle des systèmes d'intelligence artificielle tel que prévu par l'*AIA*. L'*AIA* dispose en son article 59.1 que *« des autorités nationales compétentes* [doivent être] *établies ou désignées par chaque État membre aux fins d'assurer l'application et la mise en œuvre du présent règlement »*. Dans leur avis commun, l'*EDPB* et l'*EDPS* plaident pour que « *DPAs should be designated as the national supervisory authorities pursuant to Article 59 of the Proposal »*[61]. Le directeur de la FRA, Michael O'Flaherty, cite lui aussi l'importance du rôle de l'autorité de contrôle en tant que 5e principe essentiel à appliquer avant d'envisager le déploiement de l'intelligence artificielle et de la

[59] Institut Fédéral pour la protection et la promotion des Droits Humains, https://institutfederaldroitshumains.be, Publications/Avis, p. 10.
[60] Ibid., https://fra.europa.eu/en/speech/2021/data-protection-policing.
[61] EDPB-EDPS Joint Opinion 5/2021 on the proposal for a regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (Artificial Intelligence Act), 18 June 2021, https://edps.europa.eu/Opinions | European Data Protection Supervisor (europa.eu), voir p. 14 et 15, n° 47 et 48.

technologie de reconnaissance faciale : *« Fifth, we need independent oversight of the use of high-risk technologies. ... Oversight bodies also need to be given adequate resources and training. »*[62].

34. C'est surtout ce dernier aspect des moyens humains et matériels suffisants qui est important et qui inquiète le COC. Depuis sa relance en 2018, à l'occasion de laquelle il s'est vu confier une mission additionnelle en tant qu'autorité de protection des données spécialisée pour la police et a repris ces tâches et dossiers de l'APD, le COC n'a jamais demandé de ressources supplémentaires alors que de nombreuses tâches additionnelles lui ont été attribuées en peu de temps et que la quantité de dossiers augmente de toute façon d'année en année. Le citoyen est en effet manifestement de plus en plus conscient de ses droits en général et de son droit au respect de la vie privée et à la protection des données en particulier – également en matière répressive –, ce qui est évidemment une évolution très positive en soi mais pose immanquablement problème au niveau des moyens humains et matériels mis à disposition. Pour illustrer ce constat, il suffit de faire référence aux deux rapports annuels déjà publiés par le COC (2016-2019 et 2020). Pour 2021, nous ne citerons qu'un seul chiffre : le COC a recensé pas moins de 547 demandes d'accès indirect aux banques de données policières en 2021, s'agissant de dossiers réactifs qui monopolisent une part importante de la capacité. Ce chiffre a donc pour ainsi dire doublé par rapport à 2020 et représente de toute façon une augmentation substantielle par rapport aux trois années précédentes, comme le montre le tableau ci-dessous :

Année	**Nombre de dossiers d'accès indirect**
2018	333
2019	392
2020	283
2021	547

L'effectif du COC n'a pas changé depuis sa relance le 5 septembre 2018, et le COC n'a pas non plus obtenu de crédits supplémentaires. Les augmentations substantielles des volumes que nous évoquions ont donc toujours été prises en charge avec les moyens existants en tentant d'améliorer en permanence l'efficacité, en établissant davantage de priorités et en prenant moins d'initiatives proactives, mais ce système se heurte dans l'intervalle à ses limites. Nous pensons aussi à la nouvelle compétence particulièrement importante que le COC devra bientôt assumer dans le cadre de la nouvelle législation sur la rétention des données (à savoir le contrôle des statistiques sur la base desquelles la conservation des données de téléphonie sera fixée du point de vue territorial et la vérification des requêtes adressées aux opérateurs par la cellule Disparitions de la police fédérale)[63].

[62] Soulignement propre de l'Organe de contrôle.

[63] Communiqués de presse du Conseil des ministres, « Conservation des données d'identification et des métadonnées dans le secteur des communications électroniques - Deuxième lecture », https://news.belgium.be/fr ; voir aussi l'avis DA210014 du COC du 21 mai 2020 relatif à un avant-projet de loi relatif à la collecte et à la conservation des données d'identification, de trafic et de localisation dans le secteur des communications électroniques et à leur accès par les autorités et à un projet d'arrêté royal modifiant l'arrêté royal du 19 septembre 2013 portant exécution de l'article 126 de la loi du 13 juin 2005 relative aux communications électroniques, www.organedecontrole.be.

En marge de la quantité importante de dossiers de contrôle indirect (qui augmentera sans aucun doute encore lors du déploiement de la technologie de reconnaissance faciale), il convient de faire état d'une évolution plus ou moins similaire du nombre de dossiers purement réactifs, dont :

- les avis généraux en matière de protection des données, d'utilisation de caméras et autres ;
- les avis sur les AIPD dans le sillage des AIPD déclarées ;
- les violations de données déclarées ;
- les notifications d'utilisations non visibles de caméras ;
- les avis sur la législation et la réglementation ;
- les procédures judiciaires (s'agissant actuellement de trois procédures dans lesquelles le COC doit consentir lui-même un investissement particulièrement substantiel en raison de la matière très spécialisée) ;
- les plaintes ;
- …

35. À cela viennent s'ajouter les contrôles globaux propres (proactifs) effectués soit d'office, soit à la demande d'instances administratives ou judiciaires, qui souffrent de plus en plus de l'afflux des dossiers réactifs (mais qui constituent ou devraient tout de même constituer l'activité principale du COC). Le COC mène notamment à la demande du procureur du Roi une enquête de contrôle d'envergure au sein d'une zone de police de Flandre occidentale, travaille d'arrache-pied à l'enquête 'Salduz' demandée par les ministres de l'Intérieur et de la Justice, qui est menée à l'échelle de toute la GPI sur l'utilisation de caméras et d'enregistrements audio dans le cadre de la concertation confidentielle entre l'avocat et son client, et finalise enfin l'enquête *Clearview* dont nous parlions plus haut. Les enquêtes de ce type nécessitent une capacité (technique) importante. L'unique (1) informaticien dont dispose actuellement le COC ne parvient vraiment pas à faire face à cette charge de travail, notamment parce qu'il doit consacrer trop de temps à l'environnement ICT propre du COC. Le nombre de fonctionnaires de police faisant partie du COC (deux) est insuffisant également. Cette énumération fait d'ailleurs abstraction de toutes sortes de demandes visant à dispenser des formations à la GPI (par ex. aux aspirants-commissaires ou aux candidats titulaires du brevet de commissaire principal), à venir en aide à des étudiants dans le cadre de formations de bachelier ou de master, à prendre part à de nombreuses réunions techniques et de sensibilisation avec les corps de la GPI eux-mêmes, etc. À cela se sont encore ajoutées ces dernières années des missions qui soit sont déjà en cours d'exécution (par ex. le contrôle des réquisitions adressées par la douane à la *BELPIU*, le contrôle de la banque de données commune terrorisme, le contrôle général du fonctionnement de la *BELPIU*, …), soit seront introduites dans le sillage d'une politique déjà décidée (par ex. le PV électronique[64]), soit seront introduites dans le sillage d'une politique sur le point d'être adoptée (par

[64] Arrêté royal du 18 juillet 2021 relatif aux mesures de sécurité et aux normes techniques minimales des systèmes informatiques policiers qui produisent le cachet électronique avancé et aux mentions qui figurent dans le cachet électronique avancé et dans la signature électronique qualifiée, M.B. 13.08.2021. Le rapport d'audit – relatif aux mesures de sécurité et aux normes techniques minimales des systèmes informatiques policiers qui produisent le cachet électronique avancé, qui doivent permettre d'assurer un niveau de confidentialité, de disponibilité, d'intégrité, de fiabilité, d'authenticité et d'irréfutabilité du

exemple la mission dans le cadre de la rétention des données de téléphonie), soit pourraient voir le jour (le recours à la technologie de reconnaissance faciale à des fins policières).

36. À titre de comparaison, l'Autorité de protection des données (APD) est passée en 3 ans d'une dotation d'environ 5.500 KEUR à une dotation de plus de 9.064 KEUR (soit près du double) et a pu recruter à l'avenant. L'Organe de contrôle en est toujours à sa dotation de 1.288 KEUR de septembre 2018 (alors que ses dépenses réelles s'élèvent à 1.696 KEUR). À elle seule, la masse salariale des onze membres et membres du personnel (3 membres du Comité de direction et 8 membres du personnel) absorbe toute la dotation octroyée par le Parlement. Le reste des dépenses (fonctionnement et investissements) est financé au moyen des réserves restantes accumulées dans le passé (dans le sillage du départ de membres du personnel qui n'ont pas été remplacés ou ne l'ont été qu'avec beaucoup de retard, et de postes vacants auxquels il n'a tout simplement pas été pourvu), mais ces réserves diminuent rapidement et ne tarderont pas à s'épuiser. Le COC a donc grand besoin d'une injection supplémentaire de moyens.

37. Il est essentiel que le citoyen qui subit dans ses droits ou dans son statut juridique l'impact d'une application de l'intelligence artificielle ou de la technologie de reconnaissance faciale dispose d'une solution efficace. Pour cette raison également, l'autorité de contrôle doit disposer de suffisamment de moyens humains et matériels, également en termes de ressources informatiques et d'expertise numérique. En sa qualité d'autorité de contrôle, le COC doit lui aussi disposer en interne de l'expertise technique requise. Pour toutes ces raisons, le COC tient à attirer l'attention du Parlement sur la nécessité, pour le COC, de disposer de suffisamment d'experts et de ressources (et en particulier de davantage d'expertise technique en matière de TIC et d'expertise numérique).

E. Conclusion

38. Le COC peut en tout cas adhérer à la résolution lorsque celle-ci indique que *« tous ces éléments plaident en faveur d'une grande prudence quant à l'implémentation en Belgique de tels systèmes de surveillance par caméras à reconnaissance faciale »*[65]. Il convient donc de se demander s'il est judicieux ou opportun de déjà légiférer au niveau national (belge) – du moins dans le but de parvenir à une législation définitive en matière d'intelligence artificielle ou de technologie de reconnaissance faciale – avant que le texte définitif du règlement européen sur l'intelligence artificielle n'ait été arrêté. En tout état de cause, une éventuelle législation nationale devra céder la place à la norme de droit internationale supérieure qu'est un règlement européen et en tenir compte. Et de toute façon, le législateur national ne pourra plus entreprendre de démarches juridiques pour les aspects qui ont été explicitement réglementés par le règlement européen. Si donc l'*AIA* venait par exemple à prévoir une

service de signature électronique de la police – doit être transmis par la police fédérale à l'Organe de contrôle de l'information policière qui pourra également lui-même évaluer ces mesures et normes techniques (voir l'article 10 de l'arrêté royal et le point I « Considérations générales » du Rapport au Roi).

[65] Résolution, p. 13

interdiction générale de toute forme de reconnaissance faciale en temps réel dans les lieux publics, la loi belge ne pourra évidemment plus prévoir le recours à une telle technologie. En outre, on ne saurait exclure le risque que les deux textes présentent des différences insurmontables ou que des investissements consentis en vertu de la législation nationale deviennent sans objet en raison du cadre européen plus restrictif ou, à l'inverse, que l'on néglige de consentir des investissements parce qu'un cadre national, contrairement à la réglementation européenne, ne permet pas certaines applications.

Le COC est dès lors d'avis qu'une initiative législative belge, sous réserve d'un cadre à créer concernant les environnements de test ou les projets pilotes (voir plus loin), n'est **pas** indiquée et qu'il est donc **opportun de mettre en place un moratoire sur une intervention législative prématurée, ou du moins sur son application effective avant un délai à déterminer**. Ce point de vue rejoint également l'appel lancé par l'*EDPB* et l'*EDPS*.

En ce sens, le COC est tout de même d'un avis quelque peu différent de celui de l'IFDH, qui estime *« qu'il est nécessaire que le législateur fédéral envisage au plus vite*[66] *une proposition de législation garantissant la transparence quant à l'emploi de systèmes d'intelligence artificielle par l'ensemble des autorités publiques fédérales, et non seulement par les autorités administratives »*[67]. En ce qui concerne la police, le COC est plutôt favorable au moratoire proposé dans la résolution sous réserve de ce que nous prévoyons ci-après pour les projets pilotes ainsi que du délai à prévoir. Par ailleurs, le COC plaide en tout état de cause pour une réglementation ou législation spécifique pour les finalités répressives en général, et a fortiori pour les finalités policières en particulier.

39. Une deuxième question est de savoir s'il y a lieu aussi de geler toute utilisation purement réactive de la *FRT* à des fins d'information, dans l'hypothèse où il existerait un cadre légal adéquat. Le COC est à ce sujet d'un avis plus nuancé. Dans le cadre d'une enquête préliminaire menée en matière pénale par le parquet ou le juge d'instruction, le COC estime qu'il doit être possible d'identifier et/ou d'authentifier les auteurs ou les victimes en recourant à la technologie de reconnaissance faciale. L'enquête *Clearview* a prouvé pour autant que nécessaire – *quod non* – l'ampleur (aussi internationale) des problèmes et défis posés par la détection et la poursuite par exemple de la pédopornographie et de la pédophilie. Cela dit, d'autres phénomènes comme la traite des êtres humains et la criminalité organisée pourraient sans nul doute constituer également des domaines importants (aussi à des fins d'identification des victimes). Le COC estime donc qu'il n'est que légitime, dans un tel contexte, de se mettre en quête d'outils permettant d'obtenir de meilleurs résultats (dans le cadre de l'information ou de l'instruction). Moyennant l'élaboration d'une législation claire et la mise en place des contrôles et bilans requis, avec une autorité de contrôle de la protection des données et moyennant l'intervention

[66] Soulignement du COC.
[67] Institut Fédéral pour la protection et la promotion des Droits Humains, https://institutfederaldroitshumains.be, Publications/Avis, p. 9, recommandation 4.

du magistrat, et compte tenu des limites prévues par la procédure pénale belge (qui doivent éventuellement être définies), une telle possibilité doit certainement pouvoir être envisagée.

40. La troisième question est de savoir si cela signifie qu'il y a lieu de geler toute forme d'environnement de test, phase de test ou projet pilote recourant à la technologie de reconnaissance faciale. Ici aussi, le COC a un avis nuancé. Le COC est en principe lui-même favorable à un tel cadre réglementaire restrictif. Il est en effet établi que l'on dispose encore de très peu de matériel d'évaluation objectif concernant l'utilisation de cette technologie. Seule une application expérimentale dans la pratique permettra de surmonter cet obstacle majeur qui fait que personne n'a vraiment une idée de la valeur ajoutée ni de la performance de tels systèmes. Cela signifie toutefois que la GPI, sous des conditions strictes et moyennant la transparence requise, devrait pouvoir tester cette technologie sur des données réelles sans d'emblée se retrouver dans l'illégalité. Le degré de violation de la vie privée induit par l'application de la *FRT* à des photos, par exemple, de suspects et de victimes qui sont traitées conformément aux conditions légales de la LFP (et éventuellement du Code d'instruction criminelle) est en effet d'un autre ordre que celui induit par l'application non ciblée de la *FRT* dans des lieux publics.

41. La proposition d'*AIA* prévoit en ses articles 53 et suivants la création de « bacs à sable réglementaires de l'intelligence artificielle ». Cette réglementation doit offrir un environnement contrôlé qui facilite le développement, la mise à l'essai et la validation de systèmes d'intelligence artificielle innovants. Ces bacs à sable réglementaires de l'intelligence artificielle n'ont pas d'incidence sur les pouvoirs des autorités compétentes en matière de contrôle et de mesures correctives. Tout risque significatif pour la santé, la sécurité et les droits fondamentaux constaté lors du développement et des tests de ces systèmes donne lieu à des mesures d'atténuation immédiates et, à défaut, à la suspension du processus de développement et d'essai jusqu'à ce que cette atténuation soit effective (article 53.3). Les modalités et les conditions de fonctionnement des bacs à sable réglementaires de l'intelligence artificielle, y compris les critères d'admissibilité et la procédure de demande, de sélection, de participation et de sortie du bac à sable, ainsi que les droits et obligations des participants sont définis dans des actes d'exécution de la Commission européenne (article 53.6). L'article 54.1 (a) i) prévoit la possibilité d'appliquer également ces bacs à sable réglementaires de l'intelligence artificielle à des fins répressives, même s'il fait référence à la législation nationale applicable (qui doit donc encore être élaborée dans le cas de la Belgique). L'article 54.1 (c) dispose qu'il doit exister *« des mécanismes de suivi efficaces pour déterminer si des risques élevés pour les droits fondamentaux des personnes concernées sont susceptibles de survenir lors de l'expérimentation menée dans le cadre du bac à sable, ainsi qu'un mécanisme de réponse permettant d'atténuer rapidement ces risques et, le cas échéant, de faire cesser le traitement des données ».* Le rôle décisif et l'importance de l'autorité de contrôle sont donc ici aussi mis en avant.

42. Bien que l'on puisse donc s'attendre à une réglementation européenne concernant ces « bacs à sable » ou environnements de test, on peut se demander si le législateur belge doit attendre que cette réglementation voie le jour. Quoi qu'il en soit, ces environnements de test devront également disposer d'une base légale nationale. L'utilité et la nécessité des tests semblent indiscutables pour le COC. Ce n'est en effet qu'après un nombre suffisant de phases de test et d'essais que l'on pourra se faire une meilleure idée des pourcentages de faux positifs et de faux négatifs, du type de biais qui surviennent, des restrictions ou autres garanties nécessaires, etc. Ces enseignements pourront et devront alors être pris en compte dans la législation nationale (ou européenne) définitive. Comme l'ont indiqué à juste titre l'*EDPB* et l'*EDPS* dans leur avis, cette législation nationale relèvera toutefois entièrement du RGPD en ce qui concerne l'utilisation de traitements relevant de la *LED* et de données à caractère personnel dans l'environnement de test[68]. Pour ce qui est de la GPI, le COC restera toutefois l'autorité de contrôle compétente.

43. Le COC est dès lors partisan de la mise au point d'un cadre législatif national propre et propose donc de ne pas attendre l'arrivée éventuelle d'une réglementation européenne sur les environnements de test pour prévoir leur utilisation par la police intégrée. Le COC pourra jouer un rôle dans ce cadre, par exemple à travers un système d'autorisation préalable qui requiert évidemment une étude et une mise au point plus détaillées.

PAR CES MOTIFS,

l'Organe de contrôle de l'information policière

prie le demandeur de prendre connaissance de tous les éléments du présent avis.

Avis approuvé par l'Organe de contrôle de l'information policière le 24 janvier 2022.

Pour l'Organe de contrôle,

Le Président,
Philippe ARNOULD

[68] EDPB-EDPS Joint Opinion 5/2021 on the proposal for a regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (Artificial Intelligence Act), 18 June 2021, https://edps.europa.eu/Opinions | European Data Protection Supervisor (europa.eu), voir p. 18, n° 66.