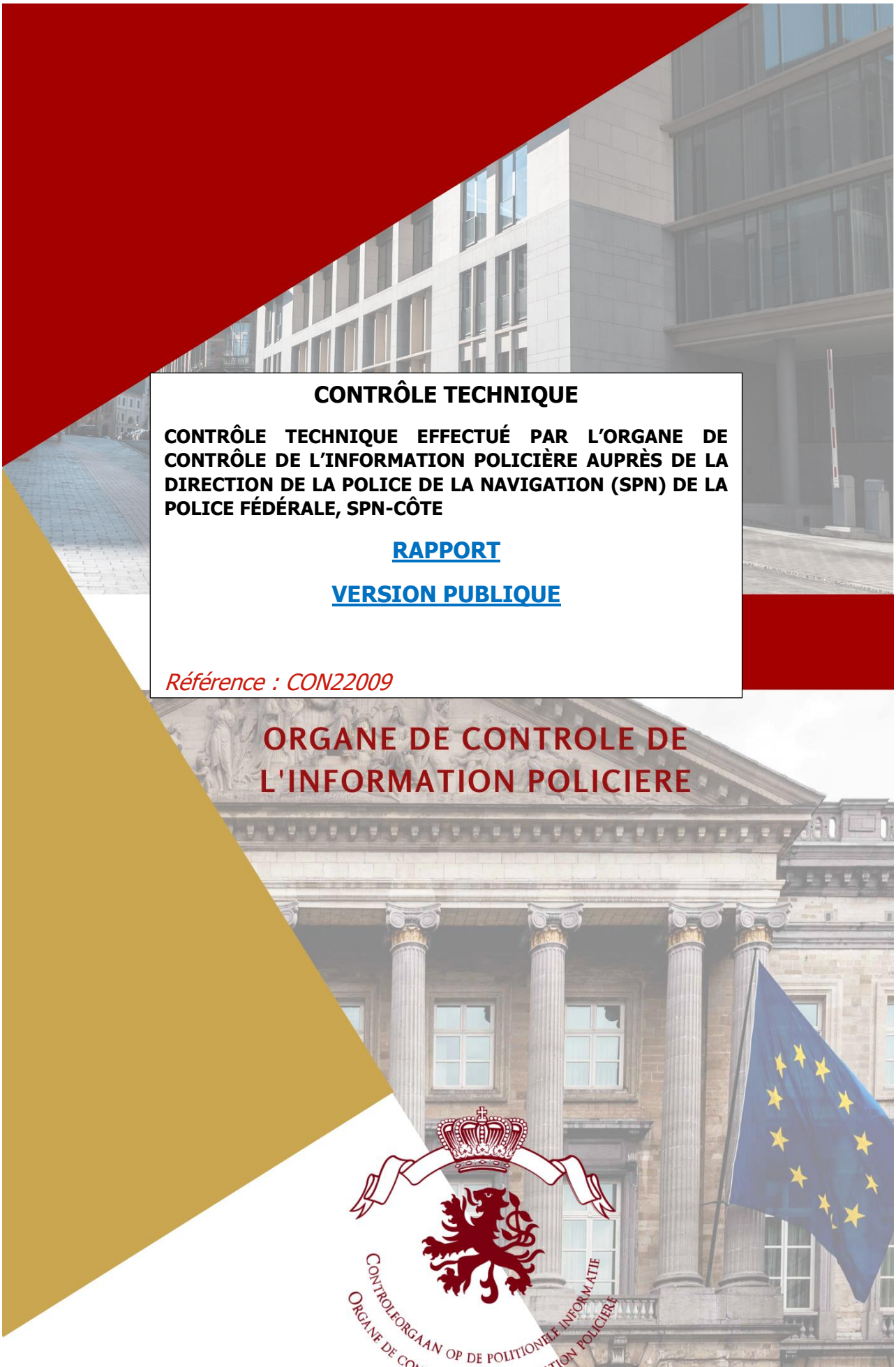
Le présent rapport est la version publique du rapport de contrôle.

Cela signifie qu'il ne comporte pas ou pas nécessairement tous les éléments ou passages figurant dans le rapport de contrôle adressé aux destinataires. Certains éléments ou passages ont été omis ou anonymisés. Il peut y avoir diverses raisons à cela, qui peuvent être de nature légale ou être dictées par des motifs d'opportunité : la volonté de ne pas divulguer des techniques ou tactiques policières, le secret de l'enquête, le secret professionnel, le fait qu'un manquement a été résolu dans l'intervalle, etc.



CONTRÔLE TECHNIQUE

CONTRÔLE TECHNIQUE EFFECTUÉ PAR L'ORGANE DE CONTRÔLE DE L'INFORMATION POLICIÈRE AUPRÈS DE LA DIRECTION DE LA POLICE DE LA NAVIGATION (SPN) DE LA POLICE FÉDÉRALE, SPN-CÔTE

RAPPORT

VERSION PUBLIQUE

Référence : CON22009

Table des matières

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

La loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel (LPD)[1] a réformé l'Organe de contrôle en une autorité de contrôle à part entière. L'article 71 §1er et les Titres 2 et 7 de la LPD décrivent les missions et les compétences du COC. Il est dans ce contexte fait référence par ailleurs aux missions de contrôle visées aux articles 44/1 à 44/11/14 inclus de la LFP, relatifs à la gestion de l'information par les services de police. L'Organe de contrôle est ainsi investi d'une mission de surveillance et de contrôle, ce qui signifie qu'en marge de la protection de la vie privée et des données, le COC prête également attention à des éléments comme l'efficacité de la gestion de l'information et de l'intervention policière. En vertu de la réglementation susmentionnée, le COC dispose dès lors d'une compétence de surveillance générale à l'égard de tous les traitements de données (à caractère personnel) opérationnels et non opérationnels effectués par la GPI.

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

Dans ce cadre, le COC procède aux constatations et peut formuler des questions, des requêtes ou des recommandations et, en tant que *« ultimum remedium »*, imposer des mesures correctrices (au caractère contraignant) si le COC constate des infractions à la réglementation applicable.

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

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

Dans le cadre de l'utilisation de caméras non visibles, l'Organe de contrôle fonctionne en quelque sorte comme une commission « MAP »[2]. Conformément à l'article 46/6 de la LFP, toute autorisation et prolongation d'utilisation non visible de caméras dans les cas visés à l'article 46/4 doit être notifiée à l'Organe de contrôle sauf lorsque l'utilisation des caméras est réalisée sous le contrôle d'un magistrat. L'Organe de contrôle doit alors examiner si les conditions pour la décision, la prolongation ou l'exécution de cette mesure sont remplies.

L'Organe de contrôle prend en outre connaissance des plaintes et statue sur leur bien-fondé[3]. Les membres et les membres du personnel de l'Organe de contrôle[4] disposent à cet égard de compétences d'investigation, après quoi le comité de direction de l'Organe de contrôle peut, en marge des requêtes et recommandations qu'il formule, prendre également des mesures correctrices[5].

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') visée dans la loi du 15 mai 2007 *« sur l'Inspection générale et portant des dispositions diverses relatives au statut de certains membres des services de police »* et de l'Unité d'information des passagers (ci-après dénommée en abrégé 'BELPIU') visée au Chapitre 7 de la loi du 25 décembre 2016 *« relative au traitement des données des passagers »*, 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 44/11/14 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].

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

---

[1] M.B. 5 septembre 2018. Cette loi contient des dispositions qui donnent exécution au 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), ci-après dénommé « RGPD », et à la Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou 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 LED (**L**aw **E**nforcement **D**irective)).

[2] MAP signifie « ***M****éthodes* ***A****dministratives* ***P****articulières* ».

[3] Art. 240, 4° de la LPD.

[4] À savoir les membres du personnel du **D**ienst **O**nderzoeken / **S**ervice d'Enquête (DOSE) et du secrétariat, c'est-à-dire des juristes et des experts en matière de TIC.

[5] Art. 244 (compétences d'investigation des membres et des membres du personnel) et 247 de la LPD (mesures correctrices à prendre par le comité de direction (DIRCOM) du COC) ; pour les pleines compétences d'investigation des membres, voir en particulier aussi Cass., 6 novembre 2023, n° C23.0092/N, www.juportal.be.

[6] Article 71 §1er, troisième alinéa *juncto* article 236 §3 de la LPD.

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 »*.

Enfin, l'Organe de contrôle est également chargé, dans le cadre de la législation sur la rétention des données et en vertu de l'article 126/3 §1er, 8e alinéa de la loi du 13 juin 2005 relative aux communications électroniques (ci-après 'la LCE')[7], de la validation (ou non) des statistiques relatives au nombre de faits punissables et au délai de conservation pour chaque arrondissement judiciaire et chaque zone de police, une matière dans le cadre de laquelle il exerce toutes les compétences qui lui ont été attribuées par le Titre 7 de la LPD. Il est par ailleurs également chargé, en application de l'article 42 §3, 2e et 3e alinéas de la LFP, du contrôle des requêtes de la Cellule Personnes disparues de la police fédérale en vue de la consultation des données relatives aux communications électroniques impliquant la personne disparue.

Un recours juridictionnel peut être introduit dans les trente jours contre certaines décisions de l'Organe de contrôle devant la Cour d'appel du domicile ou du siège du demandeur qui traite l'affaire selon les formes du référé conformément aux articles 1038, 1040 et 1041 du Code judiciaire[8].

1. INTRODUCTION

1. Dans le cadre de ses compétences d'autorité de contrôle à l'égard des traitements de données effectués par la police intégrée organisée à deux niveaux (GPI), l'Organe de contrôle a décidé d'effectuer un contrôle technique auprès de la Direction de la police de la navigation (SPN), sections X et Y (ci-après 'la SPN-Côte'). Le présent rapport présente les conclusions de l'enquête menée dans le cadre de ce contrôle technique. Les conclusions, requêtes, recommandations et mesures correctrices découlent de ces constatations et sont par conséquent adressées aux responsables fonctionnels de la police aux niveaux politique et opérationnel.

2. OBJET DE LA VISITE ET MÉTHODOLOGIE

2. Le 24.05.2023, le COC a réalisé de sa propre initiative un 'contrôle technique' auprès de la SPN-Côte. Ce contrôle ne faisait donc pas suite à une plainte (individuelle) ni ne découlait de l'existence d'indications (concrètes) d'un non-respect, par la direction de police contrôlée, de la législation et de la réglementation.

3. À travers ce contrôle technique, le COC aspire à se faire une idée des processus de travail de la direction dans le cadre de la gestion de l'information policière. Le contrôle technique du COC a été limité aux thèmes suivants :

- Utilisation de caméras :
  - finalité ;
  - type (fixes/mobiles/fixes temporaires/intelligentes) ;
  - lieux d'utilisation ;
  - utilisation visible/non visible ;
  - délais de conservation ;
  - autorisations.

- Banques de données opérationnelles, dont les banques de données particulières :
  - finalité ;
  - processus d'alimentation ;
  - relation avec les autres banques de données policières ;
  - journalisation ;
  - processus d'effacement (vérifications des délais de conservation) ;
    - gestion des accès et traçabilité ;
    - sécurité TIC.

- Triptyque (photo, empreintes digitales et signalement individuel)

- BNG : option 35[9] – validation centrale : état des lieux/points d'attention.

4. Le contrôle s'est décliné en quatre phases.

[7] Telle que modifiée par la loi du 20 juillet 2022 *« relative à la collecte et à la conservation des données d'identification et des métadonnées dans le secteur des communications électroniques et à la fourniture de ces données aux autorités »* (*M.B.* du 8 août 2022).
[8] Art. 248 de la LPD.
[9] Par 'option 35', on entend le transfert normal des données d'*ISLP* vers la Banque de données nationale générale (BNG).

Durant la première phase, les informations et documents nécessaires ont été demandés à la SPN-Côte dans un courrier du 25.01.2023 annonçant le contrôle. En fonction du contenu des réponses et des documents, des questions spécifiques ont été posées en vue d'une enquête plus approfondie pendant la visite proprement dite.

La deuxième phase a consisté en l'analyse des documents reçus le 01.03.2023.

Durant la troisième phase, un questionnaire a été établi le 25.04.2023 sur la base de l'analyse des documents transmis par la SPN-Côte dans le cadre de la deuxième phase. Ce questionnaire avait pour but d'obtenir des précisions au sujet des documents transmis par la SPN-Côte.

La quatrième phase a consisté en la visite sur place rendue à la SPN-Côte le 24.05.2023. Cette visite s'est déroulée comme suit :

1) une introduction du COC et des membres présents de la Direction générale de la SPN et de la SPN-Côte ;

2) l'examen d'un questionnaire consacré à l'utilisation de caméras au sein de la Direction de la SPN-Côte et aux banques de données particulières ;

3) une visite générale des locaux de la SPN-Côte ainsi que des locaux où est établi le CIM[10], lors de laquelle le COC a eu l'occasion de poser des questions ponctuelles.

5. Le 14.02.2024, le projet de rapport a été transmis en prélecture à la Direction de la SPN dans le cadre du droit de réponse organisé d'office par l'Organe de contrôle.

Le 07.03.2024, le COC a reçu les remarques de la Direction de la SPN au sujet du projet de rapport et, dans la mesure où elles étaient pertinentes, en a tenu compte dans le présent rapport définitif.

3. CADRE JURIDIQUE

3.1. Utilisation de caméras par la police

6. En 2018, l'utilisation de caméras par les services de police a été ancrée dans la LFP par la loi du 21 mars 2018 *« modifiant la loi sur la fonction de police, en vue de régler l'utilisation de caméras par les services de police, et modifiant la loi du 21 mars 2007 réglant l'installation et l'utilisation de caméras de surveillance, la loi du 30 novembre 1998 organique des services de renseignement et de sécurité et la loi du 2 octobre 2017 réglementant la sécurité privée et particulière »* (ci-après 'la loi du 21 mars 2018').

La loi du 21 mars 2018 visait donc à exclure les caméras des services de police du champ d'application de la loi relative aux caméras[11]. Il en découle que l'utilisation de caméras par la police est délimitée par la finalité et la compétence de traitement qui sont régies d'une part par la loi relative aux caméras et d'autre part par la LFP (Titre 2 de la LPD) ou par une loi spéciale[12]. Le fait que la police soit mentionnée dans la loi relative aux caméras – parce qu'elle peut dans certaines circonstances et sous certaines conditions avoir accès (en temps réel) aux images de caméras de tiers – ne porte en rien préjudice au fait que l'utilisation de caméras par la police dans le cadre de l'exercice des compétences générales de police relève depuis le 25 mai 2018 exclusivement de l'application de la LFP[13].

3.1.1. Responsable du traitement

7. Le droit de la protection des données réserve un rôle important au 'responsable du traitement'. Le responsable du traitement est *« la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou*

---

[10] Le Carrefour d'Information Maritime, dénommé en néerlandais MIK pour '*Maritiem Informatiekruispunt*'. Il s'agit d'un pilier de la centrale de la garde côtière, qui se compose de la Police de la navigation, de la Défense, de la DG Navigation, CLSM (Comité local de la Sûreté maritime) et de la Douane et qui a pour principale mission de traiter les informations maritimes pertinentes. Le CIM joue un rôle de point de distribution où les renseignements nationaux et internationaux concernant les activités maritimes sont rassemblés, enrichis et transmis aux partenaires nationaux et étrangers. Pour pouvoir garantir le maintien de l'ordre public dans nos contrées, le CIM se focalise sur la surveillance de la Zone économique exclusive de la Belgique (ZEE BE) en recourant à des instruments et sources d'informations avancés et en les combinant avec la présence en mer de la Police de la navigation et de la Marine.

[11] *« **Ces nouvelles règles vont donc exclure l'application de la loi caméras** (conformément à l'article 3 de cette dernière) **aux caméras des services de police**. Cela constitue un premier changement majeur. »* et *« Cette nouvelle section de la loi sur la fonction de police va régler l'utilisation de caméras de manière visible dans le cadre des missions de police (…) »,* Exposé des motifs de la loi du 18 mars 2018, Doc. Parl. *Chambre* 2017-2018, n° 54-2855/001, p. 3, 6-7 et 13.

[12] Comme le contrôle de trajet, qui relève de l'application de la loi du 16 mars 1968 relative à la police de la circulation routière (Doc. Parl. *Chambre* 2017-2018, n° 54-2855/001, p. 9).

[13] Article 89 de la loi du 21 mars 2018. L'accès en temps réel aux images de caméras de surveillance du réseau des sociétés de transport en commun est également régi conformément à l'article 9 de la loi relative aux caméras du 21 mars 2007.

conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel »[14]. En ce qui concerne les activités de traitement dans le cadre des missions de police administrative et judiciaire, le responsable du traitement est défini par la LPD comme *« l'autorité compétente qui, seule ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel. Lorsque les finalités et les moyens de ce traitement sont déterminés par la loi, le décret ou l'ordonnance, le responsable du traitement est l'entité désignée comme responsable du traitement par ou en vertu de cette loi, ce décret ou cette ordonnance. »*[15]. On entend par *« autorités compétentes » « a) les 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 »*[16].

8. Comme nous le disions plus haut, le responsable du traitement est un acteur essentiel dans le traitement de données à caractère personnel. Il doit en effet prouver que les données à caractère personnel sont traitées conformément au cadre légal[17]. Il est aussi, ou son préposé ou mandataire, la personne à l'égard de laquelle d'éventuelles mesures correctrices peuvent être imposées, ou qui peut faire l'objet d'une sanction disciplinaire ou pénale[18]. Le chef de corps, le commissaire général, le directeur général ou le directeur est le responsable du traitement pour l'utilisation des caméras et le traitement des images des caméras[19].

Le directeur est donc le responsable du traitement pour toutes les formes d'utilisations de caméras par la Direction de la SPN de la police fédérale.

3.1.2. Exigences procédurales

9. Avant que le directeur de la SPN ne puisse introduire la surveillance par caméra, il doit obtenir à cette fin l'autorisation de principe du ministre de l'Intérieur ou de son préposé[20]. Il ne faut toutefois pas d'autorisation pour l'utilisation de caméras dans les lieux fermés dont les services de police sont les gestionnaires, comme un commissariat de police[21].

3.1.3. Délai de conservation des images

10. Les images des caméras peuvent être conservées au maximum pendant 12 mois[22]. La loi ne stipule en principe pas de délai minimum[23]. En ce qui concerne les images des caméras régies par la LFP, la loi ne précise pas sur quel support de données les images doivent être enregistrées. Il est dès lors indiqué que le directeur précise dans le registre des traitements de données à caractère personnel tel que visé à l'article 55 de la LPD et à l'article 145 de la LPI[24] sur quel support de données les images sont enregistrées. L'Organe de contrôle doit avoir accès à ce support de données[25].

Les banques de données particulières servent à enregistrer des données qui n'entrent pas en ligne de compte pour un enregistrement dans la BNG bien qu'elles aient une finalité opérationnelle. Des exemples de banques de données particulières sont (1) l'enregistrement de numéros de téléphone ou de données *ANPR* collecté(e)s dans le cadre d'une enquête pénale[26] et, en l'occurrence, (2) les images de caméras. Il s'agit de données qui présentent un lien avec les missions de police administrative et judiciaire, mais qui ne doivent pas *ipso facto* être enregistrées/saisies dans la BNG[27].

---

[14] Art. 4. 7) du RGPD.
[15] Art. 26, 8° de la LPD.
[16] Art. 26, 7° de la LPD.
[17] Articles 29 §5 et 50, 2e alinéa de la LPD.
[18] Voir les articles 221 et 222 de la LPD. Concrètement, l'Organe de contrôle peut prendre notamment les mesures suivantes (art. 58.2 du RGPD) : donner un avertissement, donner une réprimande, ordonner de mettre dans un certain délai le traitement en conformité avec le cadre légal, imposer une limitation ou une interdiction temporaire ou définitive du traitement.
[19] Articles 25/4 §2, 1er alinéa *juncto* 25/5 §1er, 44/4 §1er, 3e alinéa et 44/11/3*sexies* §1er, 2e alinéa de la LFP.
[20] Art. 25/4 §1er, 2° de la LFP. En vertu de l'article 4 de la loi du 19 octobre 2023 *« modifiant la loi sur la fonction de police, en ce qui concerne l'utilisation des caméras individuelles par les services de police »*, l'autorisation du Conseil communal n'est plus requise pour l'utilisation de caméras mobiles. Cet article entre en vigueur deux mois après la publication de ladite loi au Moniteur belge (*M.B.,* 20 novembre 2023), c'est-à-dire le 20.01.2024.
[21] Art. 25/4 §5 de la LFP. Exposé des motifs, p. 21 (Doc. Parl. *Chambre* 2017-2018, n° 54-2855/001).
[22] Art. 25/6, 44/11/3*decies* §2, 1er alinéa et 46/12, 1er alinéa de la LFP. En vertu de l'article 5 de la loi du 19 octobre 2023 *« modifiant la loi sur la fonction de police, en ce qui concerne l'utilisation des caméras individuelles par les services de police »*, les mots « douze mois » sont remplacés par les mots « 365 jours ». Cet article entre en vigueur deux mois après la publication de ladite loi au Moniteur belge (*M.B.,* 20 novembre 2023), c'est-à-dire le 20 janvier 2024.
[23] La loi du 19 octobre 2023 *« modifiant la loi sur la fonction de police, en ce qui concerne l'utilisation des caméras individuelles par les services de police »* introduit toutefois un délai de conservation minimum de 30 jours pour les images des caméras individuelles et des caméras installées dans les cellules de police (article 5). Cette loi entre en vigueur le 20 janvier 2024 en ce qui concerne le délai de conservation minimum, avec une exception pour les lieux de détention. Pour ces derniers, une période transitoire de 2 ans s'applique (article 13).
[24] Loi du 7 décembre 1998 *« organisant un service de police intégré, structuré à deux niveaux »*. Voir en particulier l'article 7 de la loi du 19 octobre 2023 *« modifiant la loi sur la fonction de police, en ce qui concerne l'utilisation des caméras individuelles par les services de police »*.
[25] Art. 25/8, 3e alinéa de la LFP.
[26] MERCURE.
[27] Art. 44/11/3 de la LFP.

L'Organe de contrôle est d'avis qu'il s'agit ici (également) d'une banque de données particulière, de sorte que le directeur doit en l'occurrence être considéré comme le responsable du traitement. L'article 44/4 §1er, 3e alinéa de la LFP dispose en effet que les chefs de corps, le commissaire général, les directeurs généraux ou les directeurs sont les responsables du traitement des banques de données particulières qu'ils créent dès lors qu'ils en fixent les objectifs et les moyens. La désignation en l'occurrence du directeur en tant que responsable du traitement s'inscrit par ailleurs dans l'esprit des dispositions de la LFP relatives à la création de banques de données locales. Selon l'article 25/5 §1er de la LFP, la décision de recourir à la surveillance par caméra est prise par le fonctionnaire de police compétent et sous sa responsabilité. S'il ne s'agit pas du directeur, le fonctionnaire de police compétent agit sous la responsabilité du directeur.

3.1.4. Banques de données techniques

11. Il est important dans ce contexte de signaler qu'un régime spécifique s'applique pour l'utilisation de caméras *ANPR*. Il s'agit de *« caméras intelligentes »*, à savoir des *« caméras qui comprennent également des composantes ainsi que des logiciels qui, couplés ou non à des registres ou à des fichiers, peuvent traiter de manière autonome ou non les images recueillies »*[28]. Lorsque la surveillance par caméra *ANPR* est appliquée, les images doivent être enregistrées dans une *« banque de données technique »*[29], étant entendu que les données à caractère personnel et informations sont également transmises à la banque de données technique nationale[30]. Les images peuvent être conservées au maximum pendant 12 mois (365 jours selon la modification de la loi) et il n'est pas fixé de délai minimum[31].

La banque de données technique contient les données suivantes, si elles apparaissent sur les images des caméras[32] :
1) la date, le moment et l'endroit précis du passage de la plaque d'immatriculation ;
2) les caractéristiques du véhicule lié à cette plaque ;
3) une photo de la plaque d'immatriculation à l'avant du véhicule et le cas échéant[33], à l'arrière ;
4) une photo du véhicule ;
5) le cas échéant[34], une photo du conducteur et des passagers ;
6) les données de journalisation des traitements.

Ces données doivent donc être enregistrées dans la banque de données technique pour autant que ces données apparaissent sur les images *ANPR*.

12. Les principes relatifs aux interconnexions et corrélations des banques de données techniques avec les banques de données visées à l'article 44/2 §§ 1er et 2 de la LFP ou avec d'autres banques de données auxquelles les services de police ont accès par ou en vertu de la loi ou de traités internationaux conformément à l'article 44/4 §6 de la LFP sont régis par la directive interconnexions et corrélations *ANPR*[35]. Les interconnexions et corrélations doivent notamment tenir compte :

- des critères de temps, d'espace et de fréquence tels que visés à l'article 44/4 §6 de la LFP ;
- de l'enregistrement dans le registre des traitements REGPOL des autorisations requises ;
- de la nécessité d'adopter une procédure transparente et auditable lorsque les unités de police utilisent des listes ou des extraits en dehors des standards nationaux qu'ils interconnectent avec les *ANPR* locaux et l'*ANPR* national en vue d'établir des comparaisons ;
- de la nécessité en cas de *hit* (corrélation positive) de suivre la politique d'action nationale et une politique d'intervention ciblée ;
- de la nécessité de retourner vers la source authentique en cas d'un *hit* sur une plaque d'immatriculation, détecté à l'aide de listes ou d'extraits injectés dans une banque de données technique locale ou nationale, sauf si la corrélation se fait en temps réel avec la source authentique.

3.1.5 Accès aux images

13. L'accès aux images dépend de la finalité et est réglé de la même manière pour la surveillance par caméra ordinaire et pour l'utilisation de caméras *ANPR*. Dans les deux cas, les images peuvent être conservées au maximum pendant 12 mois (365 jours selon la modification de la loi). En ce qui concerne les missions de police administrative, l'accès est limité au premier mois à partir de l'enregistrement des images. Pour les missions de police judiciaire, les images sont

[28] Art. 25/2 §1er, 3°, *juncto* art. 44/2 §3, troisième alinéa de la LFP.
[29] Art. 44/2 §3, premier alinéa de la LFP.
[30] Art. 44/11/3*sexies* de la LFP.
[31] Art. 44/11/3*decies* §2, 1er alinéa de la LFP.
[32] Art. 44/11/3*decies* §1er de la LFP.
[33] L'expression *« le cas échéant »* renvoie à la possibilité technique de la caméra de prendre ou non ces photos.
[34] *Ibid*.
[35] Directive commune contraignante des Ministres de la Justice et de l'Intérieur relative à la détermination des mesures adéquates, pertinentes et non excessives relatives à l'interconnexion ou la corrélation des banques de données techniques suite à l'utilisation de caméras ou de systèmes intelligents de reconnaissance automatique de plaques d'immatriculation, visées à l'article 44/2 §3 de la loi sur la fonction de police, avec les banques de données visées à l'article 44/2 §§ 1er et 2 LFP, ou avec d'autres banques de données auxquelles les services de police ont accès par ou en vertu de la loi ou de traités internationaux liant la Belgique, *M.B.* 28 janvier 2021.

accessibles pendant l'entièreté du délai de conservation, étant entendu que l'intervention du procureur du Roi est requise après l'expiration du premier mois (30 jours[36])[37]. L'accès doit être motivé sur le plan opérationnel et nécessaire pour l'exercice d'une mission précise[38], ce qui revient à dire que l'accès aux images n'est autorisé que pour les personnes qui ont besoin de ces données à caractère personnel et informations et en présence d'un intérêt opérationnel concret[39].

14. La LFP ne contient aucune disposition régissant les droits du fonctionnaire de police ou du citoyen en ce qui concerne l'accès aux images dans l'hypothèse où les images ne sont pas utilisées à des fins opérationnelles (et ne servent donc par exemple pas de base pour l'établissement d'un procès-verbal). Si toutefois les images ne sont pas pertinentes pour les missions de police administrative ou judiciaire, et ne présentent donc aucun intérêt opérationnel, la LFP ne s'oppose pas à ce que la zone de police responsable organise elle-même un droit d'accès aux images[40] en prenant éventuellement pour exemple le système d'accès par analogie à la loi relative aux caméras du 21 mars 2007, selon lequel non seulement le fonctionnaire de police mais aussi le citoyen s'adressent en première instance directement au service de police concerné.

3.1.6. Utilisation de caméras visibles et non visibles

15. Les caméras visibles sont des caméras dont l'utilisation est annoncée par des pictogrammes, les caméras montées à bord de véhicules de police, de navires de police, d'aéronefs de police, ou de tout autre moyen de transport de police, identifiables comme tels, ou portées par des fonctionnaires de police identifiables comme tels[41]. Dans des circonstances exceptionnelles, la police peut recourir 'secrètement' à des caméras (utilisation non visible de caméras en vertu de la section 2 du chapitre IV/1 de la LFP). La caméra peut dans ce contexte être portée par un fonctionnaire de police non identifiable comme tel ou être montée à bord d'un véhicule de police anonyme. Il est question d'un véhicule de police anonyme lorsque le véhicule de police n'est pas identifiable comme tel. Dans ce cas, il est donc question d'une utilisation « *non visible* » de caméras[42]. Le recours à des caméras non visibles est strictement réglementé et limité à quatre situations, à savoir :
1) dans des circonstances particulières, notamment lors d'attroupements, en vue du recueil de l'information de police administrative concernant des personnes radicalisées ou des *terrorist fighters* et sur un moyen de transport de police, non identifiable comme tel, pour la lecture automatique de plaques d'immatriculation, en vue de détecter des véhicules signalés (art. 46/4 de la LFP) ;
2) pour la préparation d'actions de police judiciaire et afin de garantir l'ordre public lors de ces actions (art. 46/7 et 46/8 de la LFP) ;
3) dans le cadre de l'exécution de missions spécialisées de protection de personnes (art. 44/9 de la LFP) ;
4) dans le cadre de l'exécution de missions de transfert de personnes détenues ou arrêtées (art. 46/11 de la LFP).

Sauf lorsque l'utilisation non visible des caméras est réalisée sous le contrôle d'un magistrat, l'autorisation du commissaire général de la police fédérale ou du membre du comité de direction de la police fédérale désigné par lui, si le service demandeur fait partie de la police fédérale, ou l'autorisation du chef de corps ou de son préposé (articles 7 à 7/3 de la LFP), s'il s'agit de la police locale, doit pour cette forme d'utilisation de caméras être notifiée **au préalable** à l'Organe de contrôle. Cette notification préalable doit permettre à l'Organe de contrôle d'évaluer la licéité de la décision[43].

3.1.7. Analyse d'impact et de risques et analyse d'impact relative à la protection des données (AIPD ou *DPIA, Data Protection Impact Assessment*)

16. Depuis la loi du 21 mars 2018, il est obligatoire de procéder, préalablement au recours à la surveillance par caméra, à une analyse d'impact et de risques évaluant l'aspect de la protection de la vie privée par rapport au niveau opérationnel de l'utilisation des caméras[44]. Cet exercice doit également être réalisé avant la création d'une banque de données technique (locale)[45]. L'assistance du délégué à la protection des données est demandée dans ce contexte[46].

Pour autant que les conditions de la LPD pour une AIPD et les conditions pour une analyse de risques et d'impact relative à l'utilisation de caméras et/ou relative à la création de banques de données techniques dans le cadre de la LFP soient respectées, les deux analyses peuvent être compilées en un seul document. Étant donné qu'une AIPD dans le

[36] Art. 6 de la loi du 19 octobre 2023 *« modifiant la loi sur la fonction de police, en ce qui concerne l'utilisation des caméras individuelles par les services de police »*.
[37] Art. 25/7 §1er, 1er et 2e alinéas et 44/11/3*decies* §3, 1er alinéa de la LFP.
[38] Art. 44/11/3*decies* §3, 1er alinéa de la LFP.
[39] Exposé des motifs de cette loi, p. 29 (Doc. Parl. *Chambre* 2017-2018, n° 54-2855/001).
[40] Conformément au principe prévu à l'article 38 (droit d'accès) de la LPD.
[41] Art. 25/2 §2 de la LFP, adapté par l'article 2, e) de la loi du 19 octobre 2023 en ce sens que le fonctionnaire de police doit être identifiable conformément à l'article 41 de la LFP.
[42] Art. 46/4 et suivants de la LFP.
[43] Art. 46/5, 46/6 et 46/10 de la LFP.
[44] Art. 25/4 §2 de la LFP.
[45] Art. 44/11/3*octies* de la LFP.
[46] Art. 65, 3° *juncto* 58 de la LPD.

cadre de la LPD requiert une analyse plus large que ce que prescrit la LFP, nous précisons que si les deux analyses sont réalisées ensemble, cette analyse doit couvrir conformément à la LPD tous les systèmes et procédures pertinents des activités de traitement. En marge du respect de la LPD et de la LFP, les mesures de précaution opérationnelles et les mesures de sécurité (prises pour limiter les risques pour les données à caractère personnel à protéger) doivent également être décrites.

3.1.8. Registres

17. Conformément à l'actuel article 25/8, 1er alinéa de la LFP, de la LFP, l'utilisation de caméras doit être tenue à jour dans un registre (local) mentionnant le type de caméras et leur emplacement. Il n'existe toutefois pas encore d'arrêté royal détaillant le contenu du registre. Cette obligation est toutefois devenue caduque du fait de l'entrée en vigueur de la loi du 19 octobre 2023, le 20 janvier 2024, de sorte que l'*utilisation* de caméras ne doit plus être tenue à jour dans un registre local. Comme c'est le cas actuellement pour le traitement de toutes les données à caractère personnel, l'article 25/8 de la LFP a en effet été adapté par la loi du 19 octobre 2023 et prévoit désormais que les *traitements* relatifs à l'usage des caméras doivent être inventoriés dans le registre unique des activités de traitement (REGPOL) visé à l'article 145 de la LPI, pour lequel aucun arrêté d'exécution (article 145, 2e alinéa de la LPI) n'est cependant encore paru jusqu'à la date du présent rapport. Dans l'attente de l'arrêté d'exécution, l'Organe de contrôle est d'avis que dans l'intérêt de l'efficacité de ses compétences de contrôle, la police doit tenir à jour dans le registre REGPOL chaque *utilisation* (de n'importe quel type) de caméras, y compris les utilisations non visibles. L'article 25/8 de la LFP, enfin, fait également référence au registre national de géolocalisation, qui reprend la géolocalisation de toutes les caméras fixes utilisées par les services de police et qui est tenu au sein de la police fédérale et conservé sous une forme digitale. Ce registre répondant au nom de *« CamELIA »*[47] contient également les données de géolocalisation des caméras de surveillance qui doivent être déclarées par le(s) responsable(s) (tiers) à la police dans le cadre des dispositions de la loi du 21 mars 2007 réglant l'installation et l'utilisation de caméras de surveillance.

3.1.9. Surveillance par caméra des bâtiments et bureaux de police et cellules de police

18. La surveillance par caméra des bâtiments et bureaux de police et cellules de police relève de la LFP. C'est également le cas de la surveillance par caméra du hall d'entrée ou de l'accueil du commissariat de police. La vidéosurveillance[48] dans les lieux de détention contribue à la protection et à la garantie du bien-être des personnes qui ont été privées de leur liberté[49]. Cette vidéosurveillance n'est cependant envisageable que comme un élément venant s'ajouter à un ensemble de mesures, comme le contrôle physique régulier des personnes détenues, une politique de prévention du suicide ou de l'automutilation, un système de dénonciation efficace pour les victimes d'actes illicites dans des cellules, la séparation, l'isolement, l'application de sanctions disciplinaires ou encore la présence d'un avocat pendant l'audition par la police[50].

Le bâtiment ou poste de police doit être équipé d'une signalisation claire de la vidéosurveillance, de manière à ce que la personne détenue dans l'une des cellules en ait été explicitement informée. Les enregistrements de la détention doivent rester intégraux (aucun effacement partiel) et être conservés pendant une période permettant d'introduire une plainte dans un délai raisonnable. Dans l'intervalle, la loi susmentionnée du 19 octobre 2023 a imposé un délai de conservation minimum de 30 jours, mais cette obligation entrera seulement en vigueur au plus tard deux ans après la publication de cette loi au Moniteur belge[51].

Lors de la projection des images des différentes cellules sur les moniteurs installés au commissariat, la police doit prendre un certain nombre de mesures de sécurité et d'accès rigoureuses : l'accès doit être limité selon le principe *need to know* et doit être proportionnel (autrement dit, seules les images pertinentes sont consultées). Il convient d'éviter un accès général aux images (par exemple sur des moniteurs installés dans un local où les membres du personnel vont et viennent, ou à l'accueil).

---

[47] *CamELIA* est une application visuelle qui présente les caméras sur une carte. Le nom *CamELIA* est l'acronyme de *Camera **E**nhanced **L**ocation **I**nformation **A**pplication*. En ce sens, cette application est la matérialisation du registre national de géolocalisation visé à l'article 25/8 de la LFP. L'application *CamELIA* permet de visualiser tous les emplacements et détails des caméras, provenant de différentes sources : les caméras *ANPR* (*AMS*), les caméras de surveillance de particuliers, d'entreprises ou d'autorités locales (IBZ/Camine) et les caméras disposées par la GPI elle-même.

[48] Recommandation 06/11 de l'ancienne Commission de protection de la vie privée ou CPVP – actuellement l'Autorité de protection des données ou APD – sur l'installation et l'utilisation de caméras de surveillance dans les lieux de détention et dans d'autres lieux du commissariat.

[49] Voir l'arrêté royal du 14 septembre 2007 *« relatif aux normes minimales, à l'implantation et à l'usage des lieux de détention utilisés par les services de police »*, et en particulier l'article 10.

[50] Voir à ce sujet *« Les normes du CPT – Chapitres des rapports généraux du CPT consacrés à des questions de fond »* (document CPT/Inf/E (2002) 1 – Rév. 2009), disponible sur le site www.cpt.coe.int/en/docsstandards.htm.

[51] Articles 5 et 13 de la loi du 19 octobre 2023 *« modifiant la loi sur la fonction de police, en ce qui concerne l'utilisation des caméras individuelles par les services de police »*, *M.B.* 20 novembre 2023 (c'est-à-dire le 20.11.2025).

Comme nous le disions, la LFP ne s'oppose pas, lorsque ces images ne présentent aucun intérêt opérationnel, à ce que la personne concernée accède directement aux images des caméras de sa détention conformément à la LPD et au RGPD.

3.1.10. Images des caméras braquées sur le périmètre des installations portuaires

19. Dans le cadre de leurs missions de police administrative ou judiciaire, les services de police fédéraux et locaux ont librement et gratuitement accès en temps réel aux images des caméras qui sont braquées sur le périmètre des installations portuaires[52]. Les règles régissant ce libre accès aux images, leur transmission et leur sécurisation sont fixées dans des protocoles entre les services de police concernés et la société de transport en commun, qui sont soumis pour avis à l'Autorité de protection des données préalablement à leur signature[53]. Le COC[54] souligne ici qu'il s'agit donc effectivement de caméras de surveillance installées par le gestionnaire du lieu en question, et non de caméras installées et entièrement gérées par les services de police. S'il s'agit de caméras fixes installées par les services de police eux-mêmes dans un lieu fermé accessible au public dont ils ne sont pas les gestionnaires, cette utilisation n'est possible que dans les cas visés à l'article 25/3 §1er, 2°, b) à d) de la LFP. Il est donc ici question uniquement des cas où les caméras de surveillance sont installées en première instance par le gestionnaire du lieu, dans le respect de la loi relative aux caméras du 21 mars 2007, et où l'accès aux images est accordé en temps réel aux services de police en vertu de l'article 9, troisième alinéa, 3°, a) de la loi relative aux caméras susmentionnée. Si les parties à l'accord régissant cet accès conviennent que cet accès en temps réel s'assortira également d'un enregistrement des images auprès des services de police, ces derniers devront aussi veiller à ce que toutes les règles relatives à l'utilisation de caméras qui sont prévues par la LFP soient respectées. Cette obligation découle de l'application combinée de l'article 9 de la loi relative aux caméras et des articles 25/1 §2 et 25/4 §1er de la LFP, de sorte qu'il s'agit d'une autre hypothèse que celle visée à l'article 25/3 §1er, 2°, b), qui est régie par un autre arrêté royal spécifique[55] et vise uniquement les cas où les services de police sont en exclusivité l'installateur et l'utilisateur de caméras en un lieu impliquant un risque particulier pour la sécurité mentionné dans la liste, après accord du gestionnaire du lieu.

Pour résumer, les hypothèses sont donc les suivantes :

- la police utilise des caméras de surveillance installées et utilisées par un autre responsable du traitement (en l'occurrence la Région flamande) dans un lieu fermé accessible au public au moyen d'un accès en temps réel, sans enregistrer les images : l'article 9 de la loi relative aux caméras trouve application ;

- la police utilise des caméras de surveillance installées et utilisées par un autre responsable du traitement (en l'occurrence la Région flamande) au sens du point précédent et enregistre les images : les articles 25/1 §2 et suivants de la LFP trouvent application ;

- la police est en exclusivité l'installateur et l'utilisateur de caméras de surveillance se trouvant dans les lieux fermés accessibles au public gérés par la société de transport en commun, avec l'accord de cette dernière : l'article 25/3 §1er, 2° b de la LFP trouve application.

Le délai de conservation maximum pour le responsable du traitement, lorsque ce dernier n'est pour toute clarté *pas* la police, est dans ce cas de trois mois, conformément aux articles 5 §4, 5e alinéa, 6 §3, 3e alinéa, 7 §3, 3e alinéa et 7/3 §4, 2e alinéa de la loi relative aux caméras du 21 mars 2007. Il s'agit là d'un délai de conservation maximum qui n'implique donc aucune obligation de conserver effectivement les images pendant trois mois.

3.2. Banques de données particulières

20. L'article 44/11/3 §1er de la LFP dispose que la création d'une banque de données particulière n'est possible que lorsque l'exercice des missions de police administrative et judiciaire exige que les services de police structurent les données à caractère personnel et informations visées à l'article 44/1 de la LFP de manière à ce qu'elles puissent être retrouvées directement. Il s'agit donc d'une banque de données 'opérationnelle'.

21. La création d'une banque de données particulière est en outre soumise aux conditions cumulatives suivantes :
- dans des circonstances spécifiques ;
- pour l'exercice des missions de police administrative et judiciaire ;

[52] Installations portuaires visées à l'article 5, 6° et 7° de la loi du 5 février 2007 relative à la sûreté maritime.
[53] Article 9 de la loi du 21 mars 2007 réglant l'installation et l'utilisation de caméras de surveillance.
[54] Voir aussi le Rapport au Roi de l'arrêté royal du 6 décembre 2018 déterminant les lieux où le responsable du traitement peut diriger ses caméras de surveillance vers le périmètre entourant directement le lieu, conserver les images des caméras de surveillance pendant trois mois et donner accès en temps réel aux images aux services de police (*M.B.* 18 décembre 2018, 99553, commentaire des articles 3 et 4).
[55] À savoir l'arrêté royal du 6 décembre 2018 portant exécution de l'article 25/3 §1er, 2°, b) de la loi sur la fonction de police, *M.B.* 24 décembre 2018, 102186.

- pour des besoins particuliers.

L'article 44/11/3 §2 de la LFP prévoit par ailleurs que la création d'une banque de données particulière doit être motivée par au moins un des besoins particuliers suivants :

a) la nécessité de classifier des données à caractère personnel ou informations au sens de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité[56] ;

b) l'impossibilité technique ou fonctionnelle d'alimenter la BNG de tout ou partie des données à caractère personnel et informations traitées dans ces banques de données ;

c) le caractère non pertinent ou excessif de la centralisation dans la BNG de tout ou partie des données à caractère personnel ou des informations, dans le cadre de l'exercice des missions de police administrative et de police judiciaire.

22. Les conditions de la création d'une banque de données particulière sont donc clairement définies dans la loi. Ces dispositions légales constituent donc le cadre de référence sur lequel le COC se base pour considérer une certaine banque de données comme une banque de données particulière. Le responsable du traitement doit, avant de reprendre cette banque de données dans le registre REGPOL ou dans un registre local, examiner si la création d'une banque de données particulière est nécessaire et si l'enregistrement projeté des données répond aux conditions légales pour la qualification de banque de données particulière. La finalité spécifique en vue de laquelle la banque de données particulière est créée doit cadrer dans une mission de police administrative ou judiciaire.

23. Le responsable du traitement (l'entité de police) doit examiner si l'établissement d'une analyse d'impact relative à la protection des données (AIPD ou *DPIA*[57]) est obligatoire ou recommandée (article 58 de la LPD). Dans certaines circonstances, le responsable du traitement devra consulter le COC préalablement au traitement (l'enregistrement de données dans une banque de données particulière). Ce sera au moins le cas :

- lorsqu'un type de traitement, en particulier par le recours aux nouvelles technologies, est susceptible d'engendrer un risque élevé pour les droits et les libertés des personnes physiques (art. 58) ;
- lorsque l'AIPD indique que le traitement présente un risque élevé et que le responsable du traitement ne prend pas de mesures pour atténuer le risque ; ou lorsque le type de traitement, en particulier en raison de l'utilisation de nouveaux mécanismes, technologies ou procédures, présente des risques élevés pour les libertés et les droits des personnes concernées (art. 59 §1er, 1° et 2°).

24. La GPI ne peut par conséquent pas retenir par exemple les arguments suivants pour créer une banque de données particulière :
- alléguer la charge de travail induite par l'encodage, l'alimentation et le transfert des données à la BNG ;
- alléguer le manque de connaissance de l'utilisation de la BNG ou d'une banque de données de base ;
- alléguer le manque (prétendu) de convivialité de la BNG ou d'une banque de données de base.

3.3. Triptyque

25. La réglementation élaborée sur la base de la LFP pour la réalisation du triptyque trouve son origine dans la directive contraignante commune MFO-3, fiches B04 et B05, ainsi que dans la circulaire COL 20/2010 du Collège des procureurs généraux près les Cours d'appel intitulée *« Triptyque d'identification judiciaire – Refonte de la page de garde des procès-verbaux initiaux »*, révisée le 19 octobre 2012[58]. Le triptyque judiciaire est réalisé dans le cadre de l'identification de personnes et se compose de 3 volets :

- les empreintes digitales et palmaires ;
- les photos ;
- le signalement individuel de la personne.

26. La circulaire COL 20/2010 est publique et fait mention des circonstances dans lesquelles le triptyque doit être réalisé, dont le détail est élaboré dans les fiches susmentionnées qui n'ont pas été publiées.

---

[56] Actuellement la loi du 11 décembre 1998 *« relative à la classification, aux habilitations de sécurité, attestations de sécurité, avis de sécurité et au service public réglementé »* (intitulé remplacé par la loi du 7 avril 2023 *« portant modification de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité »*, *M.B.* 9 juin 2023).
[57] *Data Protection Impact Assessment*.
[58] Disponible sur le site https://www.om-mp.be/fr/savoir-plus/circulaires.

27. …

28. Il est **obligatoire** de relever les empreintes digitales d'un suspect lorsque cette personne est âgée de plus de 14 ans[59] et :

- soit est entendue et mise, sur la base d'informations confirmées (prouvées), en relation avec un fait concret, ou fait l'objet de présomptions sérieuses de la part des services de police (pour autant qu'il ne s'agisse pas d'un KOF4[60]) ;
- soit est privée de sa liberté (à partir du moment où, pour les besoins de l'enquête, la personne concernée n'est plus libre d'aller et venir comme elle veut) ;
- soit est mise à la disposition des instances judiciaires ou de l'Office des Étrangers ;
- soit doit être enfermée dans un établissement pénitentiaire en vertu d'un ordre judiciaire ou d'une décision judiciaire.

Le triptyque est également réalisé dans le cadre de la loi du 15 décembre 1980 sur l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers.

29. Pour les mineurs d'âge âgés de moins de 14 ans, le magistrat en charge du dossier doit en outre avoir donné son autorisation en vue de la réalisation de l'identification judiciaire en trois volets. Cette autorisation doit être consignée dans le procès-verbal.

30. En cas de séjour illégal, le triptyque judiciaire **DOIT** toujours être réalisé.

La contrainte strictement nécessaire peut être exercée pour le relevé des empreintes digitales (cf. art. 37 de la LFP).

Les modalités pratiques de la réalisation du triptyque sont décrites dans les fiches B03, B04 et B05 de la directive MFO-3.

4. CONCLUSIONS DE L'ENQUÊTE

4.1. L'utilisation de caméras

31. Lors du contrôle du registre *CamELIA*, le COC n'a pas été en mesure de retrouver des enregistrements de caméras gérées par la SPN-Côte. En ce qui concerne le registre national REGPOL, il s'est avéré que l'utilisation de caméras avait été déclarée, à l'exception des caméras installées dans les cellules de police de la section X, des caméras installées dans les locaux d'audition de la section Y et des caméras de surveillance de la section Y. Ces trois dernières n'ont été enregistrées dans le registre REGPOL qu'après l'annonce du contrôle par le COC. La SPN-Côte l'a confirmé au COC.

32. …

33. Le COC a pu déduire des réponses qui lui ont été fournies que la SPN-Côte utilise ou a utilisé d'une part des caméras mobiles comme des *bodycams* (caméras individuelles[61]), des caméras *ANPR* et des caméras montées sur des drones (chapitre 4.1.1), et d'autre part des caméras fixes comme celles installées aux accès maritimes, dans les ports de plaisance, dans les cellules de police et dans les locaux d'audition, (…). Ces premières réponses fournies par la Direction de la SPN étaient cependant à ce point imprécises ou vagues qu'elles nécessitaient encore un complément d'explications et qu'elles ont, comme nous le verrons plus loin, eu un impact sur les constatations effectuées lors de la visite.

4.1.1. Caméras mobiles

4.1.1.1. En ce qui concerne les *bodycams*

34. La SPN-Côte a déclaré avoir utilisé des *bodycams*. Selon la première réponse, la SPN-Côte aurait uniquement utilisé les *bodycams* dans une phase de test et pour évaluer l'offre disponible sur le marché. Cette phase de test était entretemps terminée. Comme le COC n'était pas en mesure d'établir clairement durant quelle période ces *bodycams*

[59] Concrètement : *« À partir du lendemain du jour de son 14e anniversaire »*, cf. la circulaire COL 20/2010.
[60] Un KOF4 est un fait concret de type 4 dont l'intérêt opérationnel est à ce point minime qu'il n'est jamais enregistré dans la banque de données opérationnelle.
[61] Définies par la loi susmentionnée du 19 octobre 2023 comme des *« caméras individuelles ».*

avaient été testées ni si elles seraient éventuellement encore utilisées à l'avenir, il a posé le 25.04.2023 quelques questions additionnelles.

35. D'après la réponse, la SPN-Côte a testé du 14.06.2019 au 17.07.2019 cinq modèles de *bodycams* durant des missions d'intervention.

36. Le COC tient à souligner que la LFP (et la LPD) ne prévoi(en)t aucun régime légal pour le 'test' de caméras. Les *bodycams* doivent déjà répondre avant leur achat et leur utilisation à toutes les conditions légales et obligations d'homologation. La SPN-Côte peut éventuellement réaliser des tests avec le fournisseur sur la base de l'un des motifs de légalité du Titre 1er de la LPD et dans le respect de toutes les conditions, dont l'obligation d'information.

37. Attendu que la SPN-Côte n'utilise plus de *bodycams* depuis le 17.07.2019, le COC n'a pas été en mesure d'effectuer d'autres constatations.

4.1.1.2. En ce qui concerne les caméras *ANPR*

38. D'après les premiers éléments de réponse, la SPN-Côte a utilisé une caméra mobile *ANPR* sur la ligne du ferry de Zeebrugge. L'intérêt opérationnel de ce déploiement a disparu du fait de la suppression de la ligne du ferry et de la mise en place du bouclier *ANPR* autour du port. En raison de problèmes techniques, la caméra *ANPR* n'aurait cependant jamais été utilisée au sein de la SPN-Côte, de sorte que le COC n'a pas pu effectuer de constatations à ce sujet.

4.1.1.3. En ce qui concerne les *drones*

39. Un autre type de caméras mobiles est celui des caméras montées sur des drones. D'après les premiers éléments de réponse de la Direction de la SPN, les images des drones sont conservées pendant maximum 30 jours et aucune journalisation n'a été prévue (voir plus loin le point 4.1.4 relatif à la conservation et à la journalisation).

4.1.2. Caméras fixes

4.1.2.1. En ce qui concerne les caméras surveillant les accès maritimes et les caméras de la Région flamande

40. D'après les premiers éléments de réponse de la Direction de la SPN, le CIM de la SPN utilise des caméras dans les ports de plaisance et des caméras (gérées par la Région flamande) à hauteur des accès maritimes.

41. Le propre système de caméras de la SPN dans les ports de plaisance n'est pas encore opérationnel du fait que l'interconnexion avec le *VMS*[62] n'a pas encore été réalisée. Au moment de la visite, il y avait seulement des caméras dans le port de Nieuport et aucune n'avait encore été placée à Ostende, Blankenberge et Zeebrugge. Jusqu'au jour de la visite, les images des caméras installées dans les ports de plaisance et gérées par la SPN-Côte n'étaient pas visibles au CIM de la SPN[63]. Lorsque les images seront visibles au CIM de la SPN, elles pourront selon la Direction de la SPN être consultées uniquement au moyen d'un identifiant individuel et d'un mot de passe. Les images ne seront pas partagées ni mises à la disposition de tiers, à l'exception de la police fédérale, du procureur du Roi et/ou du juge d'instruction.

42. Selon la réponse du CIM de la SPN, il existe deux systèmes de caméras distincts. Les caméras de la Région flamande servent des finalités de sécurité – dont l'accompagnement maritime – et sont installées aux entrées des ports. Leurs images sont partagées par le biais d'une application web et sont accessibles au CIM de la SPN, mais ne sont pas enregistrées sur le serveur de la police. Les images sont uniquement enregistrées sur le serveur du Centre Maritime de Sauvetage et de Coordination (MRCC[64]). La Douane et la Défense disposent au CIM d'un accès propre au réseau de caméras de la Région flamande.

43. Le CIM de la SPN a indiqué avoir accès en temps réel au réseau de caméras de la Région flamande. (…) Le COC a pu constater lors de la visite qu'une demande devait être adressée au MRCC pour faire s'afficher sur les écrans les images des caméras de la Région flamande. Les possibilités de ces caméras se sont cependant révélées limitées étant donné qu'elles ne peuvent être dirigées (orientées) que de manière très limitée et, là aussi, uniquement après une intervention du MRCC.

44. Lors de la visite, le COC a constaté que les images des caméras gérées par la Région flamande sont affichées sur les écrans du local du CIM. Les fonctionnaires de police du CIM de la SPN sont présents physiquement au milieu du local, entourés de collaborateurs de la Défense et de la Douane qui disposent de leur propre accès direct aux images

---

[62] ***V**ideo **M**anagement **S**ystem*.
[63] On entend par CIM de la SPN les membres de la Police de la navigation qui sont rattachés au CIM établi à Zeebrugge.
[64] Le MRCC forme avec le CIM la centrale de la garde côtière, Centrale Garde Côtière | Garde côtière (kwgc.be).

de la Région flamande. Les images sont par conséquent visibles pour toutes les personnes présentes dans le local. Si les images apparaissent uniquement sur les moniteurs du collaborateur de la SPN, le collaborateur de la Défense ou de la Douane a, de par sa position, lui aussi accès à ces images. Les images des caméras sont consultées par les opérateurs du CIM de la SPN à des fins policières, par exemple pour soutenir des actions ou diriger des interventions.

45. Le CIM de la SPN se trouve dans une situation très précaire. La SPN utilise des caméras qui ne sont pas gérées par la police (mais bien par la Région flamande) et un local de dispatching qui ne fait pas partie de la police (le CIM), où le fonctionnaire de police du CIM de la SPN se trouve en compagnie d'opérateurs de la Défense et de la Douane, chacun dans le cadre de l'exercice de ses compétences légales. Il ne s'agit donc pas d'une situation relevant de l'application de l'article 5 §4 de la loi relative aux caméras du 21 mars 2007, dans laquelle les images des caméras d'une autorité (la Région flamande) sont visionnées en temps réel sous la surveillance de la police alors que cette autorité (la Région flamande) est le responsable du traitement des images.

Il ne s'agit pas non plus d'une situation visée à l'article 25/5 §2 de la LFP, dans laquelle les images de caméras de police relevant de l'application de la LFP sont, sous la surveillance du CIM de la SPN, visionnées en temps réel également par d'autres personnes dans le cadre de leur compétence légale, sauf dans les cas prévus par la loi. Dans ce scénario, des images de caméras de police sont donc visionnées en temps réel par des tiers (Défense et Douane), ce qui n'est donc pas le cas en l'occurrence.

46. Tout comme la SPN, l'Organe de contrôle est d'avis que le CIM de la SPN se trouve dans une situation telle que visée à l'article 25/1 §2 de la LFP. Le CIM de la SPN utilise en effet des images de caméras qui ont été installées par un autre responsable du traitement en application de la loi relative aux caméras du 21 mars 2007 ou d'autres lois, et qui sont donc également traitées (utilisées) par le CIM de la SPN. De ce fait, cette utilisation de caméras par le CIM de la SPN relève de l'application de la LFP.

Recommandation n° 1
À l'heure actuelle, le CIM de la SPN se trouve dans une situation très précaire du point de vue légal. L'Organe de contrôle recommande par conséquent à la Direction de la SPN d'examiner lors du déploiement de son propre système de caméras si – et, dans l'affirmative, dans quelle mesure – ce service de police, dans un « local de dispatching » commun occupé également par des services ne faisant pas partie de la police, octroie ou peut octroyer de manière générale et systématique à ces entités l'accès aux images de caméras de police dont la Direction de la SPN est le responsable du traitement comme prévu par la LFP. Il est recommandé de faire part à l'Organe de contrôle de la conclusion de cette analyse et de la décision prise à cet égard par la Direction de la SPN.

Requête n° 1
Le COC prie la Direction de la SPN d'informer l'Organe de contrôle dès que le système de caméras de police de la SPN-Côte sera opérationnel.

4.1.2.2. En ce qui concerne les caméras installées dans les cellules de police

47. Selon les premiers éléments de réponse, la SPN-Côte utilise des caméras dans les cellules de police. Lors de la visite sur place, le COC a constaté que des caméras étaient présentes tant dans les cellules de police individuelles que dans la cellule de police collective. Le COC a constaté que les images, comme indiqué par la SPN-Côte, sont uniquement visibles pour le personnel de police. Les caméras installées dans les cellules de police n'enregistrent pas de son.

48. Les bâtiments de la SPN-Côte sont équipés des pictogrammes réglementaires requis signalant la surveillance par caméra.

4.1.2.3. En ce qui concerne les caméras installées dans les locaux d'audition

49. Selon les premiers éléments de réponse, une AIPD est en cours au sein de la SPN-Côte pour l'utilisation de caméras dans les locaux d'audition.

50. Lors de la visite, le COC a constaté que les caméras qui étaient présentes dans les locaux d'audition filment en permanence, mais n'enregistrent pas de son. Bien que l'enregistrement des images filmées dans les locaux d'audition doive être activé en appuyant sur un bouton, les caméras filment donc de toute façon.

51. Selon la SPN-Côte, les concertations confidentielles entre un suspect et son avocat n'ont pas lieu dans les locaux d'audition. Un local distinct est mis à disposition pour ces concertations confidentielles, comme le COC a d'ailleurs pu le constater par lui-même.

52. Comme le COC le disait déjà dans son rapport DIO21001[65], l'exercice généralisé, non différencié et **systématique de la surveillance par caméra dans les locaux d'audition est disproportionné et donc illicite**. Une simple notification à la personne auditionnée à des fins de transparence ne suffit pas et l'autorisation de la personne entendue ne peut pas non plus servir de fondement juridique[66]. La surveillance par caméra est possible uniquement **dans des circonstances concrètes justifiant la nécessité du recours à la surveillance par caméra pour pouvoir garantir la sécurité de toutes les personnes concernées et des personnes présentes dans le commissariat de police**.

Bien qu'il ne fût pas question d'enregistrement de communications dans les locaux d'audition, il convient par souci d'exhaustivité de faire remarquer que l'audition audiovisuelle est régie strictement par le chapitre VII*quater* (en particulier, l'article 112*ter*) du Code d'instruction criminelle, en plus des dispositions relatives à l'audition audiovisuelle pour les mineurs, qui est régie dans les articles 92 à 103 du Code d'instruction criminelle. Une audition audiovisuelle ne peut se faire que si elle est ordonnée par le procureur du Roi ou le juge d'instruction et suivie de toutes les modalités et formalités prévues dans les articles précités. Il n'appartient donc **pas** à la police de le faire d'office. Nous n'entendons par là ni de filmer (sans enregistrement) une audition (sauf pour des raisons de sécurité et donc dans le cadre de la fonction de police administrative) et moins encore d'enregistrer et, *ergo*, de filmer (et conserver) une concertation confidentielle dans un tel local d'audition.

Sur la base de ce qui précède, le COC avait donc l'intention d'imposer une mesure correctrice afin de faire cesser immédiatement ce traitement.

Dans le cadre de la phase de la prélecture, le COC a toutefois reçu une réponse de la Direction de la SPN comme quoi les caméras de surveillance des locaux d'audition ont dans l'intervalle été définitivement désactivées dans le système de gestion. Additionnellement, les caméras ont été recouvertes de ruban adhésif afin que les personnes entendues voient bien que ces caméras sont hors service. Par souci d'exhaustivité, la Direction de la SPN a également indiqué qu'une mesure similaire avait été prise auprès de la SPN-Anvers qui recourait jusqu'alors au même procédé. Les chefs de service de la SPN ont également été informés et avertis de l'interdiction de traitement le 01.03.2024.

Vu les mesures prises par la Direction de la SPN, la mesure correctrice projetée est désormais sans objet.

4.1.2.4. En ce qui concerne (...)

53. (...)

4.1.3. En ce qui concerne l'AIPD, les directives internes et les évaluations concernant les caméras

54. Préalablement à l'utilisation des caméras susmentionnées, il convient d'accomplir un certain nombre de formalités : l'établissement d'une AIPD, l'obtention de l'autorisation pour l'utilisation des caméras et, le cas échéant, l'établissement de directives internes. Une AIPD contient au moins une description générale des traitements visés et une évaluation des risques pour les droits et libertés des personnes concernées, des mesures visées en limitation des risques, des mesures de précaution, des mesures de sécurité et des mécanismes qui ont été amorcés pour protéger les données à caractère personnel. Dans le présent rapport de contrôle, le COC formule pour chaque AIPD fournie et les documents y afférents quelques remarques générales *prima facie*.

4.1.3.1. Les caméras installées dans les locaux d'audition

55. Aucune AIPD n'a été transmise au COC concernant les caméras installées dans les locaux d'audition.

Recommandation n° 2

Le COC recommande à la Direction de la SPN d'établir l'AIPD visée à l'article 58 de la loi relative à la protection des données pour les caméras installées dans les locaux d'audition et de la transmettre au COC.

[65] https://www.organedecontrole.be/files/DIO21001_Contr%C3%B4le_Restreint_Camera_Locale_Audition_F.pdf.
[66] Le consentement ne peut jamais être un motif juridique valable pour un traitement policier opérationnel ; il doit toujours y avoir une base légale (ou, éventuellement, réglementaire) expresse régissant le cas échéant les circonstances dans lesquelles et la manière dont le consentement de la personne concernée peut être obtenu (cf. art. 33 §1er, 1° et 2° de la LPD ; considérant 35 de la *LED*).

4.1.3.2. les *bodycams*/les caméras individuelles

56. En ce qui concerne l'utilisation des *bodycams*, le COC a reçu une AIPD, une note interne temporaire et une évaluation de ces *bodycams*.

57. L'AIPD a été établie en 2018 pour le test des *bodycams* à la fois pour la DAS[67], la DAH[68] et la SPN. Il ressort de cette AIPD que des données biométriques seraient traitées et que les *bodycams* pouvaient durant la phase de test être utilisées sur la base de profils standard plutôt que de profils individuels, de sorte qu'il n'était pas possible de créer des fichiers de journalisation à part entière. Le traitement de données biométriques a toutefois été démenti lors de la visite sur place.

Selon l'AIPD, les *bodycams* réalisent un enregistrement de 30 secondes avant leur activation, ce que l'on appelle le 'mode mémoire tampon'. Dans son rapport CON19008[69], le COC indiquait que l'utilisation d'un 'mode mémoire tampon' est en principe illicite dès lors que l'utilisation effective de la *bodycam* doit être annoncée par un avertissement oral préalable émanant du fonctionnaire de police. Il va de soi que cette condition légale ne peut pas être respectée lorsque la caméra traite déjà des images avant que l'avertissement ne soit donné à la personne filmée. Ce problème ne se pose cependant plus depuis l'entrée en vigueur, le 20 janvier 2024, de la loi du 19 octobre 2023 puisque le pré-enregistrement de 30 secondes est désormais prévu explicitement dans la LFP et a même été rendu obligatoire[70].

58. Il ressort de la note interne temporaire qu'en marge des missions d'intervention, il a également été procédé à des enregistrements de test. La note ne permet toutefois pas de déterminer clairement s'il a seulement été procédé à des enregistrements de test, ni si ceux-ci ont été réalisés dans le cadre des missions opérationnelles ou à d'autres moments. Lors de la visite, le COC a été informé que les tests avaient été réalisés dans l'espace public[71] à Zeebrugge et que rien n'avait été enregistré durant des missions opérationnelles, ce qui contredit ce qui avait été initialement affirmé dans les premiers éléments de réponse.

59. Dans l'évaluation des *bodycams*, le COC peut lire que la SPN-Côte part du principe que la *bodycam* ne peut pas être utilisée par la SPN pour les contrôles aux frontières (article 21 de la LFP[72]). Elle se réfère à ce sujet à l'article 25/3 §2 de la LFP[73]. Le COC tient à souligner que l'objectif de cet article semble être d'éviter la discrimination. Cet article n'exclut pas que les caméras soient utilisées pour des missions de police judiciaire, dont la recherche d'illégaux dans le cadre de la traite et du trafic d'êtres humains, de sorte qu'il s'agit clairement de la détection d'infractions auxquelles l'exclusion de l'article 25/3 §2 de la LFP ne s'applique pas. Il n'est pas non plus exclu qu'une intervention de police comporte une dimension de police administrative. Une intervention ne vise alors pas en soi les étrangers, mais bien le maintien de l'ordre public dans le cadre, par exemple, d'un contrôle de police d'illégaux se trouvant sur la plage ou de personnes présentes dans le port dans le but de rejoindre le Royaume-Uni par bateau. Pour le service de police qui effectue l'intervention, il n'est donc pas établi *ab initio* et juridiquement qu'il s'agit d'étrangers et l'intervention ne vise *ab initio* pas des étrangers en tant que tels, mais bien des personnes qui semblent ne pas respecter la législation sur les étrangers. La situation semble différente dans l'hypothèse où la caméra serait, en dehors de la détection du séjour illégal en Belgique et du concours apporté à ce séjour illégal, utilisée en vue de la surveillance préventive par exemple des habitudes de vie (occupations) d'étrangers (en un lieu donné). Ce dernier cas semble être un exemple plus plausible d'une finalité potentiellement exclue visée par l'article 25/3 §2 de la LFP, et donc une situation induisant un risque de traitements d'images discriminatoires (délibérés ou non).[74]

60. Il ressort du rapport d'évaluation des *bodycams* que les utilisateurs avaient quelques objections fondamentales, dont le fait que les images sont conservées sur les caméras et y restent accessibles pour n'importe quel membre de la SPN-Côte et le fait qu'il existait une possibilité que les images des caméras soient consultées par un « sous-traitant », à savoir la firme X. Le COC partage ces inquiétudes et s'inquiète au plus haut point du fait qu'il était question – ou qu'il aurait été question – d'une possibilité que les images des caméras soient consultées en direct par un « sous-traitant », à savoir la firme X, mais il n'a pas pu le constater par lui-même.

---

[67] DAS : Direction de la sécurité publique.
[68] DAH : Direction de la police de la route.
[69] https://www.organedecontrole.be/files/CON19008_Avis_dOffice_COC_Bodycam_F.PDF.
[70] Articles 2, b) et 3, c) de la loi du 19 octobre 2023.
[71] Selon le régime prévu pour l'utilisation de caméras dans la LFP, le terme juridique est *« lieu ouvert »* (art. 25/2 §1er, 4°).

[72] Art. 21 de la LFP : *« (Les services de police) veillent au respect des dispositions légales relatives à l'accès au territoire, au séjour, à l'établissement et à l'éloignement des étrangers. (Ils) se saisissent des étrangers qui ne sont pas porteurs des pièces d'identité ou des documents requis par la réglementation sur l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers, et prennent à leur égard les mesures prescrites par la loi ou par l'autorité compétente. »*.
[73] Art. 25/3 §2 de la LFP : *« L'utilisation visible des caméras pour le recueil de l'information de police administrative visée à l'article 44/5 §1er, n'est autorisée que dans les hypothèses visées à l'article 44/5 §1er, alinéa 1er, 2° à 6°. En ce qui concerne l'article 44/5 §1er, alinéa 1er, 5°, cette utilisation ne peut en outre être autorisée qu'à l'égard des catégories de personnes visées aux articles 18, 19 et 20. »*.
[74] Cf. Doc. Parl. *Chambre*, n° DOC 54-2855/001, p. 21.

61. De surcroît, le COC remarque qu'il relève de la responsabilité de la Direction de la SPN de vérifier s'il est question dans le cadre de l'utilisation de caméras de police d'une relation entre un responsable du traitement et un sous-traitant et, dans l'affirmative, d'établir si une convention de sous-traitance doit être conclue (articles 53 et suivants de la LPD). Il fait par ailleurs observer que le projet de traiter certaines catégories (particulières) de données à caractère personnel doit correspondre à l'intention effective de la SPN. Le but n'est donc pas de faire mention dans l'AIPD du traitement de données biométriques alors que ce n'était/n'est en réalité pas l'intention, comme l'a constaté le COC. Selon la réponse formulée par la Direction de la SPN durant la phase de prélecture, le projet pilote se déroulait sous la responsabilité de la Direction générale de la police administrative (DGA) de la police fédérale, dont la SPN fait partie. Cela dit, cela n'empêche évidemment pas que la SPN traite ces images en vue de ses propres finalités.

4.1.3.3. Les *ANPR*

62. Une AIPD a également été transmise pour les caméras mobiles *ANPR*, qui ne sont plus en usage au sein de la SPN-Côte. Dans cette AIPD, le COC pouvait par exemple lire qu'auprès du PC et de la clé USB se trouve une fiche de procédure plastifiée faisant mention de l'identifiant et du mot de passe. Selon l'AIPD, il s'agirait là d'un *« risque négligeable »*. Attendu que d'autres sections de la Direction de la SPN utilisent des caméras *ANPR* mobiles, le COC se pose de sérieuses questions quant à l'évaluation du risque et aux mesures de sécurité.

Recommandation n° 3
Attendu que d'autres sections de la SPN utilisent des caméras ANPR mobiles, le COC recommande à la Direction de la SPN d'actualiser cette AIPD et de dûment tenir compte des mesures de sécurité nécessaires et d'usage concernant l'accès aux données ANPR et leur utilisation.

4.1.3.4. Les *drones*

63. En ce qui concerne l'utilisation des drones, le COC a reçu un document *« Flux de données interne »* et une AIPD relative aux *drones*. Il en ressort que la direction utilise des *drones* qui recourent à chaque fois à une seule caméra pour toutes les actions (pilotage, infrarouge et caméra ordinaire). Il n'y a pas d'enregistrement de son et la communication entre le pilote et l'opérateur n'est pas enregistrée non plus.

64. Pour montrer qu'il s'agit d'un *drone* de la police, des insignes reconnaissables ont été apposés sur le *drone*. En réalité, il s'agit d'un autocollant portant la mention *« politie Kust »*. Le COC fait observer – et est rejoint en cela par la SPN – que comme le *drone* vole à 90 mètres d'altitude, cette mention n'est en réalité pas visible et que le *drone* n'est donc pas identifiable comme un drone de police.

65. L'AIPD ne précise pas les lieux où le déploiement des *drones* est envisagé. Lors de la visite, il a été dit que le lieu et les modalités du déploiement dépendaient de la mission. La SPN s'acquitte de missions pour tous les services de police locaux et fédéraux qui le demandent, ainsi que pour des services externes comme les pompiers, la Douane, etc. … Initialement, les demandes sont adressées à l'Appui aérien (DAFA), mais lorsque celui-ci ne peut pas fournir l'assistance requise, les zones de police de Flandre occidentale et la SPN sont sollicitées. Actuellement, l'objectif premier est d'utiliser les *drones* pour des missions de police administrative.

Recommandation n° 4
Attendu que le drone n'est dans la pratique pas identifiable comme un drone de police, le COC recommande à la Direction de la SPN de vérifier s'il existe une manière plus transparente de rendre le drone mieux identifiable à une altitude de 90 mètres. Le COC renvoie à ce sujet à une solution pratique qui est proposée au point 44 du rapport du COC du 15 mars 2022 intitulé « Contrôle thématique et avis d'initiative relatifs à l'utilisation, par la police intégrée, de caméras montées sur des drones » (DIO20009/1)[75]*.*

Recommandation n° 5
Le COC recommande à la Direction de la SPN d'actualiser cette AIPD consacrée aux drones en fonction de l'usage effectif qui est fait des drones.

Recommandation n° 6
Attendu que l'on est passé au système de streaming de DAFA – qui inclut l'enregistrement des images – et que les dossiers en Teams ne sont plus utilisés, le COC recommande à la SPN-Côte de supprimer en Teams les dossiers désormais inutilisés.

4.1.3.5. Caméras fixes installées dans les ports de plaisance

[75] Disponible sur le site www.organedecontrole.be/publications/rapports.

66. En ce qui concerne les caméras fixes installées dans les ports de plaisance, le COC a reçu une AIPD et une note d'instructions. Selon la note d'instructions, il a été mis un terme à l'accès en temps réel aux caméras de la Région flamande en raison du manque de clarté quant à l'existence d'une convention avec le gestionnaire, à savoir le MRCC, et du fait qu'il n'avait pas été établi d'AIPD. Dans la réponse, il est indiqué que l'accès en temps réel était en passe de disparaître et qu'il y serait mis un terme lorsque les caméras seraient (actives) en gestion propre. Lors de la visite, le COC a été informé que l'accès aux images des caméras gérées par le MRCC n'était possible qu'en cas de nécessité et moyennant une demande adressée au MRCC. Auparavant, les opérateurs du CIM de la SPN avaient eux-mêmes la possibilité de visionner ces images en temps réel par le biais d'une application web qui fonctionnait avec un identifiant générique attribué par le MRCC. Les caméras de la Région flamande ne sont pas gérées par la Police de la navigation.

67. À la lecture de l'AIPD, le COC constate que les images des caméras en gestion propre seront visibles au dispatching de Nieuport et d'Ostende afin de permettre de diriger les équipes dans le cadre des contrôles des frontières et pour les *call takers*[76] du CIC de Flandre occidentale en cas d'appel d'urgence ou d'agissements suspects. Le CIM obtiendrait quant à lui un accès intégral. Cette situation précaire a déjà été abordée aux points 45 et 46 et assortie d'une recommandation, et nous y revenons également au point 93.

Lors de la visite, le COC a appris que ces caméras étaient braquées sur les ports de plaisance de manière à pouvoir voir où un bateau va accoster afin de pouvoir au besoin le soumettre à un contrôle. Les caméras permettent de zoomer jusqu'à voir à l'intérieur des cabines/parties privatives des bateaux. Selon la Direction de la SPN, le but n'est cependant pas de mettre en place une surveillance d'un bateau donné. Cependant, le COC déduit de cette possibilité de zoomer qu'il existe un risque que des données à caractère personnel puissent être traitées, intentionnellement ou non, ce qui peut constituer une violation de l'article 8 de la Convention européenne des droits de l'homme[77], qui garantit le droit à la protection de la vie privée.

68. Le COC fait remarquer qu'il appartient à la Direction de la SPN de paramétrer la portée des caméras de manière à ce qu'elle réponde à l'exigence de proportionnalité.

4.1.3.6. Caméras installées dans les cellules de police

69. En ce qui concerne les caméras installées dans les cellules de police, le COC a reçu un manuel intitulé *« Utilisation et surveillance des lieux de détention de la SPN-Côte »*. Il ressort de ce manuel qu'une surveillance par caméra permanente est prévue dans les cellules. Les images des cellules occupées doivent être projetées et surveillées sur ces écrans par le personnel présent. Lors de la visite sur place, la SPN-Côte a fait savoir que les images n'étaient pas enregistrées. Le COC constate toutefois que l'on peut déduire du manuel que l'objectif est d'enregistrer les images des caméras étant donné qu'il y est question de différents profils donnant accès aux images. De plus, la loi du 19 octobre 2023 fait de la conservation des images des caméras installées dans les lieux de détention une obligation légale, ne serait-ce que pour une période minimale de trente jours (article 5, qui modifie l'article 25/6 de la LFP et y ajoute un 2e alinéa), et ce au plus tard à partir du 20 novembre 2025 (article 13). Quoi qu'il en soit, il relève également de la responsabilité de la SPN de veiller à ce que les enregistrements dans le registre REGPOL correspondent à la réalité (art. 55 de la LPD *juncto* 145 de la LPI).

70. Une AIPD aurait déjà été établie pour les caméras installées dans les cellules de la section Y de la SPN-Côte, mais elle n'a pas été validée ni transmise au COC. Une AIPD est en cours d'élaboration pour les caméras installées dans les cellules de la section X de la SPN-Côte.

Requête n° 2
Le COC prie la direction de la SPN de transmettre les AIPD pour les caméras installées dans les cellules de police des sections X et Y de la SPN-Côte au COC dans les trois mois de la réception du présent rapport.

Recommandation n° 7
Vu les contradictions entre d'une part ce qui a été dit et constaté pendant et après la visite du COC et d'autre part ce qui figure dans le manuel intitulé « Utilisation et surveillance des lieux de détention de la SPN-Côte » qui a été soumis au COC, le COC recommande d'actualiser ce manuel.

[76] Il s'agit des membres du personnel de la police fédérale et de la police locale qui sont visés dans l'arrêté royal du 26 juin 2002 concernant l'organisation des centres de dispatching centralisés et du point de contact national.

4.1.4. En ce qui concerne les délais de conservation des images et des informations recueillies au moyen des caméras

71. En ce qui concerne les délais de conservation des images des caméras montées sur des *drones*, le COC constate une potentielle contradiction entre le document *« Flux de données interne »* (pièce 48) et l'AIPD relative aux *drones* (pièce 21). Selon le document *« Flux de données interne »*, les images administratives sont transmises dans les 30 jours et sont ensuite soit supprimées, soit conservées pendant 12 mois dans les archives. L'AIPD faisait quant à elle uniquement mention d'un délai de conservation de 30 jours. Le COC lit par ailleurs qu'il ne faut pas spécifier de motif de consultation pour visionner les images. Selon la SPN, le système de la transmission dans les 30 jours au service de police ayant sollicité l'appui était utilisé à l'époque où l'on recourait à un stockage local.

Lors de la visite, le COC a appris que seul le système de streaming de DAFA[78] est désormais utilisé. Avec ce système, les images sont collectées dès le décollage du *drone* et transmises en temps réel au serveur de DAFA. Les images sont conservées pendant un an et ne sont plus accessibles au bout de 30 jours si ce n'est moyennant une apostille. Au terme du délai de conservation d'un an, les images sont automatiquement effacées. Avant l'introduction du système de streaming de DAFA, il était recouru à un stockage local avec des dossiers par pilote en *Microsoft Teams*, auxquels seuls le pilote et le coordinateur des *drones* avaient accès. Le contrôle de ces dossiers incombait au coordinateur des *drones*. Ces dossiers en *Teams* existent encore, mais sans les images étant donné que celles-ci étaient effacées au bout de 30 jours.

72. Depuis avril 2021, toutes les opérations et manipulations – comme la connexion, la consultation et le transfert des images – sont journalisées dans le système. Il existe à présent trois profils d'utilisateurs. Cependant, il n'a pas été prévu dans le système d'exiger la spécification d'un motif de consultation.

73. (…).

Recommandation n° 8
Vu la possibilité de consulter/revisionner les images, le COC recommande de prévoir techniquement que le système exige la spécification d'un motif de consultation.

4.1.5. En ce qui concerne la consultation des images et des informations recueillies au moyen des caméras

74. La journalisation fonctionne actuellement sur la base du numéro de matricule[79] avec des identifiants individuels permettant d'accéder aux images dont la distribution et la gestion sont assurées par DAFA. En ce qui concerne la consultation des images, le COC lit dans l'AIPD qu'aucun motif de consultation ne doit être spécifié. Cette absence de motivation est manifestement contraire à l'article 56 §1er, 1° de la LPD et aux articles 25/7 §1er, 3e alinéa et 44/4 §2 de la LFP, qui prévoient explicitement que le motif de consultation doit être spécifié et être traçable (contrôlable). Il s'agit donc d'une obligation légale dans le chef du responsable du traitement.

4.1.6. En ce qui concerne la convention de sous-traitance pour les *drones*

75. Selon l'AIPD, une convention de sous-traitance a été conclue avec la S.A. X. Selon les réponses apportées aux questions additionnelles, cette convention aurait été conclue au niveau de DAFA. Lors de la visite, il a été dit que tous les aspects de la convention de sous-traitance et de la gestion des accès aux serveurs passaient par la DRI[80]. Selon la Direction de la SPN, la S.A. X. est en charge de la maintenance des serveurs mais n'est pas en mesure de consulter quoi que ce soit au niveau du contenu.

Requête n° 3
Le COC prie la Direction de la SPN de transmettre dans le mois de la réception du présent rapport au COC la convention de sous-traitance conclue avec la firme X.

4.2. Banques de données et banques de données particulières

76. Lors de l'annonce de la visite, le COC a interrogé la Direction de la SPN au sujet des banques de données en usage, y compris les banques de données particulières.

[78] DAFA = Direction de la police administrative – Force Aérienne (Appui aérien).
[79] Un numéro de matricule est un numéro unique qui identifie un membre du personnel de la police intégrée.
[80] La DRI est la Direction de l'information policière et des moyens ICT de la police fédérale.

77. (…).

78. (…).

79. (…).

80. (…).

81. (…).

82. (…).

83. (…).

84. En ce qui concerne les banques de données en usage auprès de la SPN, il a été convenu lors de la visite sur place d'accorder à la SPN un certain délai pour établir une liste actuelle et une analyse fonctionnelle des banques de données utilisées par ses services.

Requête n° 4
Le COC prie la SPN de transmettre un ***nouvel état des lieux général*** *concernant les* ***banques de données particulières****, et ce au plus tard dans les 3 mois de la réception du présent rapport.*

Recommandation n° 9
Les données peuvent uniquement être traitées si elles présentent encore un caractère adéquat, pertinent et non excessif. Le COC recommande de prévoir pour les ***banques de données particulières*** *une* ***évaluation régulière*** *et des* ***délais de conservation****.*

Recommandation n° 10
Pour la consultation des ***banques de données particulières****, le COC recommande de prévoir un* ***champ libre*** *permettant de saisir le* ***motif de consultation****. L'utilisation d'une case à cocher ne suffirait pas à obtenir un motif identifiable et à satisfaire aux exigences légales des articles 56 §1er, 2° et 3° de la LPD juncto 44/4 §2 et 44/11/3 §4 de la LFP.*

Mesure correctrice

85. Il découle de ce qui précède que la SPN n'a pas ou pas suffisamment examiné si les banques de données particulières considérées par la SPN répondent aux conditions de l'article 44/11/3 de la LFP. Une banque de données particulière ne peut par exemple pas être en même temps une banque de données de base au sens de la LFP. Par ailleurs, l'identité du responsable du traitement de la banque de données particulière doit être clairement établie. Comme pour les autres banques de données policières, le traitement des informations et données à caractère personnel policières doit présenter un caractère adéquat, pertinent et non excessif (article 44/1 §1er de la LFP). Le fait que les informations et données à caractère personnel puissent être 'intéressantes' pour la SPN ne constitue pas non plus une base légale permettant de conserver ces données. En conséquence, la SPN doit mettre le traitement de données à caractère personnel dans une banque de données particulière en conformité avec la LPD et la LFP. Lorsque la création d'une banque de données particulière ne remplit pas les conditions prévues à l'article 44/11/3 de la LFP, la conservation d'informations et de données à caractère personnel dans cette banque de données est illicite.

Mesure correctrice

L'Organe de contrôle ordonne au directeur de la SPN de mettre les informations et données à caractère personnel dans les banques de données particulières créées par la SPN en conformité avec l'article 33 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et avec les articles 44/1 §1er et 44/11/3 de la loi du 5 août 1992 sur la fonction de police.

Vu la nature et la gravité de l'infraction, il est nécessaire et proportionnel d'ordonner l'établissement d'une analyse fonctionnelle pour les banques de données particulières, conformément aux modalités décrites dans le dispositif du présent rapport.

4.3. Triptyque

86. Une bonne gestion de l'information policière est entièrement tributaire de l'accomplissement correct d'une série d'actes de base, dont le triptyque. Lors de la visite sur place, un contrôle par échantillonnage restreint a été effectué auprès du service de gestion fonctionnelle de la SPN-Côte, dans le cadre duquel le COC a consulté au hasard un nombre

arbitraire de procès-verbaux en *ISLP*. Il en est ressorti qu'un numéro AFIS[81] a pu être retrouvé pour chaque procès-verbal, ce qui permet de conclure que le triptyque est réalisé et enregistré de manière correcte et satisfaisante.

4.4. Validation centrale ou 'option 35'

87. Un dernier aspect qui a été examiné avait trait à la réalisation de ce que l'on appelle une validation centrale[82] (option 35) au sein de la Direction de la SPN (SPN Ostende).

88. Les données structurées enregistrées principalement des procès-verbaux, des rapports d'information (RIR) et des fiches d'enquêtes (DOS) sont en fin de traitement enregistrées définitivement dans la BNG et peuvent donc être consultées (par le biais de l'application 'BNG-contrôle', 'BNG-consultation', …) et/ou modifiées (par le biais de l'enregistrement central), en fonction du profil de l'utilisateur. S'ils ne satisfont pas à certaines exigences de qualité, les enregistrements sont renvoyés au service concerné pour validation parce qu'une intervention humaine (autrement dit, un nouveau contrôle) est requise. Cela donne lieu à ce que l'on appelle des 'lignes ouvertes' ('rejets') au sein d'un service/d'une direction, s'agissant d'un indicateur de la mesure dans laquelle et de la rapidité avec laquelle ce service ou cette direction s'occupe (de la qualité) des enregistrements dans la BNG. Un **'gestionnaire fonctionnel'** de l'information doit être désigné au sein de chaque direction ou service. La mission du gestionnaire fonctionnel est cruciale pour une bonne gestion de l'information au niveau de la police locale et de certaines directions de la police fédérale ainsi que pour l'efficacité du flux d'informations vers les autres services de police (e.a. par le biais de la BNG) et donc pour le fonctionnement intégré global de la GPI. Toutes les entités de la SPN ont leur propre gestionnaire fonctionnel.

89. Afin de pouvoir contrôler la réalisation de la validation centrale par la SPN, le COC a demandé un point de la situation en date du 09.10.2023. Cet état des lieux a révélé qu'il n'y avait pas de lignes ouvertes, ni pour les procès-verbaux initiaux, ni pour les procès-verbaux subséquents.

90. Le COC peut en conclure qu'il est régulièrement procédé à la validation centrale ('option 35') au sein de la Direction de la SPN et que les données des banques de données de base sont transférées à la BNG correctement et dans le délai imparti.

5. CONCLUSION – REQUÊTES, RECOMMANDATIONS ET MESURES CORRECTRICES

91. Après l'annonce du contrôle technique, qui était principalement axé sur l'utilisation des caméras et des banques de données au sein de la SPN-Côte, la Direction de la SPN a commencé à transmettre des documents et des réponses concernant l'utilisation de caméras et les banques de données de base et particulières, ainsi que des documents généraux concernant la sécurité de l'information et le partage d'informations.

92. La SPN-Côte utilise plusieurs types de caméras fixes et mobiles. Selon les premiers éléments de réponse, il apparaît cependant que certaines caméras ne sont plus en usage et qu'il existe une certaine confusion quant à l'identité des responsables du traitement. Sur la base des réponses formulées initialement par la Direction de la SPN et des contradictions constatées, le COC estime pouvoir conclure que la Direction de la SPN ne dispose pas de connaissances suffisantes dans le domaine de l'utilisation de caméras ou n'y consacre pas suffisamment d'attention. D'un autre côté, il est apparu lors du contrôle que la Direction de la SPN fait indéniablement preuve de beaucoup de bonne volonté et est déterminée à faire en sorte que tous les traitements des caméras soient conformes à la législation en vigueur.

93. La Police de la navigation collabore dans le cadre du CIM avec plusieurs services externes, dont la Défense et la Douane. Le local du CIM se trouve toutefois dans les bâtiments de la Défense, ce qui place les collaborateurs de la SPN dans une situation de travail complexe en termes d'hébergement, en particulier en ce qui concerne la configuration du local dans lequel ces collaborateurs de la SPN travaillent physiquement au sein du CIM. Cette situation est aussi reconnue et confirmée par le délégué à la protection des données (DPO) et par les fonctionnaires de police habilités du CIM. En dépit de cette situation complexe, le COC est convaincu que la Direction de la SPN parviendra à trouver avec les services du ministère de la Défense une solution pour aménager le local de manière à ce que chaque service puisse poursuivre ses propres finalités conformément à la législation à laquelle il est soumis.

94. La sécurité de l'information requiert des efforts continus et de préférence une approche structurelle et un suivi périodique. La Direction de la SPN renvoie à ce sujet au cadre de sécurité de l'information de la police fédérale.

95. La SPN doit examiner la licéité des banques de données particulières qu'elle crée ainsi que des informations et données à caractère personnel qui y sont traitées. L'utilisation de ces banques de données doit être clairement décrite et les collaborateurs doivent être sensibilisés au sujet du cadre des recherches, du motif de consultation, etc. … Un suivi

[81] Numéro identique dans *ISLP* qui fait référence aux empreintes digitales relevées.
[82] Les données structurées enregistrées sont, à l'issue de leur préparation dans l'application locale (*ISLP*, enregistrement local, *FEEDIS*, …), transmises au niveau central où elles font l'objet d'un contrôle automatique.

adéquat, par le DPO, de la mise en œuvre de la sécurité de l'information en général au sein de la Direction revêt dans ce contexte une importance primordiale.

96. L'Organe de contrôle est d'avis qu'en dépit du constat qu'il y a encore matière à amélioration dans plusieurs domaines – dont certains relevaient du périmètre du présent contrôle –, la Direction de la SPN se montre déterminée à plancher sur ces aspects et à mettre en œuvre une politique adéquate en matière de sécurité de l'information. Le COC a également perçu chez les fonctionnaires de police qui ont participé à la visite une volonté manifeste de s'acquitter de leurs tâches correctement et conformément à la loi.

* * * * * *

PAR CES MOTIFS,

l'Organe de contrôle de l'information policière

A. prie la Direction de la SPN,

Requête n° 1
Le COC prie la Direction de la SPN d'informer l'Organe de contrôle dès que le système de caméras de police de la SPN-Côte sera opérationnel.

Requête n° 2
Le COC prie la direction de la SPN de transmettre les AIPD pour les caméras installées dans les cellules de police des sections X et Y de la SPN-Côte au COC dans les trois mois de la réception du présent rapport.

Requête n° 3
Le COC prie la Direction de la SPN de transmettre dans le mois de la réception du présent rapport au COC la convention de sous-traitance conclue avec X.

Requête n° 4
Le COC prie la SPN de transmettre un nouvel état des lieux général concernant les banques de données particulières, et ce au plus tard dans les trois mois de la réception du présent rapport.

B. adresse à la Direction de la SPN les recommandations suivantes,

Recommandation n° 1
À l'heure actuelle, le CIM de la SPN se trouve dans une situation très précaire du point de vue légal. L'Organe de contrôle recommande par conséquent à la Direction de la SPN d'examiner lors du déploiement de son propre système de caméras si – et, dans l'affirmative, dans quelle mesure – ce service de police, dans un « local de dispatching » commun occupé également par des services ne faisant pas partie de la police, octroie ou peut octroyer de manière générale et systématique à ces entités l'accès aux images de caméras de police dont la Direction de la SPN est le responsable du traitement comme prévu par la LFP. Il est recommandé de faire part à l'Organe de contrôle de la conclusion de cette analyse et de la décision prise à cet égard par la Direction de la SPN.

Recommandation n° 2
Le COC recommande à la Direction de la SPN d'établir l'AIPD visée à l'article 58 de la loi relative à la protection des données pour les caméras installées dans les locaux d'audition et de la transmettre au COC.

Recommandation n° 3
Attendu que d'autres sections de la SPN utilisent des caméras ANPR mobiles, le COC recommande à la Direction de la SPN d'actualiser cette AIPD et de dûment tenir compte des mesures de sécurité nécessaires et d'usage concernant l'accès aux données ANPR et leur utilisation.

Recommandation n° 4
Attendu que le drone n'est dans la pratique pas identifiable comme un drone de police, le COC recommande à la Direction de la SPN de vérifier s'il existe une manière plus transparente de rendre le drone mieux identifiable à une altitude de 90 mètres. Le COC renvoie à ce sujet à une solution pratique qui est proposée au point 44 du rapport du COC du 15 mars 2022 intitulé « Contrôle thématique et avis d'initiative relatifs à l'utilisation, par la police intégrée, de caméras montées sur des drones » (DIO20009/1)[83].

[83] Disponible sur le site www.organedecontrole.be/publications/rapports.

Recommandation n° 5
Le COC recommande à la Direction de la SPN d'actualiser cette AIPD consacrée aux drones en fonction de l'usage effectif qui est fait des drones.

Recommandation n° 6
Attendu que l'on est passé au système de streaming de DAFA – qui inclut l'enregistrement des images – et que les dossiers en Teams ne sont plus utilisés, le COC recommande à la SPN-Côte de supprimer en Teams les dossiers désormais inutilisés.

Recommandation n° 7
Vu les contradictions entre d'une part ce qui a été dit et constaté pendant et après la visite du COC et d'autre part ce qui figure dans le manuel intitulé « Utilisation et surveillance des lieux de détention de la SPN-Côte » qui a été soumis au COC, le COC recommande d'actualiser ce manuel.

Recommandation n° 8
Vu la possibilité de consulter/revisionner les images, le COC recommande de prévoir techniquement que le système exige la spécification d'un motif de consultation.

Recommandation n° 9
Les données peuvent uniquement être traitées si elles présentent encore un caractère adéquat, pertinent et non excessif. Le COC recommande de prévoir pour les banques de données particulières une évaluation régulière et des délais de conservation.

Recommandation n° 10
Pour la consultation des banques de données particulières, le COC recommande de prévoir un champ libre permettant de saisir le motif de consultation. L'utilisation d'une case à cocher ne suffirait pas à obtenir un motif identifiable et à satisfaire aux exigences légales des articles 56 §1er, 2° et 3° de la LPD juncto 44/4 §2 et 44/11/3 §4, 2e alinéa de la LFP.

C. ordonne les mesures correctrices suivantes à l'égard du directeur de la police fédérale, Direction de la SPN,

Considérant que le COC, en sa qualité d'autorité de contrôle, tient compte d'une part de la licéité des traitements de données (à caractère personnel) et de la gestion de l'information policière, et d'autre part du fonctionnement opérationnel de la police et de la continuité de la prestation de services en faveur du citoyen.

Considérant qu'une mesure correctrice vise à rétablir et à faire respecter la conformité aux dispositions du Titre 2 de la loi relative à la protection des données et de la loi sur la fonction de police.

Considérant que toute mesure correctrice prise par le COC doit être appropriée, nécessaire et proportionnée en vue de garantir le respect du Titre 2 de la loi relative à la protection des données, compte tenu des circonstances de l'espèce[84].

Considérant que l'article 247, 4° de la LPD confère à l'Organe de contrôle la compétence d'ordonner aux services de police ou à leur sous-traitant de mettre un traitement en conformité avec les dispositions de la réglementation relative au traitement des données à caractère personnel, le cas échéant, de manière spécifique et dans un délai déterminé. Qu'il peut être déduit de cette disposition de compétence que celle-ci prévoit que le COC peut prendre des mesures pour (faire) mettre un traitement illicite en conformité avec les dispositions et la réglementation relatives au traitement de données à caractère personnel. Que cette disposition confère au COC une compétence discrétionnaire pour, notamment, imposer ou non au responsable du traitement un délai qui soit nécessaire et proportionné, compte tenu des circonstances spécifiques de l'espèce, pour remédier à l'illicéité constatée.

Considérant que la mesure correctrice imposée ci-après prévoit un délai de six mois pour mettre les traitements de données dans les banques de données particulières créées par la Direction de la SPN ainsi que les informations et les données à caractère personnel traitées dans ces banques de données en conformité avec les articles 44/1 §1er et 44/11/3 de la loi sur la fonction de police.

Vu les articles 71 et 247, 4° de la loi relative à la protection des données.

Mesure correctrice

[84] Considérant 82 de la *LED*.

Le COC **ordonne** au directeur de la SPN de mettre dans les six mois de la réception du présent rapport les informations et données à caractère personnel dans les banques de données particulières créées par la SPN en conformité avec l'article 33 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et avec les articles 44/1 §1er et 44/11/3 de la loi du 5 août 1992 sur la fonction de police et de réaliser par ailleurs, vu la nature et la gravité de l'infraction, une analyse fonctionnelle des banques de données particulières dans un délai de 4 mois à compter de la réception du présent rapport.

* * * * * *

Dit pour droit que le délai de respectivement six (6) mois et quatre (4) mois prévu dans la mesure correctrice commence à courir à partir de la date de sa prise en connaissance, laquelle doit être comprise comme la date de l'accusé de réception du présent rapport définitif ou la date du cachet de la poste du courrier recommandé envoyé par l'Organe de contrôle, plus deux jours ouvrables (samedis et dimanches non inclus).

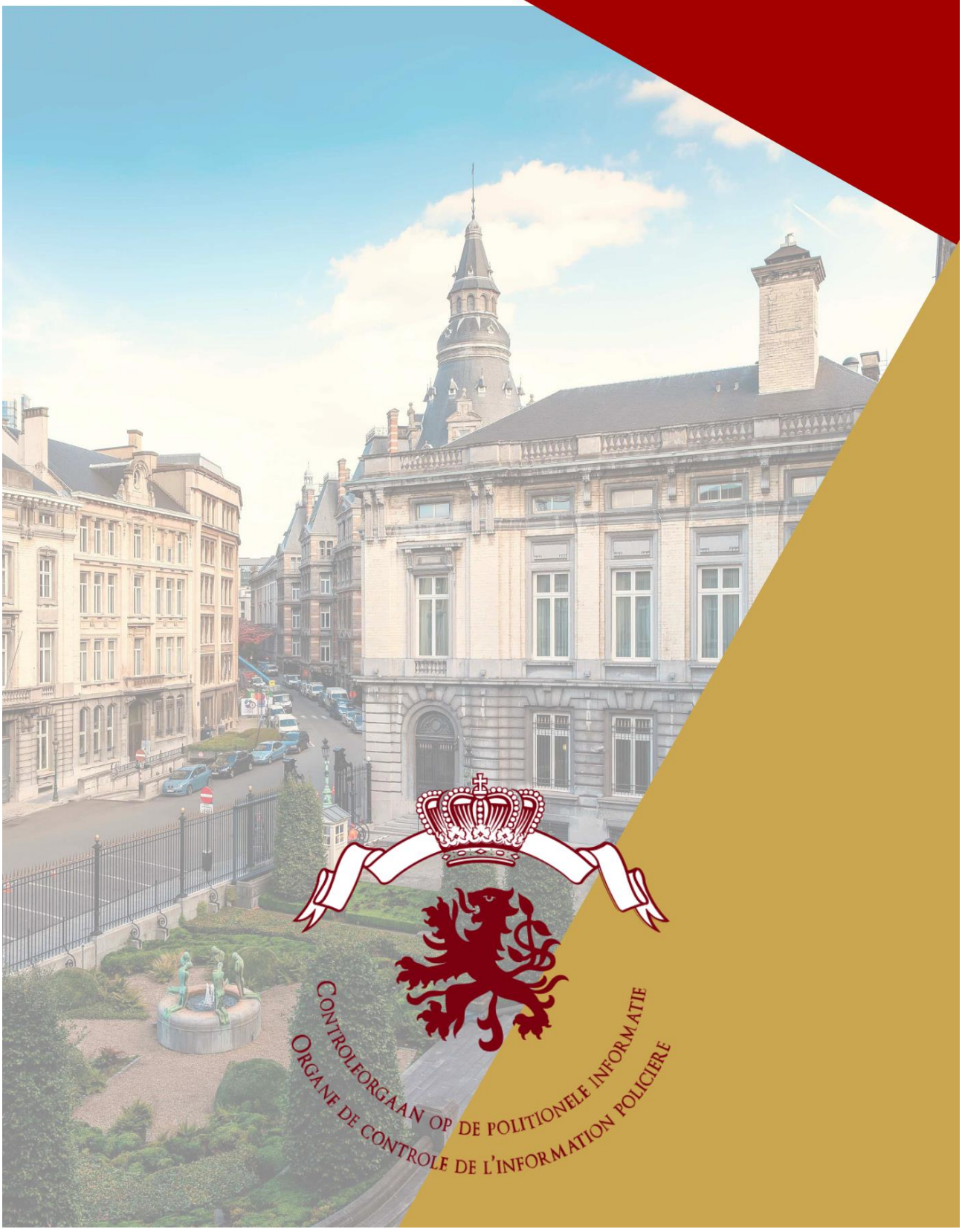
L'Organe de contrôle rappelle la possibilité, pour la Direction, d'introduire un recours auprès de la Cour d'appel du ressort du domicile ou du siège du demandeur dans les 30 jours de la décision de l'Organe de contrôle (article 248 §1er, premier alinéa, et §2 de la LPD).

Les documents eux-mêmes (cf. annexe) peuvent être obtenus à première demande auprès de l'Organe de contrôle (info@controleorgaan.be, en mentionnant la référence du COC : CON22009).

Ainsi décidé par l'Organe de contrôle de l'information policière le 2 avril 2024.

Pour l'Organe de contrôle de l'information policière,

Frank SCHUERMANS
Président *a.i.* (Sé)



Controleorgaan op de politionele informatie

Organe de contrôle de l'information policière