

CONTRÔLE RESTREINT

RAPPORT DE VISITE ET DE SURVEILLANCE AUPRÈS D'UNE ZONE DE POLICE EN FLANDRE ORIENTALE PAR L'ORGANE DE CONTRÔLE DE L'INFORMATION POLICIÈRE DANS LE CADRE DE SA COMPÉTENCE DE SURVEILLANCE ET DE CONTRÔLE

Référence : DIO21001

**ORGANE DE CONTROLE DE
L'INFORMATION POLICIÈRE**



Table des matières

1	INTRODUCTION	3
1.1	Les compétences de l'Organe de contrôle de l'information policière.....	3
2	OBJECTIF DE LA VISITE.....	4
3	CADRE JURIDIQUE	4
3.1	Surveillance par caméras	4
3.1.1	Fondement juridique	4
3.1.2	Responsable du traitement.....	5
3.1.3	Exigences procédurales.....	6
3.1.4	Délai de conservation des images.....	6
3.1.5	Banques de données techniques	6
3.1.6	Accès aux images	7
3.1.7	Utilisation visible et invisible de caméras	8
3.1.8	Analyse d'impact et de risques et évaluation de l'impact sur la protection des données (EIPD ou <i>DPIA</i> , <i>Data Protection Impact Assessment</i>).....	8
3.1.9	Registre	8
3.1.10	Surveillance par caméras des bâtiments, bureaux de police et cellules de police	9
3.2	Enregistrement audiovisuel dans le cadre d'une instruction pénale	9
3.3	Concertation confidentielle avec un avocat	10
4	RESULTATS DU CONTRÔLE.....	10
4.1	Utilisation de caméras par la zone de police en général	10
4.1.1	Utilisation du pictogramme de l'art. 25/2 §2 LFP et de l'A.R. du 22 mai 2019.....	10
4.1.2	Décisions du conseil communal relative à l'utilisation de caméras (autorisation préalable de principe 25/4 LFP) 10	
4.1.3	Analyse d'impact et de risques relative à l'utilisation de caméras (25/4 LFP)	11
4.1.4	Utilisation et respect des principes de proportionnalité et de subsidiarité (art 25/5 LFP)	11
4.1.5	Enregistrement et délai de conservation des images (art 25/6 LFP)	11
4.1.6	Accès, motif de la consultation et fichiers de journalisation (art 25/7 LFP)	12
4.1.7	Registres (art 25/8 LFP).....	12
4.1.8	Droit d'accès aux images (art 42 LPD et art 12 de la loi de 2007 sur les caméras).....	12
4.2	Utilisation de caméras pendant la concertation confidentielle avec un avocat.....	13
5	CONCLUSIONS – REQUÊTES, RECOMMANDATIONS ET MESURES CORRECTRICES	13

1 INTRODUCTION

1. Compte tenu de ses compétences en tant que service de contrôle externe et autorité de contrôle compétente en matière de traitement de données par la police intégrée structurée à deux niveaux (GPI), l'Organe de contrôle de l'information policière (Organe de contrôle ou COC) a décidé d'effectuer une visite dans une zone de police en Flandre orientale dans le cadre d'une « Contrôle restreint¹ », ce à l'occasion d'une plainte (COC référence DKL21002) relative à l'enregistrement des images et du son pendant une concertation confidentielle avec un avocat. Le plaignant affirme qu'après la concertation confidentielle qu'il a eue avec son avocat dans le bâtiment de la police de la zone de police concernée, les fonctionnaires de police concernés étaient apparemment au courant du contenu de cette conversation. Aucune notification préalable n'a été faite de la possibilité d'un enregistrement des images et du son dans le bâtiment de la police ou dans le local où s'est déroulée la concertation confidentielle. L'accès aux images a posteriori n'a pas été autorisé. Le présent rapport présente les conclusions de l'enquête réalisée à l'occasion de la visite.

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

2. Dans le cadre de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel (LPD)², le COC a été réformé et est devenu une autorité de contrôle à part entière, outre ses compétences de contrôle existantes en matière de traitement policier de l'information tel qu'il est prévu dans la loi du 5 août 1992 sur la fonction de police (LFP). L'article 71 §1 et le titre 7 LPD définissent les tâches et compétences du COC. Ils renvoient également aux missions de contrôle spécifiées dans les articles 44/1 à 44/11/14 LFP relatifs au traitement de l'information des services de police. De cette manière, l'organe de contrôle est investi d'une mission de surveillance et de contrôle. Cela signifie qu'au-delà de la protection de la vie privée et des données à caractère personnel, le COC prête également attention à des éléments tels que l'efficacité et l'efficacité du traitement de l'information et de l'intervention policière. En vertu de la réglementation susmentionnée, le COC a par conséquent une compétence générale de surveillance sur tous les traitements de données (à caractère personnel), tant opérationnels que non opérationnels, par la GPI.

Le COC est compétent notamment pour les services de police³, pour l'Inspection générale de la police fédérale et locale (AIG)⁴ et pour l'unité d'Information des Passagers (UIP)⁵. La compétence du COC en ce qui concerne les services de police couvre à la fois les activités de traitement opérationnelles (Titre 2 LPD) et non opérationnelles (RGPD)⁶.

¹ Le COC fait la distinction entre plusieurs formes de contrôle ou de supervision :

- **Contrôle global** : il s'agit d'une enquête de contrôle qui s'accompagne d'une ou plusieurs visite(s) approfondie(s) sur le terrain ou de visites où la portée de la surveillance est très large.

- **Contrôle thématique** : comme son nom l'indique, une enquête est menée sur un thème spécifique, ce qui permet à la fois une recherche documentaire et/ou des visites sur place.

- **Contrôle technique** : ces contrôles se limitent principalement à vérifier la légalité, l'exhaustivité et l'exactitude des saisies et des traitements dans les banques de données policières.

- **Contrôle restreint** : ces contrôles portent sur un ou seulement quelques (sous-)aspect(s) du traitement des données policières opérationnelles ou non-opérationnelles.

- **Contrôle international** : il s'agit des éventuelles enquêtes internationales auxquelles le COC collabore ou qui s'inscrivent dans le cadre de ses obligations internationales.

- **Contrôle particulier** : il s'agit d'enquêtes et de contrôles dans des domaines particuliers, tels que les contrôles annuels des banques de données communes sur le terrorisme et l'extrémisme..

² M.B. 5 septembre 2018. Elle contient également des dispositions d'application du Règlement (UE) n° 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données et abrogeant la directive 95/46/CE (règlement général sur la protection des données), ci-après la LPD, et la Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière, ou aux fins de l'exécution de sanctions pénales, et de libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil.

³ Tel que défini à l'article 2, 2° de la loi du 7 décembre 1998 organisant un service de police intégré structuré à deux niveaux (article 26, 7°, a) LPD).

⁴ Tel que défini à l'article 2 de la loi du 15 mai 2007 relative à l'Inspection générale contenant diverses dispositions concernant le statut juridique de certains membres des forces de police (article 26, 7°, d) LPD).

⁵ Conformément au chapitre 7 de la loi du 25 décembre 2016 sur le traitement des données des passagers (art. 26, 7°, f) LPD).

⁶ Art. 4 § 2, quatrième alinéa, de la loi du 3 décembre 2017 instituant l'Autorité de protection des données.

En ce qui concerne la mission de contrôle, le COC est chargé de contrôler le traitement des informations et des données visées à l'article 44/1 LFP, en ce compris celles introduites dans les banques de données visées à l'article 44/2 de la même loi. Le COC est également chargé de toutes les autres missions qui lui sont confiées par ou en vertu d'autres lois.

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

Le COC est également chargé de vérifier le respect des règles concernant l'accès à la banque de données nationale générale (BNG) et à sa consultation directe, ainsi que le respect de l'obligation, visée à l'article 44/7, paragraphe 3 LFP, pour tous les membres des services de police, d'alimenter cette banque de données.

Le COC vérifie également le bon fonctionnement de la BNG et la procédure de traitement des données et informations qu'elle contient afin de déterminer si celle-ci est conforme aux dispositions des articles 44/1 à 44/11/13 LFP et à leurs mesures d'application.

En ce qui concerne l'utilisation de caméras non visibles, le COC agit comme une sorte de commission « MPA »⁷. Selon l'article 46/6 LFP, toute autorisation et modification de l'utilisation non visible de caméras dans les cas visés à l'article 46/4 doit être notifiée au COC, sauf lorsque l'utilisation de caméras est effectuée sous l'autorité d'un magistrat. Dans ce cadre, le COC examine si les conditions de la décision de mise en œuvre ou de la prolongation de la mesure sont remplies.

En outre, le COC traite les plaintes relatives à l'application de la législation qui concerne le traitement des données personnelles par les services de police⁸. A cette fin, les membres du COC et les membres du service d'enquête (DOSE)⁹ disposent de pouvoirs d'enquête et des mesures correctrices peuvent être prises¹⁰.

Certaines décisions du COC peuvent faire l'objet d'un recours dans un délai de 30 jours devant la Cour d'Appel du lieu de résidence ou du siège social du plaignant, qui traitera l'affaire comme une procédure interlocutoire conformément aux articles 1038, 1040 et 1041 du Code judiciaire¹¹.

2 OBJECTIF DE LA VISITE

3. Le 11 février 2021, l'Organe de Contrôle a effectué de sa propre initiative une visite à l'improviste¹² dans la zone de police concernée en vue du contrôle des traitements à l'aide de caméras dans le bâtiment de la police. La visite était la conséquence de la plainte individuelle susmentionnée à l'occasion d'irrégularités éventuelles lors de l'enregistrement d'images et de sons pendant une concertation confidentielle avec un avocat.

3 CADRE JURIDIQUE

3.1 Surveillance par caméras

3.1.1 Fondement juridique

⁷ Méthodes Particulières en police Administrative.

⁸ Art. 240, 4° et 247 LPD.

⁹ Dienst Onderzoeken / Service d'Enquête.

¹⁰ Art. 244 et 247 LPD.

¹¹ Art. 248 LPD.

¹² Une visite à l'improviste dans le cadre d'un Contrôle restreint est une enquête dirigée sur un thème spécifique et, plus spécifiquement, sur des aspects juridiques spécifiques ou des aspects inhérents à la protection des données ou à la protection de la vie privée. Étant donné la crise du COVID et les mesures de santé correspondantes, la décision a été prise, pour des raisons d'opportunité, d'annoncer la visite au chef de corps la veille, sans toutefois en mentionner le thème spécifique.

4. Depuis la loi d'adaptation de la LFP du 21 mars 2018, la décision de placer des caméras dans les espaces publics ne peut plus être prise que par une autorité publique, comme la commune¹³. Lorsque la police utilise une surveillance par caméras, les dispositions de la LFP sont applicables sauf lorsque l'utilisation de caméras est régie par une autre législation¹⁴.

3.1.2 Responsable du traitement

5. Dans le droit relatif à la protection des données, un rôle important est dévolu au « responsable du traitement ». Il s'agit de « *la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement* »¹⁵. En ce qui concerne les activités de traitement dans le cadre des missions de police administrative et judiciaire, le responsable du traitement est défini dans 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* »¹⁶. Par « *autorité compétente* », il faut entendre « *a) les services de police au sens de l'article 2, 2^o, de la loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux* »¹⁷.

6. Bien que le responsable du traitement dans la LFP se voie attribuer un rôle (spécifique) à certains endroits, ce n'est pas le cas en ce qui concerne l'utilisation de caméras. Comme indiqué précédemment, le responsable du traitement est un acteur essentiel dans le traitement des données à caractère personnel. Il doit en effet démontrer que les données à caractère personnel sont traitées conformément au cadre légal. Lui, son préposé ou mandataire, est aussi la personne à laquelle des mesures correctrices éventuelles peuvent être imposées ou qui peut être poursuivi pénalement¹⁸. Le chef de corps est le responsable du traitement pour l'enregistrement d'images de caméras dans une banque de données technique locale¹⁹.

Le chef de corps est aussi le responsable du traitement pour les banques de données particulières²⁰. Dans les banques de données particulières, sont enregistrées des données qui ne sont pas susceptibles d'être reprises dans la BNG bien qu'elles aient une nécessité opérationnelle. Des exemples d'une banque de données particulière sont (1) l'enregistrement de numéros de téléphone ou de données ANPR qui sont recueillis dans le cadre d'une instruction pénale²¹ et (2) des images de caméra classiques. Il s'agit de données en rapport avec des missions de police administrative et judiciaire mais elles ne doivent pas *ipso facto* être enregistrées/résumées dans la BNG²². En ce qui concerne ces dernières, nous vous renvoyons à l'article 25/6 de la LFP qui stipule seulement que les informations et les données à caractère personnel doivent pouvoir être conservées 12 mois maximum²³. Un responsable du traitement n'est cependant pas désigné pour la conservation des données.

L'Organe de contrôle estime qu'il s'agit (également) d'une banque de données particulière de telle sorte que le chef de corps doit être considéré comme le responsable du traitement. L'article 44/4 § 1er, 3^e alinéa de la LFP stipule en effet que les chefs de corps, le commissaire général, les directeurs généraux ou les directeurs qui ont fixé les objectifs et les moyens relatifs à ces banques de données particulières sont les responsables du traitement pour les banques de

¹³ 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, M.B. 16 avril 2018.

¹⁴ Comme le contrôle de tronçon, 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, 9).

¹⁵ Art. 4. 7) du RGPD.

¹⁶ Art. 26, 8^o de la LPD.

¹⁷ Art. 26, 7^o de la LPD.

¹⁸ Voir les articles 221 et 222 de la LPD. Concrètement, l'Organe de contrôle peut notamment prendre les mesures suivantes (art. 25.2, RGPD) : - donner un avertissement ; - donner une réprimande ; - ordonner de mettre les opérations de traitement en conformité avec le cadre légal dans un délai déterminé ; imposer une limitation temporaire ou définitive, y compris une interdiction, du traitement.

¹⁹ Art. 44/11/3^{sexies} § 1, 2^e alinéa de la LFP.

²⁰ Article 44/4 § 1, troisième alinéa de la LFP.

²¹ MERCURE.

²² Art. 44/11/3 de la LFP.

²³ Remarquons, par souci d'exhaustivité, que la LFP n'impose pas de délai de conservation ferme pour les données qui sont enregistrées dans les banques de données particulières (art. 44/11/3, §4 de la LFP). Étant donné que l'article 25/6 de la LFP impose un maximum de 12 mois, le délai maximum est ainsi déterminé aussi pour cette banque de données particulière.

données particulières qu'ils constituent. La désignation du chef de corps comme responsable du traitement s'inscrit par ailleurs dans l'esprit des dispositions de la LFP relatives à la constitution de banques de données locales. Selon l'article 25/5 de la LFP, l'utilisation de caméras a lieu sur décision et sous la responsabilité du fonctionnaire de police compétent. Si ce n'est pas le chef de corps, le fonctionnaire de police compétent agit sous la responsabilité du chef de corps. En effet, le chef de corps, en vertu de l'article 44 de la loi sur la police intégrée, est responsable de l'exécution de la politique policière locale, et plus particulièrement de l'exécution du plan zonal de sécurité et assure la direction, l'organisation et la répartition des tâches au sein du corps de police locale et l'exécution de la gestion de ce corps²⁴.

Le chef de corps est donc le responsable du traitement en ce qui concerne toutes les formes d'utilisation de caméras dans sa zone de police.

3.1.3 Exigences procédurales

7. Avant qu'un service de police puisse installer des caméras de surveillance sur le territoire d'une commune, il a besoin à cet effet de l'autorisation préalable de principe du conseil communal²⁵. Toutefois, une autorisation n'est pas nécessaire pour l'utilisation de caméras dans des lieux fermés dont la police elle-même est le gestionnaire, comme un commissariat de police²⁶. Il importe de préciser que, lorsque l'autorisation du conseil communal a déjà été obtenue avant la modification de loi du 21 mars 2018 en application de la loi sur les caméras de 2007, il ne faut pas obtenir une nouvelle autorisation du conseil communal²⁷. Cette autorisation initialement obtenue reste donc valable. La même autorisation ne peut toutefois pas être employée pour l'utilisation de nouveaux types de caméras qui ont été introduits par la loi du 21 mars 2018. C'est ainsi que la LFP impose des conditions spécifiques à l'utilisation de caméras fixes temporaires sur lesquelles le conseil communal doit se prononcer²⁸. Dans ce cas, il faut donc obtenir une autorisation nouvelle, ou complémentaire, du conseil communal.

3.1.4 Délai de conservation des images

8. Les images des caméras peuvent être conservées pour une durée n'excédant pas douze mois²⁹. La loi ne fixe pas de délai minimum. En ce qui concerne les images de caméra classiques, la LFP ne spécifie pas sur quel support de données les images doivent être enregistrées. Par conséquent, il est indiqué que le chef de corps indique dans le registre relatif au traitement de données à caractère personnel, tel qu'il est visé dans l'article 55 de la LPD (voir numéro 3.3.8), sur quel support de données les images sont enregistrées. Ce support de données doit être accessible pour l'Organe de contrôle.

3.1.5 Banques de données techniques

9. Bien que l'on sorte du contexte de l'objet de la plainte, il importe de préciser en l'espèce qu'un régime spécifique est d'application 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 »³⁰. Lorsque des caméras de surveillance ANPR sont utilisées, les images doivent être traitées dans une « banque de données technique »³¹, les données à caractère personnel et les informations étant également transmises à la banque de données technique nationale³². Les images peuvent être conservées pour une durée n'excédant pas douze mois sans qu'un délai minimum ne soit spécifié ici non plus³³.

²⁴ Voir aussi et plus en détail, Avis d'initiative du COC DD200026 du 11.02.2021 concernant la question de savoir qui est le responsable du traitement pour les traitements de données par les services de police dans le cadre de l'exécution de missions policières d'une part et pour les traitements de données en vertu du RGPD d'autre part, https://www.organedeconrole.be/files/DD200026_Responsible_de_Traitements_GPI_F.PDF

²⁵ Art. 25/4 § 1, 1^o de la LFP.

²⁶ Exposé des Motifs de cette loi, p. 21 (Doc. parl. *Chambre* 2017-2018, n° 54-2855/001).

²⁷ Art. 88 de la loi du 21 mars 2018 et Exposé des Motifs de cette loi, p. 113-114 (Doc. parl. *Chambre* 2017-2018, n° 54-2855/001).

²⁸ Art. 25/4 § 2, 2^e alinéa de la LFP.

²⁹ Art. 25/6, 44/11/3 *decies* § 2, alinéa premier, et 46/12, alinéa premier de la LFP.

³⁰ Art. 25/2 § 1, 3^o, *juncto* 44/2 § 3, troisième alinéa de la LFP.

³¹ Art. 44/2 § 3, alinéa premier de la LFP.

³² Art. 44/11/3 *sexies* de la LFP.

³³ Art. 44/11/3 *decies* § 2, alinéa premier de la LFP.

La banque de données technique contient les données suivantes, si elles apparaissent sur les images³⁴ :

- 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 échéant³⁵, à l'arrière,
- 4) une photo du véhicule,
- 5) le cas échéant³⁶, une photo du conducteur et des passagers,
- 6) les données de journalisation des traitements.

Ces données doivent donc être traitées dans la banque de données technique pour autant qu'elles apparaissent sur les images *ANPR*.

10. Les principes relatifs à l'interconnexion ou à la corrélation des banques de données techniques avec les banques de données visées à l'article 44/2 §§ 1 et 2 LFP ou avec d'autres banques de données à laquelle ont accès les services de police par ou en vertu de conventions internationales conformément à l'article 44/4 §6 LFP sont régis par la directive interconnexion et corrélation³⁷. Les interconnexions et corrélations servent notamment à tenir compte des facteurs suivants :

- les critères de temps, d'espace et de fréquence des interconnexions et corrélations, tels que prévus à l'article 44/4, § 6 LFP ;
- l'enregistrement dans le registre des traitements REGPOL des autorisations requises ;
- 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 ;
- la nécessité en cas de *hit* (corrélation positive) de suivre la politique d'action nationale et une politique d'intervention ciblée ;
- la nécessité de retourner vers la source authentique en cas d'un *hit* sur une plaque d'immatriculation, détecté à l'aide de liste ou d'extrait injectés dans une banque de données technique locale ou nationale, sauf si la corrélation se fait en temps réel avec la source authentique.

3.1.6 Accès aux images

11. L'accès aux images dépend de la finalité et est réglé de la même manière tant pour la surveillance par caméras ordinaires que pour l'utilisation de caméras *ANPR*. Dans les deux cas, les images peuvent être conservées pendant 12 mois maximum. En ce qui concerne les missions de police administrative, l'accès est limité au premier mois suivant l'enregistrement des images. Pour les missions de police judiciaire, les images sont accessibles pendant toute la durée de leur conservation mais l'intervention du procureur du Roi est nécessaire après le premier mois³⁸. L'accès doit être motivé sur le plan opérationnel et nécessaire pour l'exercice d'une mission précise³⁹. Autrement dit, l'accès aux images est autorisé uniquement aux personnes qui ont besoin de ces données à caractère personnel et informations et lorsqu'un intérêt opérationnel concret est donc présent à cet effet⁴⁰.

12. En ce qui concerne le droit d'accès aux images de toute personne filmée, le droit à un accès indirect tel qu'il est prévu à l'art. 42 LPD est d'application s'il s'agit d'images traitées à des fins opérationnelles. La LFP ne contient toutefois pas de réglementation relative aux droits du fonctionnaire de police ou du citoyen dans le cadre de l'accès aux images dans l'hypothèse où les images et le son ne sont pas utilisés à des fins opérationnelles (donc, par exemple, lorsqu'elles ne servent pas de base à l'établissement d'un procès-verbal). Si les images ne sont pas pertinentes pour les missions de police administrative ou judiciaire et n'ont donc pas d'intérêt opérationnel, la LFP ne s'oppose pas non plus à ce que

³⁴ Art. 44/11/3 *decies* § 1 de la LFP.

³⁵ « Le cas échéant » fait référence aux possibilités techniques de la caméra, présentes ou non.

³⁶ Ibid.

³⁷ 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.

³⁸ Art. 25/7 § 1, 1^{er} et 2^e alinéas et 44/11/3 *decies* § 3, deuxième alinéa de la LFP.

³⁹ Art. 44/11/3 *decies* § 3, 1^{er} alinéa de la LFP.

⁴⁰ Exposé des Motifs de cette loi, p. 29 (Doc. parl. *Chambre* 2017-2018, n° 54-2855/001).

la zone de police responsable organise elle-même un droit d'accès aux images⁴¹. En l'occurrence, le système d'accès, par analogie à la loi sur les caméras du 21 mars 2007, peut servir d'exemple, le fonctionnaire de police mais aussi le citoyen pouvant s'adresser directement au service de police concerné au premier chef.

3.1.7 Utilisation visible et invisible de caméras

13. Les caméras visibles sont les caméras dont l'utilisation est signalée 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 ou portées par des fonctionnaires de police qui sont identifiables comme tels⁴². Dans des situations exceptionnelles, la police peut faire un usage dissimulé de caméras (utilisation non visible). Dans ce cas, la caméra est portée par le fonctionnaire de police ou placée dans un véhicule de police banalisé. Il est question d'un véhicule de police banalisé lorsque le véhicule de police n'est pas reconnaissable en tant que tel. Dans ce cas, il est donc question d'utilisation « *non visible* » de la caméra⁴³. L'application de caméras non visibles est régie strictement et se limite à quatre situations. À savoir :

- 1) en raison de circonstances particulières, notamment en cas d'attroupements, en vue de recueillir des informations de police administrative sur des personnes radicalisées ou *terrorist fighters*, et de véhicules de police banalisés pour la lecture automatique de plaques d'immatriculation, en vue de détecter des véhicules signalés. (art. 46/4 LFP) ;
- 2) pour la préparation d'actions de police judiciaire ou pour le respect de l'ordre public pendant ces actions (articles 46/7 et 46/8 LFP) ;
- 3) dans le cadre de missions spécialisées de protection des personnes (art. 44/9 LFP) et
- 4) pendant le transfert de personnes détenues ou arrêtées (art. 46/11 LFP).

Sauf si l'utilisation non-visible de caméras est effectuée sous l'autorité d'un magistrat, cette forme d'utilisation de caméras doit toutefois être notifiée **préalablement** à l'Organe de contrôle. Cette notification préalable doit permettre à l'Organe de contrôle d'apprécier la légalité de la décision⁴⁴.

3.1.8 Analyse d'impact et de risques et évaluation de l'impact sur la protection des données (EIPD ou *DPIA, Data Protection Impact Assessment*)

14. Depuis la loi du 21 mars 2018, il est obligatoire d'établir une analyse d'impact et de risques préalablement à l'utilisation de caméras de surveillance, la protection de la vie privée étant mise en balance avec le niveau opérationnel de l'utilisation des caméras⁴⁵. Cet exercice doit également être établi avant la constitution d'une banque de données technique (locale)⁴⁶. À cet effet, l'assistance du *DPO* est demandée⁴⁷.

À condition que les conditions de la LPD pour une *DPIA* et les conditions pour une analyse des risques et de l'impact concernant l'utilisation visible des caméras et/ou concernant la constitution des banques de données techniques en vertu de la LFP soient satisfaites, les deux analyses peuvent être réunies en un seul document. Étant donné qu'une *DPIA* en vertu de la LPD nécessite une analyse plus étendue que celle prescrite dans la LFP, il est signalé que, dans le cas où les deux sont traités ensemble, cette analyse doit, conformément à la LPD, couvrir tous les systèmes et procédures pertinents d'activités de traitement. Hormis le respect de la LPD et de la LFP, les mesures de précaution opérationnelles et les mesures de protection (qui sont prises pour limiter les risques pour les données à caractère personnel à protéger) doivent également être décrites.

3.1.9 Registre

⁴¹ Comme spécifié en principe dans l'article 14 (droit de consultation) de la Directive Police-Justice

⁴² Art. 25/2 § 2 de la LFP.

⁴³ Art. 46/4 et suiv. de la LFP.

⁴⁴ Art. 46/6 et 46/10 de la LFP.

⁴⁵ Art. 25/4 § 2 de la LFP.

⁴⁶ Art. 44/11/3 *octies* de la LFP.

⁴⁷ Art. 65, 3° *juncto* 58 de la LPD.

15. Les utilisations de caméras doivent être consignées dans un registre (local)⁴⁸. Le registre indique le type de caméras et leur localisation. Cependant, aucun arrêté royal n'a encore été promulgué pour préciser le contenu de ce registre. Néanmoins, l'Organe de Contrôle estime qu'à la lumière de l'efficacité de ses compétences de contrôle, la police, en l'attente de l'arrêté d'exécution, doit constituer de sa propre initiative un registre qui reprend toutes les utilisations de (types de) caméras, y compris l'utilisation non-visible de caméras. De cette manière, l'Organe de Contrôle (et, du reste, la zone de police elle-même, en premier ressort) se fait une vue d'ensemble et une idée de l'utilisation de caméras de surveillance sur le territoire de la commune qui relève de sa compétence. Dans le même temps, l'utilisation de caméras de surveillance peut être contrôlée en fonction du registre des activités de traitement. Étant donné que des données à caractère personnel sont traitées par la caméra, ce traitement doit également figurer dans le registre des activités de traitement⁴⁹. Les deux registres sont ou doivent être disponibles pour l'Organe de contrôle.

3.1.10 Surveillance par caméras des bâtiments, bureaux de police et cellules de police

16. La surveillance par caméras des bâtiments et bureaux et cellules de police relève de la LFP⁵⁰. C'est également le cas de la surveillance par caméras du hall d'entrée ou de l'accueil du commissariat de police. La vidéosurveillance⁵¹ dans les lieux de détention contribue à la protection et à la garantie du bien-être des personnes qui sont privées de leur liberté et contribue par ailleurs à un meilleur respect des droits de la défense, visés à l'article 6 Conv. eur. D.H.⁵². Toutefois, cette vidéosurveillance est imaginable seulement en tant qu'élément ajouté à une série de mesures comme un contrôle physique régulier des personnes détenues, une politique de prévention des suicides, un système efficace de déclaration pour les victimes d'actes illicites dans les cellules, la séparation, l'isolement, l'application de sanctions disciplinaires ou encore la présence d'un avocat pendant l'audition de la police⁵³. Le bâtiment de la police – ou le poste de police doit être équipé d'une signalisation claire de la vidéosurveillance de telle sorte que la personne détenue dans l'une des cellules en soit expressément informée. Les enregistrements de la détention doivent rester complets (aucun effacement partiel) et être conservés pendant une période raisonnable durant laquelle une plainte peut être déposée.

Étant donné que ces images n'ont pas nécessairement, voire généralement pas d'intérêt opérationnel, la procédure pour l'accès indirect à ces images par l'intermédiaire du COC n'est pas d'application et, conformément à la LPD et au RGPD, l'intéressé peut avoir accès directement aux images enregistrées de sa détention.

Lors du visionnage des images des différentes cellules sur les moniteurs dans le commissariat, la police doit prendre plusieurs mesures strictes de sécurité et d'accès : l'accès doit être limité conformément au principe *need to know*. Un accès général aux images (par exemple : moniteurs dans un local de passage des membres du personnel ou à l'accueil) doit être évité.

3.2 Enregistrement audiovisuel dans le cadre d'une instruction pénale

17. En vertu de l'article 112ter du Code d'Instruction criminelle (C. I. cr.), « *le procureur du Roi ou le juge d'instruction peut ordonner l'enregistrement audiovisuel ou audio d'une audition. La personne à entendre est préalablement mise au courant de cette décision.* » (§ 1). L'enregistrement audiovisuel ou audio de l'audition peut être effectué par un fonctionnaire de police (§ 2) qui doit dans ce cas reprendre ce mode d'audition dans le procès-verbal (§ 3). Il ne s'agit donc pas d'une forme de surveillance par caméra (avec audio), telle que visée et régie dans la LFP. Par ailleurs, la décision de procéder à un enregistrement audiovisuel ou audio n'est pas prise par le chef de corps à son initiative. La personne à entendre (et l'avocat) ne peut pas davantage ignorer l'enregistrement audiovisuel ou audio. Un

⁴⁸ Art. 25/8 de la LFP.

⁴⁹ Art. 55 de la LPD.

⁵⁰ Voir aussi l'A.R. 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, en particulier l'art. 10.

⁵¹ Recommandation 06/11 émanant de l'ancienne Commission de la Protection de la Vie privée ou CPVP – aujourd'hui appelée l'Autorité de Protection des Données ou APD - sur l'installation et l'utilisation de caméras de surveillance dans les lieux de détention (cellules et locaux d'audition) et dans d'autres lieux du commissariat

⁵² Convention européenne des Droits de l'Homme

⁵³ Voir à ce propos : « Les normes du CPT – Chapitres des rapports généraux du CPT consacrés à des questions de fond » (document CPT/Inf/E (2002) 1 – Rev. 2009), disponible sur www.cpt.coe.int/en/docsstandards.htm

enregistrement audiovisuel dissimulé ou l'utilisation dissimulée de l'enregistrement audiovisuel tel que visé à l'article 112ter C. I. Cr. sont donc illégaux.

3.3 Concertation confidentielle avec un avocat

18. Tout cela ressort de la jurisprudence de la Cour européenne des Droits de l'Homme (CEDH)⁵⁴ relative à la confidentialité de la relation entre le client et l'avocat. La confidentialité de cette relation⁵⁵ est fondamentale et est protégée par les articles 6 et 8 de la Convention européenne des Droits de l'Homme (Conv. Eur. D.H.)⁵⁶. Cette relation touche donc à la fois au droit à la vie privée, au sens large, de l'intéressé (article 8) et à son droit à un procès équitable (article 6).

Nous retrouvons un exemple éloquent d'une affaire dans un commissariat de police dans le cas suivant R.E. c/ Royaume-Uni⁵⁷ qui renvoie également à la jurisprudence antérieure : « 131. *The present case concerns the surveillance of legal consultations taking place in a police station, which the Court considers to be analogous to the interception of a telephone call between a lawyer and client. The Court has recognised that, while Article 8 protects the confidentiality of all correspondence between individuals, it will afford "strengthened protection" to exchanges between lawyers and their clients, as lawyers would be unable to defend their clients if they were unable to guarantee that their exchanges would remain confidential (Michaud v. France, no. 12323/11, § 118, ECHR 2012).* »

Même la simple présence d'une caméra dans un local destiné à des entretiens confidentiels entre l'avocat et son client peut être contraire aux articles 6 et 8 de la Conv. eur. D.H., indépendamment du fait que celle-ci filme/enregistre effectivement ou non, plus spécifiquement parce que la confidentialité qui devrait pouvoir s'établir pendant un tel entretien n'est pas garantie. *A fortiori* si les images et le son sont effectivement enregistrés ou si l'audio peut être entendu. C'est seulement si l'avocat le demande, dans le cadre de sa sécurité, que l'utilisation de la vidéo et donc **pas** de l'audio peut être justifiée.

4 RESULTATS DU CONTRÔLE

4.1 Utilisation de caméras par la zone de police en général

4.1.1 Utilisation du pictogramme de l'art. 25/2 §2 LFP et de l'A.R. du 22 mai 2019

19. L'utilisation de caméras fixes dans la zone de police est présente à différents endroits du territoire.

Au sein du bâtiment de la zone de police, nous constatons que le pictogramme est clairement visible à l'entrée du complexe de cellules. À l'entrée des visiteurs, aucun pictogramme clairement visible n'est présent. La zone de police fait cependant savoir que les pictogrammes ont été commandés et que leur affichage n'est qu'une question de temps.

4.1.2 Décisions du conseil communal relative à l'utilisation de caméras (autorisation préalable de principe 25/4 LFP)

20. La zone de police indique que l'autorisation pour l'installation de caméras de surveillance pour le territoire de la zone est déjà antérieure au 21 mars 2018 et, le cas échéant, tient à disposition les décisions pour consultation par le COC. Comme déjà indiqué précédemment pour l'utilisation de caméras au sein du bâtiment de la zone de police, aucune autorisation préalable du conseil communal n'est requise.

⁵⁴ Cour européenne des Droits de l'Homme

⁵⁵ Nous renvoyons notamment à CEDH 10 septembre 2013, Helander c/ Finlande, n° 10410/10, et à CEDH 21 février 1975, Golder c/ Royaume-Uni, n° 4451/70.

⁵⁶ Convention européenne des Droits de l'Homme

⁵⁷ CEDH R.E. c/ Royaume-Uni du 27 octobre 2015, n° 62498/11.

4.1.3 Analyse d'impact et de risques relative à l'utilisation de caméras (25/4 LFP)

21. La zone de police indique que l'autorisation de l'installation de caméras de surveillance est antérieure au 21 mars 2018. Aucune analyse d'impact et de risques n'est donc présente pour leur utilisation. En ce qui concerne l'utilisation de caméras à l'intérieur du bâtiment de la police, reste toutefois à s'interroger sur la question de l'application des articles 55 à 62 LPD inclus, en particulier l'article 58, concernant l'établissement d'une évaluation des activités de traitement visées sur la protection des données à caractère personnel.

Pour anticiper les conclusions de ce rapport, il manque manifestement à la zone de police une description générale des utilisations visées de la caméra, une évaluation des risques pour les droits et libertés des intéressés, 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 respect des droits et intérêts légitimes des personnes concernées et des autres intéressés.

4.1.4 Utilisation et respect des principes de proportionnalité et de subsidiarité (art 25/5 LFP)

22. Il n'existe pas de réglementation interne claire relative à l'utilisation des caméras dans le bâtiment de la police. Leur utilisation prête aussi à confusion dans la zone de police. Le corps dispose toutefois d'une sorte de règlement du corps dans lequel peuvent être reprises de telles directives. Selon le corps, l'élaboration d'une politique interne à ce sujet fait partie de ses intentions.

Par souci de clarté et d'exhaustivité, le COC entend toutefois faire remarquer que les caméras ont été installées dans les cellules d'une manière qui respecte la vie privée au sens de l'article de l'A.R. du 14 septembre 2007.

4.1.5 Enregistrement et délai de conservation des images (art 25/6 LFP)

23. Les caméras présentes dans le bâtiment filment en permanence. L'enregistrement des images est effectué automatiquement, à l'exception des images des locaux d'audition. **Dans les locaux d'audition, l'enregistrement se fait au moyen d'un bouton mais les images sont filmées de toute façon. L'activation du bouton d'enregistrement active toutefois l'enregistrement de la vidéo et celui de l'audio. Cette pratique et ce traitement (dans les locaux d'audition) sont illégaux.**

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 juridique⁵⁸. Comme indiqué précédemment, l'audition audiovisuelle est régie strictement dans le chapitre VII^{quater} (en particulier, l'art. 112^{ter} C. I .cr.), en plus des dispositions relatives à l'audition audiovisuelle pour les mineurs, qui est régie dans les articles 92 à 103 C. I. Cr. Une audition audiovisuelle ne peut se faire que si elle est ordonnée par le procureur du Roi ou le juge d'instruction, suivie par 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.**

Il existe une infrastructure séparée qui permet l'enregistrement d'une audition audiovisuelle conformément aux dispositions susmentionnées. Même la seule présence de la possibilité d'un enregistrement audio des auditions dans les locaux d'audition semble du reste un peu excessive dans les faits. Le COC peut difficilement se figurer que tous les locaux d'audition sont utilisés en même temps (ou l'aient été dans le passé) pour effectuer une audition audiovisuelle au sens du C.I. cr. Mais bon, la possibilité existe en théorie.

Pendant la visite, le COC constate par ailleurs que la configuration du module audio dans un local d'audition donné n'est pas correcte étant donné que l'officier de police judiciaire (OPJ) présent peut entendre en permanence ce qui se dit

⁵⁸ 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 (cf. art. 33 §1, 1° et 2° LPD).

dans le local, donc même sans l'activation du bouton d'enregistrement. Le local d'audition en question s'avère encore être celui dans lequel une concertation confidentielle entre l'avocat et le client peut se dérouler et se déroule d'ailleurs en général. Bien que l'infrastructure ne soit pas illégale en soi, celle-ci n'est en tout cas pas utilisée correctement et les connaissances techniques pour configurer correctement cette utilisation ne semblent pas suffisamment présentes. **Quoi qu'il en soit, (pouvoir) procéder à une écoute audio d'une concertation confidentielle entre l'avocat et le client, voire l'enregistrement (et la conservation) de celle-ci sont totalement inadmissibles. Pire encore, l'écoute, en soi, est une infraction pénale aux articles 151 et 259 bis C. pén. et à l'article 222, 1°, 2° LPD.**

Le choix de ce local d'audition comme espace pour la concertation confidentielle semble dicté par l'emplacement spécifique dans le bâtiment. C'est le seul local d'audition qui permet, grâce à une paroi vitrée laissant passer le son, de parler à une personne se trouvant de l'autre côté. Cet autre côté comprend un local accessible uniquement via le complexe de cellules.

En ce qui concerne le délai de conservation des images, la zone de police ne peut donner de réponse concluante.

4.1.6 Accès, motif de la consultation et fichiers de journalisation (art 25/7 LFP)

24. La zone de police travaille pour le moment à un accès générique aux images du bâtiment de la police. La nécessité de motiver ou non cet accès n'est pas encore établie clairement. Avec l'identifiant générique, l'utilisateur générique peut procéder à des rétro-interrogatoires. Il n'est pas établi clairement si une distinction doit être opérée en l'occurrence entre la première période d'enregistrement d'un mois et l'interrogatoire après le premier mois, y compris la décision écrite et motivée du procureur du Roi.

À deux endroits au moins, un accès en temps réel aux images de caméra est possible par un écran de visualisation, à savoir dans le local de l'OPJ de garde ainsi que dans le local de l'accueil. Il s'agit effectivement, en l'occurrence, d'un accès à toutes les caméras présentes dans le bâtiment. Aucune distinction n'est opérée entre les images. Dès lors, il est possible de voir ce qui se passe dans **les cellules et les locaux d'audition** même à partir du local de l'accueil. L'écran de visualisation dans le local de l'accueil est installé d'une manière qui permet de voir l'écran par la fenêtre à partir du parking réservé au public. **C'est aussi une pratique inadmissible, manifestement illégale.**

La zone de police n'a pas pu répondre à la question de l'existence d'une vue sur la présence de fichiers de journalisation des accès aux images des caméras. Quoi qu'il en soit, l'identifiant générique ne permet pas d'établir une corrélation avec un utilisateur spécifique de telle sorte que les fichiers de journalisation éventuels ne peuvent réellement servir à la fin à laquelle ils sont destinés, à savoir un contrôle éventuel des accès aux images.

4.1.7 Registres (art 25/8 LFP)

25. L'utilisation de caméras n'est pas indiquée dans le registre des catégories des activités de traitement REGPOL⁵⁹. Le COC constate toutefois à la vérification de ce registre que la zone de police dispose d'une Banque de données technique locale (BDTL) mais sans analyse d'impact et de risques correspondante.

La zone de police ne dispose pas d'un registre relatif à l'utilisation de caméras à l'intérieur de la zone comme imposé par l'art. 25/8 LFP.

Le COC constate que des synthèses ont été reprises dans le registre national pour la Géolocalisation « *Camelia* », mais constate également que l'utilisation de caméras dans le bâtiment de la police n'a pas été indiquée dans le registre.

4.1.8 Droit d'accès aux images (art 42 LPD et art 12 de la loi de 2007 sur les caméras)

26. La zone de police n'est pas au courant du point de vue du COC à propos du droit d'accès aux images de la personne filmée s'il ne s'agit pas d'images qui n'ont pas de nécessité opérationnelle, la zone de police pouvant organiser elle-même ce droit d'accès dans pareil cas.

⁵⁹ REGPOL est le registre unique des traitements des données à caractère personnel institué au niveau de la police intégrée, telle que visé à l'article 145 de la loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux.

4.2 Utilisation de caméras pendant la concertation confidentielle avec un avocat

27. Pendant la visite, le COC a pu constater clairement que la zone de police disposait de la possibilité de procéder à des enregistrements vidéo mais aussi audio dans les locaux d'audition en appuyant sur un bouton d'enregistrement. En l'occurrence, il a pu constater également qu'à la suite d'un problème de configuration dans un local d'audition déterminé, à savoir le local où se déroule en général (mais pas exclusivement) la concertation confidentielle entre l'avocat et son client, la diffusion de cette piste audio dans le local de l'OPJ était permanente et les conversations étaient donc **toujours** audibles (sur écoute). Comme indiqué précédemment, cette pratique constitue une infraction aux articles 151 et 259bis C. pén., à savoir intercepter, prendre connaissance et enregistrer le contenu de communications non accessibles au public ou de données d'un système informatique ou en matière de secret de communications non accessibles au public ou de données d'un système informatique et constitue également un traitement de données irrégulier, qui fait aussi l'objet de sanctions correctionnelles (art. 222, 1^o et 2^o LPD).

Le COC part du principe que la pratique illégale susmentionnée n'a pas été exercée « sciemment ». Cela n'empêche pas que des faits répréhensibles soient commis en continu et qu'il faille y mettre fin immédiatement. Il est en tout cas question de négligence grave.

Quoi qu'il en soit, tout cela est subordonné à la propre responsabilité du chef de corps en tant que responsable du traitement dans le cadre de toute l'utilisation de caméras au sein de la zone de police.

5 CONCLUSIONS – REQUÊTES, RECOMMANDATIONS ET MESURES CORRECTRICES

28. La plainte a révélé que le plaignant et l'avocat avaient clairement remarqué, compte tenu des remarques/réactions des fonctionnaires de police présents, que ceux-ci avaient entendu l'entretien confidentiel entre le plaignant et son avocat.

29. Il ressort des constatations du COC pendant la visite du 11 février 2021 que la plainte était fondée.

Plusieurs non-conformités sur le plan de la réglementation en vigueur apparaissent également. Ces non-conformités semblent, avec beaucoup de bonne volonté dans le chef du COC, découler plutôt de l'ignorance que de relever d'une politique délibérée. Mais cette ignorance supposée n'est pas admissible dans le chef d'un service de police. En tout cas, on ne peut que constater une négligence grave et profonde. Une organisation professionnelle et ses dirigeants peuvent et doivent être supposés savoir que l'audition audio (voire l'enregistrement) d'un entretien confidentiel entre un avocat et son client n'est pas autorisée.

Les connaissances en matière d'utilisation de ces systèmes sont globalement médiocres dans la zone de police et en tout cas insuffisantes et disséminées, ce qui engendre un risque sérieux pour la responsabilité, la sécurité et la vie privée de toutes les personnes concernées.

PAR CES MOTIFS,

L'Organe de Contrôle ;

demande la zone de police,

1. Demande

d'utiliser pour la concertation confidentielle entre un avocat et son client un local qui garantit la confidentialité de cette concertation, mais peut assurer la sécurité de l'avocat si ce dernier le demande ou du moins ne s'y oppose pas. Cela signifie concrètement que **seul** un visuel (avec ou sans caméra) sur cette concertation confidentielle est admissible après autorisation de l'avocat ou à sa demande ;

2. Demande

de procéder à une évaluation relative à l'utilisation de caméras dans le bâtiment de police sur le plan des traitements visés, des risques pour les droits et libertés des personnes concernées, les mesures visées en vue de la limitation des risques, les mesures de précaution, les mesures de protection et les mécanismes qui ont été instaurés pour protéger les données à caractère personnel, moyennant respect des droits et intérêts légitimes des personnes concernées et des autres intéressés et ce dans les six mois suivant la réception du présent rapport ;

3. Demande

d'adopter des directives claires en matière d'utilisation de caméras dans la zone de police en général et dans le bâtiment de police en particulier. Ces directives doivent au moins tenir compte des profils, compléter le motif de la consultation, les délais d'enregistrement et les fichiers de journalisation et ce dans les six mois à compter de la réception de ce rapport ;

4. Demande

d'établir et compléter clairement les registres prévus en matière de traitements, d'utilisation de caméras et de géolocalisation et ce dans les trois mois qui suivent la réception de ce rapport ;

5. Demande

d'aménager un droit d'accès pour la personne filmée s'il s'agit d'images qui ne répondent pas à un besoin opérationnel.

* * * * *

Vu les articles 221 § 1 et 247, 4°, 5° et 6° LPD,

Ordonne les mesures correctrices suivantes à la zone de police,

a. Mesure correctrice

À effet immédiat mettre fin à la prise et l'enregistrement audio dans les locaux d'audition en dehors des circonstances prévues dans le Code d'Instruction criminelle et en donner confirmation à l'Organe de contrôle ; dit pour droit qu'il faut entendre par « *effet immédiat* » la date de la transmission du présent rapport (par e-mail) par l'Organe de contrôle majorée de deux jours ouvrables (samedi et dimanche non inclus) ;

b. Mesure correctrice

prendre les mesures techniques et organisationnelles nécessaires pour régir l'accès aux images dans le local de l'accueil conformément à la réglementation en vigueur (cf. numéro 24), et ce dans les trois mois qui suivent la réception de ce rapport ;

c. Mesure correctrice

en vertu des articles 44/11/3^{octies} de la LFP et de l'art 59 de la LPD, la zone de police doit établir un projet de constitution d'une banque de données technique locale avec mention des objectifs et des modalités de traitement, y compris une analyse d'impact et de risques sur le plan de la protection de la vie privée et au niveau opérationnel, notamment en ce qui concerne les catégories de données à caractère personnel traitées, les objectifs opérationnels à atteindre et le délai de conservation des données nécessaires pour atteindre cet objectif.

Étant donné la charge de travail que représente un tel effort, un premier point de la situation est attendu dans un délai de six mois à compter de la réception de ce rapport ;

d. Mesure correctrice

apposer les pictogrammes nécessaires à l'entrée principale du commissariat et ce dans le mois qui suit la réception du présent rapport.

* * * * *

Dit pour droit que la date d'entrée en vigueur, pour la détermination des délais tels que visés dans les demandes 1 à 5 susvisées et les mesures correctrices b, c et d doit être comprise comme étant la date de la transmission du présent rapport (par courrier électronique) de l'Organe de contrôle augmentée de deux jours ouvrables (samedi et dimanche non inclus).

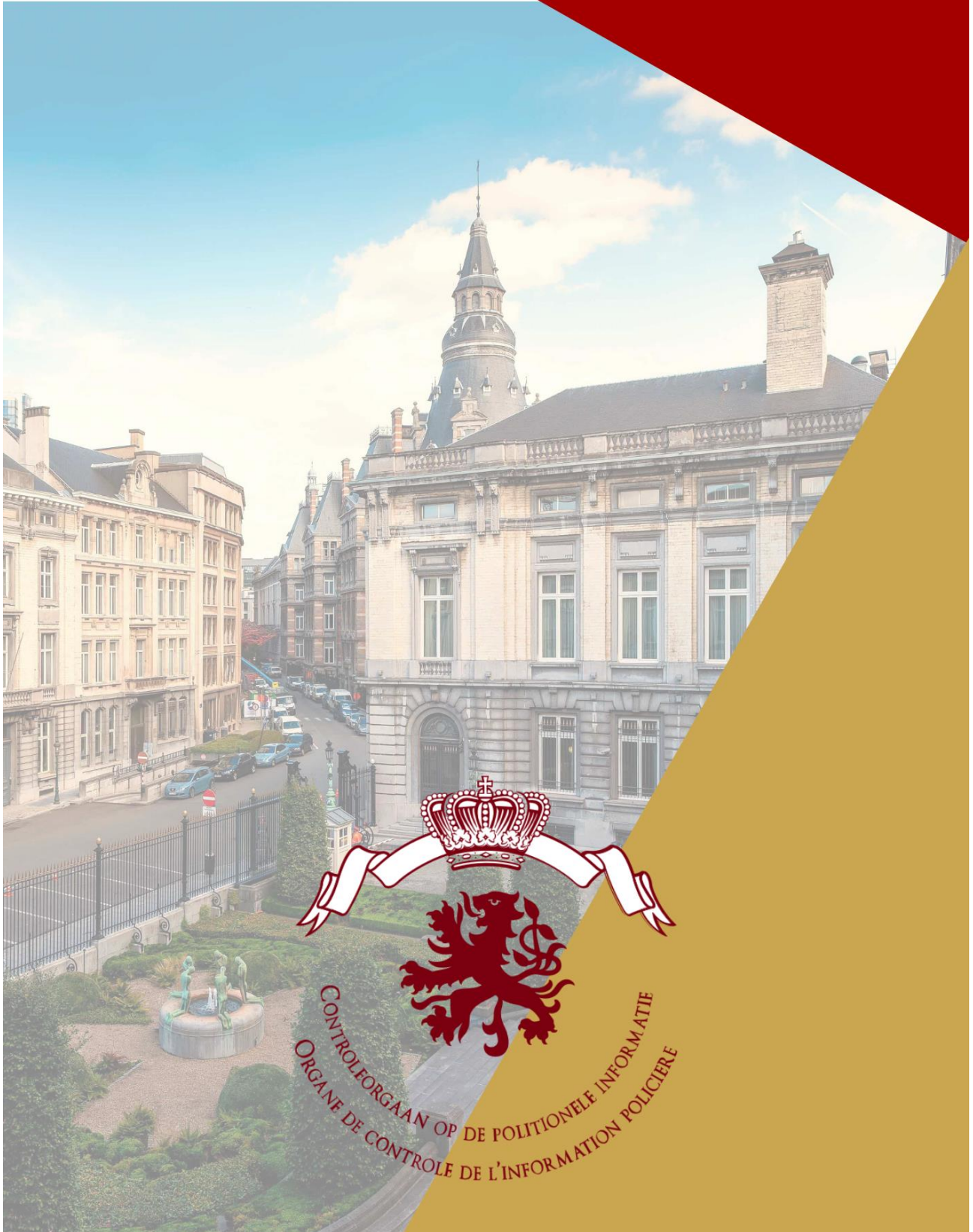
Ainsi décidé par l'Organe de contrôle de l'information policière le 26 mars 2021.

Pour l'Organe de contrôle,

Philippe Arnould (SIGNÉ)
Président

Copie :

- Le président du collège de police
- Le procureur du Roi de Flandre orientale



CONTROLEORGaan OP DE POLITIONELE INFORMATIE
ORGANE DE CONTROLE DE L'INFORMATION POLICIERE

