Rapport d'activités

2016 - 2019

ORGANE DE CONTROLE DE L'INFORMATION POLICIERE

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

Editeur responsable:

Philippe Arnould – Président de l'Organe de contrôle de l'information policière

Adresse : ***Rue de Louvain 48 - 1000 Bruxelles***

E-mail: ***info@organedecontrole.be***

Images:

(1) Photos du Parlement fédéral et alentours – Kurt Van Den Bossche – Droits réservés à la Chambre des Représentants

(2) Photos du corps policier – Droits réservés à la police

(3) Illustrations/tableaux/graphiques – Droits réservés à l'Organe de contrôle

TABLE DES MATIERES

LEXIQUE

AIG : Inspection générale de la police fédérale et de la police locale

AIPD : Analyse d'impact relative à la protection des données

ANPR : *Automatic Number Plate Recognition*

APD : Autorité de Protection des Données

API *: Advanced Passenger Information*

BDC : Banques de Données Communes

BELPIU : L'Unité belge d'Information des Passagers

BNG : Banque Nationale Générale

CALOG : Cadre Administratif et Logistique

CG/ISPO : Commissariat-général/*Information Security & Privacy Office*

COC : Organe de contrôle de l'information policière

CPVP : La Commission de la protection de la vie privée

DIRCOM : Comité de Direction du COC

DPA : *Data Protection Authority*

DPIA : *Data Protection Impact Assesment*

DOSE : *Dienst Onderzoeken* – Service d'Enquête

DPO : *Data Protection Officer*

DRI : Direction de l'information policière et des moyens ICT

ETP : Équivalents Temps Plein.

GPI : *Geïntegreerde Politie* – Police Intégrée

HRM : *Human Ressources Management*

ICT : *Information and Communication Technology*

LCA : Loi du 3 décembre 2017 portant Création de l'Autorité de protection des données

LED : *Law Enforcement Directive*

LFP : Loi du 5 août 1992 sur la Fonction de Police

LPD : Loi du 30 juillet 2018 relative à la Protection des personnes physiques à l'égard des traitements de Données à caractère personnel

OCAM : Organe de Coordination pour l'Analyse de la Menace

ONG : Organisation Non Gouvernementale

PIU : *Passenger Information Unit* (zie ook PIE)

PLIF : Personnel-Logistique-Informatique-Finances

PNR : *Passenger Name Record*

RGPD : Règlement Général sur la Protection des Données

SCHEVAL : *Schengen Evaluation*

SICAD : Service d'Information et de Communication de l'Arrondissement

UIP : L'Unité d'Information des Passagers

ZP : Zone de Police

A. Préambule du Président et des membres du comité de direction

1. Le présent rapport annuel – ou plutôt : rapport d'activité – 2019 a principalement trait à l'année de fonctionnement 2019. Il prête cependant aussi attention dans une certaine mesure aux années 2016, 2017 et surtout 2018, des années pour lesquelles l'Organe de contrôle de l'information policière (en abrégé 'Organe de contrôle' ou 'COC'[1]) n'a, pour des raisons diverses, pas établi de rapport d'activité distinct. Le COC a en effet connu quelques années institutionnelles mouvementées durant lesquelles, en particulier pour les années charnières 2017 et 2018, les membres (de l'époque) n'étaient absolument pas certains que le COC subsisterait, ni, dans l'affirmative, sous quelle forme. Cette incertitude, combinée à un déficit substantiel en termes de moyens et de personnel, a fait que le COC de l'époque a établi un rapport d'activité succinct en 2015 uniquement, mais plus les années suivantes. Ce n'est en effet qu'avec le nouveau cadre européen et national de protection de la vie privée et des données,[2] qui a été finalisé en septembre 2018, que la clarté a enfin été faite sur la subsistance du COC, sa (nouvelle) structure, ses moyens, ses tâches et ses compétences. Cette certitude a d'emblée marqué dès le 5 septembre 2018 une relance – ou plutôt un nouveau départ – pour l'Organe de contrôle de l'information policière, qui existe déjà depuis la réforme de la police de 1998. Sur cette courte période, le COC a subi de nombreuses réformes, peut-être trop, mais il nous semble aujourd'hui avoir définitivement conquis sa place dans le 'paysage belge du contrôle policier' et surtout – mais pas uniquement – en tant qu'autorité de protection des données policières. Le présent rapport se penche plus en détail sur ces aspects.

---

[1] Acronyme pour '***C****ontroleorgaan* - **O**rgane de **C**ontrôle'.

[2] *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 (RGPD) ou *GDPR* en anglais, signifiant *General Data Protection Regulation* - et *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* - également désignée dans le présent rapport sous l'appellation 'directive police/justice' ou en anglais *LED* signifiant *Law Enforcement Directive.*

2. Le présent rapport d'activité n'est pas le canal approprié pour retracer toute l'histoire du COC, mais un aperçu historique succinct semble néanmoins s'imposer.

3. Créé dans le sillage de 'l'affaire Dutroux' en tant qu'organe spécifique chargé de contrôler la légalité, l'efficacité et l'effectivité de la gestion de l'information policière dans son ensemble – avec comme priorité l'efficacité - vu les manquements constatés dans le cadre de l'échange d'informations entre les services, le COC se trouvait à l'époque sous l'autorité conjointe des Ministres de l'Intérieur et de la Justice. Jusqu'en 2014, le COC de l'époque a connu une existence plutôt latente. C'est sous le gouvernement Di Rupo que le COC s'est vu imprimer un nouvel élan, principalement sous l'effet de son transfert au pouvoir législatif initié par la loi de 2014 relative à la gestion de l'information policière.[3] L'intention poursuivie par la loi à travers ce transfert a été formulée en ces termes dans les documents parlementaires : *« Dans la foulée de la refonte des articles 44/1 et suivants de la loi sur la fonction de police, il est apparu nécessaire que le contrôle de la gestion de l'information policière opérationnelle soit réalisé par un organe indépendant et externe aux services de police. Cette indépendance se marque tout d'abord par rapport aux deux responsables du traitement des données et informations de police administrative et de police judiciaire, c'est-à-dire, respectivement les ministres de l'Intérieur et de la Justice. Initialement, l'organe de contrôle était placé sous l'autorité de ces deux ministres. Avec les modifications proposées, l'organe de contrôle de la gestion de l'information policière opérationnelle ressortira directement du Parlement. »*[4] En ce qui concerne le COC, l'intention du législateur de 1998 – à savoir le fait qu'il se consacrerait au fonctionnement de l'organisation policière dans le domaine de la gestion de l'information – est restée inchangée aux yeux du législateur de 2014.

[3] Loi du 18 mars 2014 relative à la gestion de l'information policière et modifiant la loi du 5 août 1992 sur la fonction de police, la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel et le Code d'instruction criminelle, *M.B.* 28 mars 2014, 27465.
[4] *Doc. Parl.* Chambre 2013-2014, n° 3105/001, 63.

4. Fin 2015, le nouveau COC a pris son envol en tant qu'institution ayant droit à une dotation du parlement fédéral. Il se composait de 8 membres équivalents : 1 président qui devait faire partie de la magistrature assise, 1 membre de la CPVP[5] (exerçant sa fonction seulement à temps partiel), 2 membres de la police locale, 2 membres de la police fédérale, et 2 experts. Tous les membres étaient nommés par le Parlement sans être unis entre eux par des liens hiérarchiques et formaient un collège.

Jusqu'à sa refonte en 2018, le COC n'a cependant jamais disposé d'un cadre complet, et ce pour diverses raisons. Il a longtemps fonctionné avec 5 membres (dont le membre de la CPVP exerçait seulement sa fonction à raison de 20 à 25 % d'un horaire à temps plein). Pour ces 5 membres, ce fonctionnement incluait non seulement les aspects opérationnels, mais aussi et surtout les aspects non-opérationnels de leur propre organisation, comme le budget, la comptabilité, l'économat, la gestion du personnel, etc. Il tombe dès lors sous le sens que le travail de contenu portant sur les aspects opérationnels proprement dits incombait dans la pratique à tout au plus 3 ETP.[6]

Entre la fin 2015 et septembre 2018, le COC s'est donc équipé des moyens disponibles afin de réaliser ses missions décrites dans l'article 44/6 de la LFP et le chapitre VII ter de la loi du 8 décembre 1992 relative à la vie privée.[7]

[5] Commission pour la protection de la vie privée (Commission Vie privée).
[6] Équivalents temps plein.
[7] Ce chapitre prévoyait la nouvelle base juridique du COC, qui était intégré à la CPVP de l'époque mais qui n'en était pas moins autonome, et incluait les articles 36ter à 36ter/14 inclus de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel (en abrégé 'LVP').

Il a mené un certain nombre d'enquêtes de contrôle générales - comme celle portant sur la banque de données essentielle 'Infothèque'[8] qui est actuellement toujours utilisée dans nombre de zones de police de Flandre - et rendu des avis prescrits par la loi sur les banques de données particulières que les services de police devaient à l'époque encore déclarer au COC (voir l'article 44/11/3 de la LFP de l'époque[9]).

En l'espace de 2 ans, des avis ont été rendus au sujet de pas moins de 800 banques de données particulières. Ces avis étaient tantôt favorables ou défavorables, tantôt favorables sous conditions. Comme leur nom l'indique, ils demeuraient cependant des 'avis', qui étaient/sont alors suivis ou non par la police intégrée (GPI). La déclaration permettait quoi qu'il en soit au COC de disposer d'un aperçu très fiable du paysage policier des banques de données particulières, ce qui est malheureusement nettement moins évident aujourd'hui.

5. La loi du 3 décembre 2017 portant création de l'Autorité de protection des données (en abrégé 'LCA') et la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel (en abrégé 'LPD' ou 'loi relative à la protection des données') ont à partir du 5 septembre 2018, soumis le COC à sa 3e transformation, qui est aussi la plus profonde. Il s'est en effet vu doté d'un nouveau cadre juridique et organisationnel très détaillé et très complet que nous retrouvons à l'article 4, §2, 4e alinéa de la LCA, à l'article 71 et au titre VII de la LPD et dans la LFP (principalement aux articles 25/1 à 25/8 inclus, 44/1 à 44/11/13 inclus et 46/1 à 46/14 inclus).

[8] Cette application, qui est toujours opérationnelle et cruciale, se définit au mieux comme une interconnexion entre l'*ISLP* (*Integrated System for the Local Police*, la banque de données essentielle de la police locale) et les banques de données des zones de police participantes. Elle permet d'être très rapidement au courant de tous les faits et événements policiers opérationnels pertinents des autres zones de police participantes.

[9] Cet article a en effet été modifié dans l'intervalle par la loi du 22 mai 2019 modifiant diverses dispositions en ce qui concerne la gestion de l'information policière, *M.B.* 19 juin 2019, 61992 (loi de 2019 sur la gestion de l'information policière).

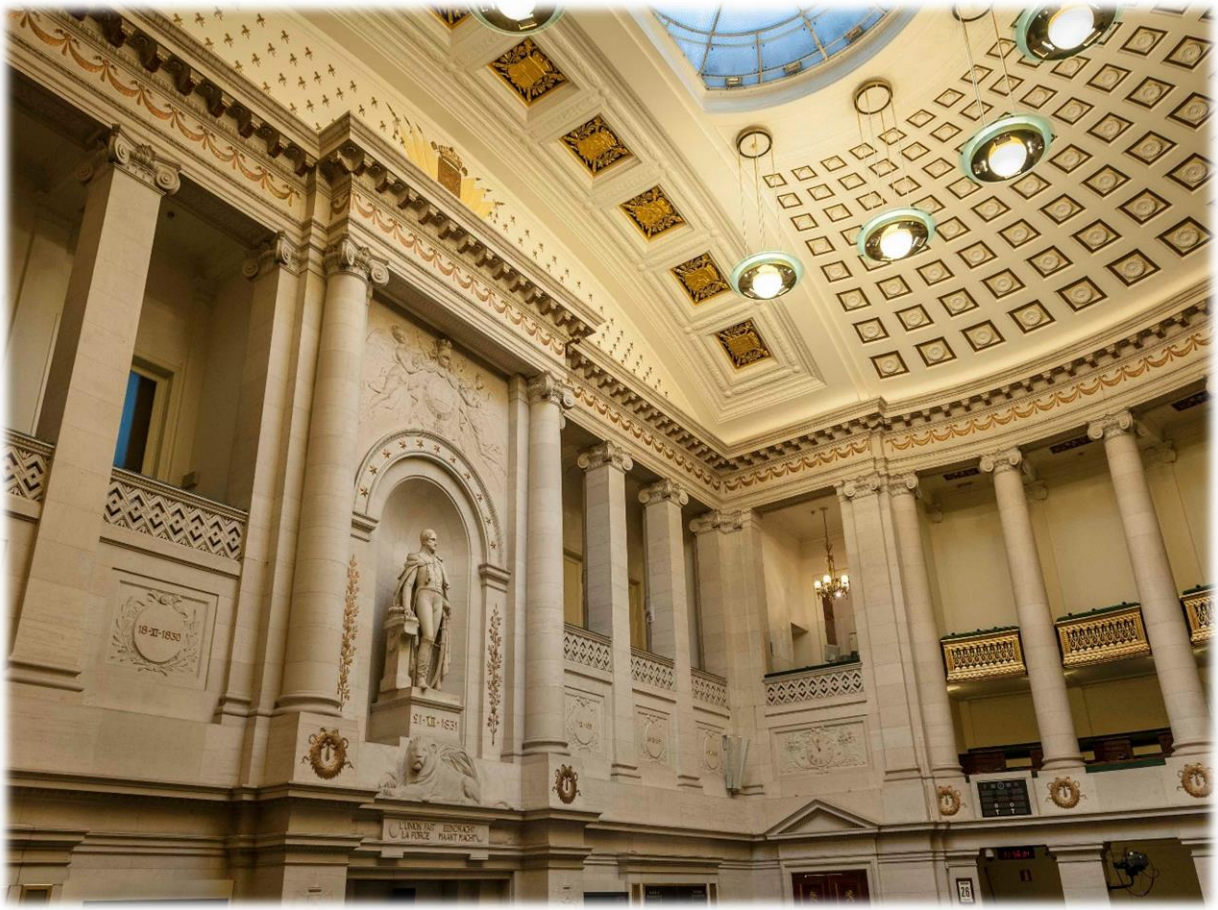
B. Cadre légal

6. Le cadre légal a déjà été décrit et se compose avant tout des normes internationales – à savoir le RGPD (Règlement général sur la protection des données) et la *LED* (la *Law Enforcement Directive* ou directive police/justice 2016/680) – et d'autre part des normes nationales, à commencer par la LPD (loi relative à la protection des données), la LFP (loi sur la fonction de police) et la LCA (loi portant création de l'Autorité de protection des données). À cela s'ajoutent naturellement des lois sectorielles ainsi que nombre d'arrêtés d'exécution et de circulaires qui, pour autant qu'ils soient pertinents pour la GPI et pour les autres services soumis au contrôle du COC, le sont également pour le COC.

C. Vision et mission

7. Le COC aspire à contribuer à un fonctionnement policier et une gestion de l'information policière qui soient à la fois performants, démocratiques et conformes à la définition d'un État de droit. Il est investi de la même mission à l'égard de l'AIG[10] et de la BELPIU.[11]

Il adopte comme vision une attitude constructive en commençant par assister et sensibiliser les institutions contrôlées. Ce n'est qu'en dernier recours, ou en cas de constatation d'une pratique illégale/irrégulière, qu'il procédera éventuellement à une répression à travers la prise de mesures correctrices.



[10] Inspection générale de la police fédérale et de la police locale - cf. article 2 de la loi du 15 mai 2007 sur l'Inspection générale et portant des dispositions diverses relatives au statut de certains membres des services de police.
[11] L'Unité belge d'information des passagers (*Passenger Information Unit* ou *PIU*) visée au chapitre 7 de la loi du 25 décembre 2016 relative au traitement des données des passagers.

D. Les activités de l'Organe de contrôle (COC)

I. INTRODUCTION

1.1. Compétences et missions

1.1.1. Quatre missions et tâches prioritaires

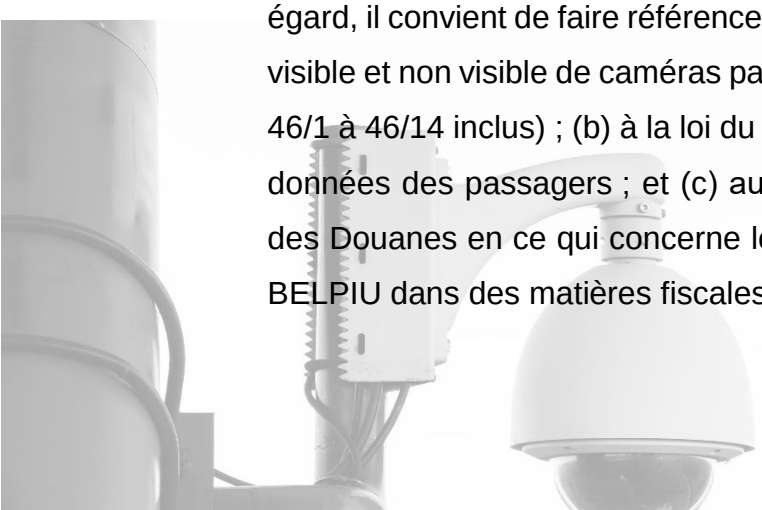
8. Les compétences, missions et tâches du COC sont principalement définies dans la LPD, et en particulier à l'article 71 et au titre VII, d'une part, et dans la LFP d'autre part. Dans les grandes lignes, elles incluent :

(1) la surveillance de l'application du titre II de la LPD à l'égard de la GPI, de l'AIG et de la BELPIU et toutes les missions ayant trait à la protection de la vie privée dans le cadre de l'exécution des missions opérationnelles de ces institutions (dont, à titre principal, les missions de police administrative et judiciaire) ;

(2) la surveillance de l'application du RGPD et du titre I^{er} de la LPD par la GPI et toutes les missions ayant trait à la protection de la vie privée dans le cadre de l'exécution des missions non opérationnelles (par exemple le recrutement et la sélection) ;

(3) le contrôle du traitement de l'information et des données à caractère personnel visées aux articles 44/1 à 44/11/13 de la LFP, y compris celles introduites dans la BNG, les banques de données essentielles, les banques de données particulières, les banques de données techniques et les banques de données communes terrorisme et extrémisme susceptible de conduire au terrorisme ;

(4) toute autre mission qui lui est confiée par ou en vertu d'autres lois. À cet égard, il convient de faire référence (a) à la LFP et plus précisément à l'utilisation visible et non visible de caméras par la GPI (articles 25/1 à 25/6 inclus ou articles 46/1 à 46/14 inclus) ; (b) à la loi du 25 décembre 2016 relative au traitement des données des passagers ; et (c) aux nouvelles compétences du COC à l'égard des Douanes en ce qui concerne les réquisitions adressées par ce service à la BELPIU dans des matières fiscales.



9. En regroupant ces compétences, missions et tâches en volets, nous pouvons donc distinguer les 4 grands domaines d'activités suivants :

(1) Activité 'Autorité de protection des données' à l'égard de la GPI, de l'AIG et de la BELPIU ;

(2) Activité 'Contrôle et surveillance de la gestion de l'information policière et des banques de données communes terrorisme'[12] à l'égard de la GPI et de l'OCAM ;

(3) Activité 'Méthodes administratives particulières', et plus précisément – actuellement – toutes les formes d'utilisation de caméras par la police ;

(4) Activité à l'égard de l'Administration générale des Douanes et Accises dans les matières fiscales et ayant trait aux données de l'information des passagers.

1.1.2. Compétences

10. Les compétences du COC sont décrites au titre VII de la LPD. En résumé, il s'agit de missions d'inspection classiques englobant un droit d'accès illimité à toutes les informations et données - d'enquêtes sur le terrain s'assortissant d'un droit d'accès illimité incluant entre autres la saisie d'objets et de documents, la réalisation de toutes les constatations utiles, l'imposition de délais de réponse contraignants, l'accès au Registre national et l'utilisation du numéro de Registre national, la réalisation d'auditions, la réquisition d'experts et d'interprètes, etc. Ces compétences s'inspirent très largement de celles des Comités P et R et/ou de leurs services d'enquête. Il n'en subsiste pas moins à l'heure actuelle quelques problèmes et points susceptibles d'amélioration, que nous épinglerons dans la suite du présent rapport annuel.

[12] Dans les travaux parlementaires de la loi de 2014 relative à la gestion de l'information policière, nous pouvons lire à ce propos ce qui suit : *« Par ailleurs, les missions essentielles, en termes de contrôle de la gestion de l'information policière opérationnelle, dévolues initialement à l'organe de contrôle restent inchangées, à savoir, contrôler la circulation efficace, maximale, sécurisée des données et informations policières sur la base du besoin d'en connaître, ainsi que le respect des procédures de traitement de l'information policière opérationnelle. », Doc. Parl.* Chambre 2013-2014, n° 3105/001, 63.

1.1.3. Organisation et composition

11. La structure du COC s'est inspirée du Comité permanent R existant. Le nombre de membres a cependant été limité à 3 : un Président/magistrat du siège, un membre-conseiller/magistrat du ministère public et un membre-conseiller/expert, qui possèdent tous le même statut que les membres des Comités permanents et constituent ensemble le comité de direction (DIRCOM). Un 'service d'enquête' (DOSE[13]) composé de 3 membres a également été créé : 2 membres provenant de la GPI et 1 expert. Vient enfin un 'service d'appui' (secrétariat) composé de 1 juriste, 1 informaticien et 1 assistant de direction. Le COC peut en outre recruter contractuellement[14] jusqu'à maximum 30 % de son effectif total (sur un cadre de 9 ETP), ce qu'il a fait en partie, en recrutant 1 juriste contractuel, portant ainsi l'effectif total à 10 ETP. Actuellement, le COC affiche donc un cadre quasiment complet et exploite pour ainsi dire entièrement ses possibilités.

Il convient à cet égard de souligner que toute la politique de gestion des ressources humaines doit également être assurée par les membres du DIRCOM, et ce sans soutien. Cette mission englobe l'élaboration d'un statut et l'établissement d'ordres de service, la conduite d'entretiens de fonctionnement et d'évaluation, le fonctionnement journalier de la politique du personnel (gestion des maladies, des congés, etc.) sans oublier les autres dossiers journaliers dits PLIF,[15] à savoir la logistique, tous les aspects des TIC et les finances (budget, comptes, etc.). Il va de soi que tout cela coûte aux membres du DIRCOM une certaine capacité qu'ils ne peuvent donc pas investir dans le contenu de leur fonction. Contrairement à toutes les autres institutions parlementaires collatérales, le COC ne dispose pas d'une administration et encore moins d'un dirigeant administratif (comme par exemple, le greffier auprès des Comités P et I ou l'administrateur auprès de l'Autorité de protection des données ainsi que leur personnel), de sorte que ce rôle doit lui aussi être assumé par les membres du DIRCOM.

[13] **D**ienst **O**nderzoeken/**S**ervice d'**E**nquête.
[14] En vertu de l'article 21, 1er et 2e alinéas du Règlement d'ordre intérieur du COC tel qu'approuvé par la Chambre des Représentants le 14 novembre 2018, *M.B* 27 novembre 2018, 90687.
[15] Personnel, Logistique, Informatique et Finances.

1.1.4. Quelques chiffres-clés relatifs à l'organisation interne

12. Il est clair que le COC est une institution de petite envergure, non seulement compte tenu de ses missions et des institutions et organes qu'il doit contrôler, mais aussi en comparaison d'institutions parlementaires similaires. Le Comité P possède par exemple un cadre de 93 ETP, dont 52 enquêteurs et 36 collaborateurs administratifs,[16] autrement dit 10 fois plus de capacité que le COC. Le Comité R compte 24 ETP, dont 5 enquêteurs et 16 collaborateurs administratifs,[17] ce qui lui confère donc plus du double de la capacité du COC.

13. Il convient également de souligner que cette pleine capacité de 10 ETP n'a été atteinte que le 1er octobre 2019. L'effectif de départ au 5 septembre 2018 se composait de 5 ETP, à savoir 3 membres de direction et 2 membres du DOSE. Ce n'est qu'en 2019 que le COC a été complété d'une assistante de direction (1er mars 2019), d'un conseiller en technologies et sécurité de l'information (1er mars 2019), d'un membre-fonctionnaire de police (1er juin 2019) et de 2 juristes (respectivement le 1er septembre et le 1er octobre 2019) afin de parvenir à un cadre pour ainsi dire complet.

Le nombre et la taille de la ou des organisation(s) et des services relevant de sa surveillance doivent être rappelés et obligent le COC à opérer des choix difficiles :

(1) la GPI dans son ensemble, à savoir la police fédérale (52 entités) et les corps de la police locale (185 au 1er janvier 2019), soit au total quelque 240 entités composées d'environ 50.000 membres du personnel ;

(2) l'Inspection générale de la police fédérale et de la police locale ;

(3) l'Unité d'information des passagers ;

(4) l'OCAM dans le cadre du contrôle des banques de données communes ;

[16] Voir *www.comitep.be*.
[17] Voir *www.comiteri.be*.

(5) le département contentieux de l'Administration générale des Douanes et Accises dans le cadre des réquisitions adressées à la BELPIU dans des matières fiscales.

14. A elle seule, la quantité de données à caractère personnel et d'informations contenues dans les banques de données policières opérationnelles existantes est de nature à amener le COC à mettre en garde contre des attentes irréalistes. La BNG contient par exemple plus de 70.000.000 données, plus de 25.000.000 faits, plus de 270.000 enquêtes, plus de 3.000.000 personnes et environ 70.000 organisations. Plus de 45.000 événements et quelques 17.000 personnes à suivre par la police administrative donnent également une indication de l'envergure des activités policières ayant directement trait à des données à caractère personnel. Le nombre de notifications (plus de 5.000.000), d'interventions (environ 3.000.000), d'apostilles (plus de 1.300.000), de procès-verbaux judiciaires (plus de 1.300.000) et de rapports d'information (plus de 50.000) est tout simplement impressionnant et contraint tout organe de contrôle au réalisme. Un peu plus d'un an de fonctionnement du COC sous sa nouvelle forme a d'emblée démontré l'augmentation exponentielle de la charge de travail à laquelle il a été confronté. Le COC est dès lors contraint d'établir des priorités.

15. En 2018 et durant le premier semestre de 2019, il était assez logiquement encore en train de mettre au point sa propre organisation : l'établissement d'un budget, l'élaboration d'un statut pour les membres de son personnel,[18] l'établissement d'un règlement d'ordre intérieur,[19] la mise au point de son propre environnement de ICT, l'élaboration d'un plan stratégique (voir plus loin), etc. La capacité existante, dont on peut s'attendre à ce qu'elle ne soit pas élargie dans l'immédiat, est donc une réalité qui conduit inévitablement à l'établissement de priorités, mais qui n'empêche pas le nouveau COC de nourrir de grandes ambitions.

[18] Statut faisant partie du Règlement d'ordre intérieur qui a été approuvé par l'assemblée plénière de la Chambre des Représentants, voir *Doc. Parl.* Chambre 2018-19, n° 3332/001.
[19] Ibidem.

Ce n'est qu'au bout de quelques années de fonctionnement que l'on saura si ces ambitions pourront être entièrement réalisées. L'actuel DIRCOM établira ce bilan en fin de mandat.

1.1.5. Quelques mesures internes pertinentes

16. Le COC dispose aussi de sa propre infrastructure informatique, pour laquelle il fait appel à un fournisseur externe (qui dessert également un grand nombre de zones de police) mais vu la sensibilité des données et le rôle de modèle que le COC endosse en matière de sécurité de l'information, il sollicite énormément la capacité de son propre informaticien, qui est seul pour s'acquitter de ces tâches.

Le COC est en tout état de cause en quête de synergies avec d'autres institutions (parlementaires ou non), dont le Service public fédéral (SPF) BOSA.[20] En application d'un accord-cadre avec le SPF BOSA, le COC soumettra aussi régulièrement son propre environnement de ICT à des tests PEN.[21] Le résultat d'un tel test de cybersécurité permet de se faire une idée du niveau de maturité de la cybersécurité au sein de sa propre organisation. Des synergies ont par ailleurs été recherchées,[22] notamment avec la Commission de nomination pour le notariat, de sorte que le COC bénéficie d'un soutien comptable et budgétaire partiel, et avec l'Autorité de protection des données (en abrégé 'APD') en ce qui concerne un certain nombre de missions de traduction aussi longtemps que le COC ne dispose pas d'une capacité de traduction propre.

Par ailleurs, le COC s'occupe de conclure des conventions de traitement avec des fournisseurs tiers.

[20] Stratégie et Appui.
[21] Tests de pénétration.
[22] Moyennant il est vrai, le paiement d'un tarif avantageux.

II. LES ACTIVITES DANS LE CADRE DE DOSSIERS AXES SUR LA PROTECTION DES DONNEES

2.1. Protection des données : les demandes d'accès indirects

17. Les demandes formulées par la personne concernée (le citoyen) en vue de l'exercice de ses droits d'accès/prise en connaissance, de la rectification ou de la suppression de ses données à caractère personnel dans les banques de données policières, constituent une part substantielle du travail quotidien du COC. Dans la pratique, les 'dossiers article 42 de la LPD'[23] ou 'dossiers AI'[24] (anciennement dénommés 'dossiers articles 13 de la LVP 1992') ont été repris de l'APD dès mai 2018 (et donc bien avant le moment auquel le COC a véritablement acquis la compétence juridique à cette fin), dans le sillage d'une réunion entre le COC et l'APD pendant laquelle il était apparu que ces dossiers s'étaient retrouvés dans une sorte de vide juridique depuis l'entrée en vigueur de la LCA et du RGPD le 25/5/2018. Le COC s'est montré disposé à reprendre dès ce moment les dossiers existants dans lesquels la Commission de protection de la vie privée/APD n'avait pas encore contacté la GPI (et qui en étaient donc encore à un stade initial), ainsi que tous les nouveaux dossiers à partir du 31.05.2018.

18. Contrairement à la grande majorité des polices des pays de l'UE qui disposent d'un système d'accès direct, en Belgique, ces dossiers sont traités en première ligne par le COC. Chaque fois que le citoyen adresse à la GPI une demande en la matière, la GPI la transmet au COC.

---

[23] L'article 42 de la LPD est l'article de base en la matière et dispose en son premier alinéa : *« La demande d'exercer les droits visés au présent chapitre à l'égard des services de police au sens de l'article 2, 2°, de la loi du 7 décembre 1998 organisant la police intégrée, structurée à deux niveaux ou de l'Inspection générale de la police fédérale et de la police locale, est adressée à l'autorité de contrôle visée à l'article 71* (terme désignant le COC, NDLR.) *»*.

[24] 'AI' signifiant 'Accès indirect'.

Le COC constate que même dans les cas où la police elle-même est déjà d'avis qu'un certain enregistrement doit être effacé ou corrigé, elle ne le fait pas mais se contente de réorienter le citoyen vers le COC et attend la décision du COC. Le COC doit régulièrement attirer l'attention de la GPI sur le fait que cette méthode n'est pas correcte. Rien ne l'empêche en effet – et elle y est même obligée en sa qualité de responsable du traitement – de procéder elle-même immédiatement à la rectification ou à l'effacement du (des) enregistrement(s) ou d'adresser une demande à cette fin à l'unité d'enregistrement, et ce en vertu notamment des articles 44/1, §1er de la LFP et 28, 1° à 4° inclus de la LPD. Les données à caractère personnel que la police traite doivent en effet être 'exactes' (principe d'exactitude).

19. Le volume de dossiers a connu depuis la publication du nouveau cadre de la protection des données une augmentation exponentielle, de sorte que le COC a fait face et doit faire face à l'énorme affluence. En 2018, le COC a reçu pas moins de 322 demandes. En 2019, le COC a recensé 392 nouvelles demandes. À titre de comparaison, la CPVP traitait en moyenne entre 100 et 150 dossiers par an, de sorte que le nombre de dossiers a plus que doublé depuis l'entrée en vigueur du nouveau cadre de la protection des données.

Tableau 1 : Evolution du nombre de demandes d'accès indirect adressées au COC

Année	Nombre de dossiers AI
2018	333[25]
2019	392

20. Des 392 dossiers AI qui ont été introduits en 2019, 243 avaient déjà été traités au 01/03/2020. Autrement dit, cela signifie que 62 % des demandes sont clôturées dans l'année avec réponse à la personne concernée.

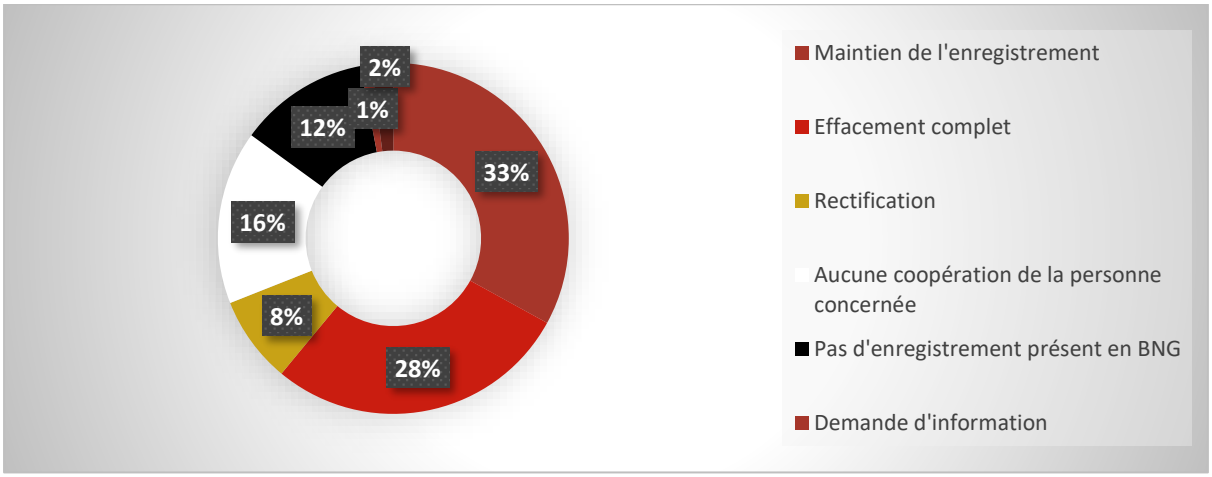
[25] Comme nous le disions, le COC n'a pas repris tous les dossiers de 2018, bien que le COC considère, vu les délais qui avaient cours à l'époque au sein de la Commission de protection de la vie privée et les conventions qui ont été passées par la suite, qu'il a bel et bien reçu et traité la grande majorité des dossiers d'accès indirect introduits en 2018.

Vu le fort coefficient de travail et le fait que le COC dépende de la rapidité avec laquelle la GPI répond aux demandes qu'elle reçoit, le COC considère d'ores et déjà ce chiffre comme méritoire et en tout état de cause, plus performant que les délais de traitement de la Commission de protection de la vie privée de l'époque. Le DIRCOM n'en aspire pas moins à améliorer ce pourcentage dans les années à venir.

21. De ces 243 dossiers, 171 avaient trait à la Banque de données nationale générale (BNG). Voici les résultats et/ou l'orientation finale donnée pour ces 171 'dossiers BNG' :

- maintien de l'enregistrement : 59, soit 33,33 %
- effacement complet du (des) enregistrement(s) : 49, soit 27,68 %
- rectification du (des) enregistrement(s) : 15, soit 8,47 %
- aucune coopération de la part de la personne concernée[26] : 29, soit 16,38 %
- il n'y avait pas d'enregistrement dans la BNG : 21, soit 11,86 %
- la demande était en réalité purement une demande d'informations : 1, soit 0,56 %
- la demande n'était pas recevable : 3, soit 1,69 %

<u>Figure 1 :</u> Décisions finales des demandes AI ayant trait à la BNG



[26] Ce manque de coopération peut revêtir différentes formes : absence de réaction aux demandes ultérieures du COC, absence de transmission d'une copie de la carte d'identité ou d'un autre document pouvant attester de l'identité, etc.

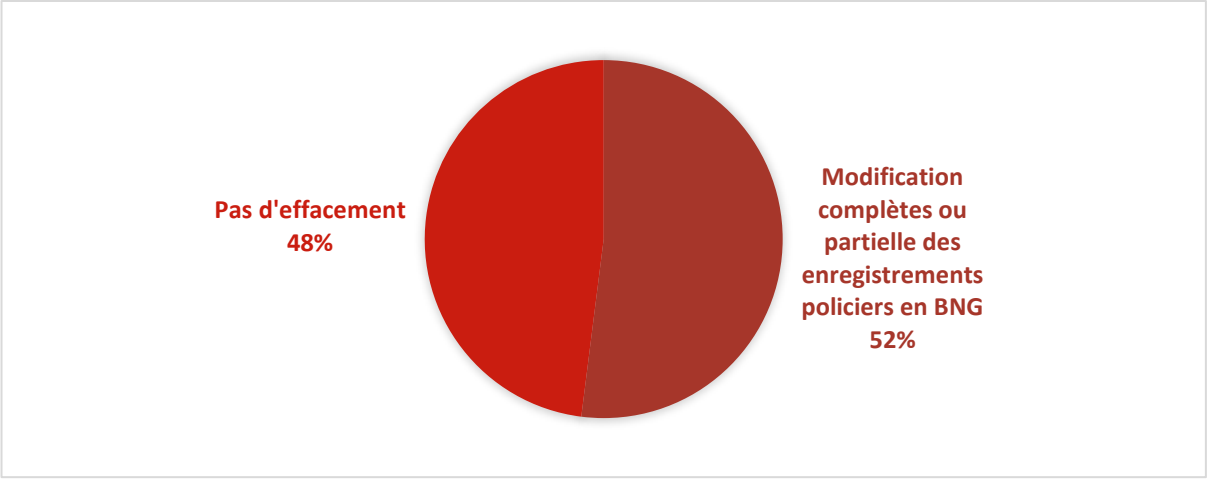
Le nombre total de résultats/orientations est légèrement supérieur au nombre total de dossiers BNG (171) du fait qu'un dossier peut parfois conduire à plusieurs orientations/décisions finales. Les dossiers qui ne sont pas recevables ou dans lesquels il n'y a pas ou plus de coopération de la part de la personne concernée peuvent par exemple se solder par un maintien de l'enregistrement.

Tableau 2 : Décisions finales concrètes du COC dans le cadre des demandes d'accès indirect ayant trait à la BNG

Résultat	**2019**
Maintien de l'enregistrement	59
Rectification	15
Archivage/effacement	49
Total	**123**

Si nous prenons uniquement les dossiers dans lesquels le COC a émis une **évaluation concrète,**[27] nous constatons qu'environ **52 %** des dossiers traités en 2019 (64 dossiers sur 123) se sont soldés par un effacement complet ou partiel des enregistrements effectués par la police dans la BNG. C'est beaucoup, et il y a de quoi inciter la GPI à la réflexion et à l'action.

Figure 2 : Décisions finales concrètes du COC dans le cadre des demandes AI



[27] À savoir uniquement les dossiers qui se sont soldés par un maintien de l'enregistrement, une rectification ou un effacement complet.

Chaque dossier requiert un investissement substantiel de la part des gestionnaires de dossiers du COC. Ces gestionnaires de dossiers sont en principe les deux membres-conseillers et les deux juristes du COC. Le DOSE n'est en principe pas chargé de ces dossiers, si ce n'est en présence de demandes spécifiques concernant le fonctionnement opérationnel concret de la police ou pour venir temporairement en appui des membres-conseillers.

Tableau 3 : Nombre de dossiers clôturés en 2019, ventilés en fonction du type de banque de données policière auquel la demande avait trait[28]

Type de banque de données	2019
BNG	171
SIS II	68
Autre[29]	1
Europol	7
Interpol	3
Total	250[30]

22. Un dossier AI induit un très fort coefficient de travail et inclut plusieurs étapes que nous résumons en substance ci-après : analyse de la demande, consultation de la (des) banque(s) de données policière(s) concernée(s), consultation (des divers organes ou entités[31]) de la GPI (et éventuellement du ministère public compétent) concernant la pertinence opérationnelle d'un ou plusieurs enregistrements, concertation entre la GPI et le COC, correction/ventilation éventuelle ou archivage des données, contrôle par le COC des rectifications ou effacements promis par la GPI, communication avec le plaignant/déclarant ou son avocat, etc.

[28] Vu que le programme informatique du COC n'a permis qu'à partir de la fin 2018 de distiller les résultats et orientations finales des dossiers, seuls les chiffres de 2019 peuvent être fournis.
[29] Le type 'Autre' couvre notamment les banques de données communes terrorisme et extrémisme, les banques de données d'Interpol, une banque de données particulière, etc.
[30] Ce total de 250 dépasse le nombre de dossiers clôturés (234) étant donné qu'une même demande peut avoir trait à plusieurs banques de données policières.
[31] Une demande peut en effet avoir trait à plusieurs enregistrements réalisés par différents services de police.

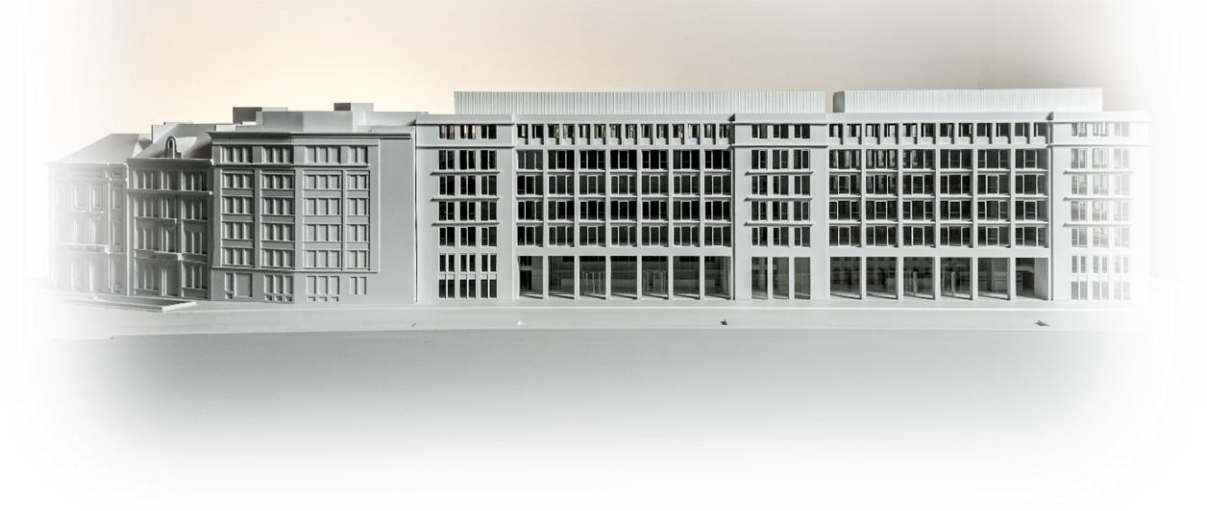
Nous constatons par ailleurs que les citoyens se font de plus en plus souvent assister par un avocat.

23. C'est notamment sur la base de ces dossiers que le COC est amené à constater au quotidien, par le biais de sa possibilité de consultation directe de la BNG, que la BNG contient encore de nombreuses inexactitudes et/ou erreurs. Il peut par exemple s'agir d'enregistrements qui auraient déjà dû être archivés, d'enregistrements qui confèrent aux faits une qualification erronée (soit *ab initio*, soit à partir d'un certain stade d'une enquête, soit après que le parquet a qualifié les faits), de rapports d'information qui ont soit perdu une grande partie de leur pertinence ou auraient dû eux-mêmes être effacés, de signalements qui restent ouverts sans aucune valeur ajoutée et ne font plus l'objet d'aucune évaluation, etc.

24. Enfin, les dossiers AI sont parfois l'occasion pour le COC de se pencher et/ou de formuler des réponses sur des problèmes, des questions ou des thèmes qui relèvent plutôt des principes ou qui reviennent fréquemment. Le présent rapport annuel n'est pas l'endroit où s'appesantir sur ce point, mais il vaut néanmoins la peine de mentionner l'hypothèse erronée mais fréquemment évoquée – aussi par des avocats – selon laquelle un classement sans suite par le ministère public doit *ipso facto* conduire à une 'ventilation'[32] des enregistrements policiers dans la BNG. Le même raisonnement est évoqué avec encore plus de pertinence en cas de non-lieu prononcé par une juridiction d'instruction ou d'acquittement prononcé par une juridiction de jugement. Ce raisonnement est erroné. Les règles régissant l'enregistrement policier, la conservation et le délai de conservation sont des règles juridiques autonomes qui sont en principe entièrement indépendantes de toute décision du parquet ou verdict judiciaire.

[32] Le terme relève du jargon professionnel. Du point de vue légal, seuls 'l'archivage et l'effacement' de données à caractère personnel existent. La notion de 'ventilation' vise dans la pratique les deux termes. Dans le système prévu par la LFP, les données sont en effet en principe d'abord archivées et ensuite effacées.

Par ailleurs, il est important de préciser qu'une personne concernée n'a à notre avis pas la possibilité d'opposer un moyen de droit à la décision prise par le COC dans le cadre d'un dossier AI. Le COC ne fait en effet que se substituer à la personne concernée dans l'exercice de ses droits. Cela ne veut naturellement pas dire que la personne concernée ne puisse pas intenter une action en justice lorsque la réponse du COC ou la manière dont le COC a exercé ses compétences ne lui donne pas satisfaction. Néanmoins, l'action doit dans ce cas être intentée contre le responsable du traitement (soit les ministres compétents, soit la GPI), et non contre le COC. Le COC est demandeur de davantage de clarté à ce sujet dans la LPD (voir plus loin).



2.2. Protection des données : les demandes d'information et les demandes d'avis

25. En outre, le COC est régulièrement consulté tant par des citoyens que par des professionnels (fonctionnaires de police, fonctionnaires en charge de la protection des données – DPO,[33] syndicats, mutualités, instances judiciaires, universités, autres organes de contrôle, avocats, ONG, etc.) concernant principalement – mais pas exclusivement – des questions ayant trait à la protection de la vie privée et à la protection des données.

Une grande part de ces questions ont trait à la licéité de certains flux de données à destination, mais surtout en provenance de la GPI. La GPI est-elle autorisée à transmettre des données opérationnelles à des huissiers de justice, des curateurs, des parties impliquées dans un accident de la circulation, des services d'incendie, une CSIL[34] ou CSIL-R[35] ou en son sein, à la STIB,[36] à un bourgmestre, au service Perception et Recouvrement du SPF Finances, etc. ?

26. De nombreuses questions sont aussi posées spécifiquement en ce qui concerne l'utilisation de caméras par la GPI, mais nous y reviendrons plus loin. Voici quelques exemples des questions posées au COC :

(1) Quand y a-t-il lieu de signaler une brèche de sécurité ?[37]
(2) Quelles données la GPI est-elle autorisée à communiquer dans le cadre d'enquêtes de moralité et de sécurité ?
(3) Quid de l'accès aux banques de données policières des collaborateurs de police absents (pour une longue période) ?

[33] Délégué à la protection des données.
[34] Cellule de Sécurité Intégrale Locale.
[35] Cellule de Sécurité Intégrale Locale Radicalisme. Voir aussi la loi du 30 juillet 2018 portant création de cellules de sécurité intégrale locales en matière de radicalisme, d'extrémisme et de terrorisme.
[36] Société des transports intercommunaux de Bruxelles.
[37] Une brèche de sécurité (*data breach* en anglais) est une violation de la sécurité (voir l'article 61 de la LPD).

(4) La GPI doit-elle donner suite à une demande émanant d'un citoyen/avocat en vue de l'obtention d'une fiche d'intervention ?

(5) Quand faut-il procéder à une analyse d'impact relative à la protection des données (AIPD) ?[38]

(6) La GPI peut-elle recourir à un système d'empreintes digitales dans un contexte relevant du droit du travail (accès au bâtiment/bureaux de la police pour le personnel, utilisation des photocopieuses par le personnel après vérification des empreintes digitales, etc.) ?

(7) Quid des enregistrements sonores réalisés par des *bodycams* ?

(8) Etc.

27. L'afflux de ces questions et/ou problèmes est la preuve que le COC a en peu de temps, gagné en notoriété et en confiance, mais cette médaille a évidemment son revers. La capacité requise pour apporter une réponse qualitative à ces demandes se retrouvera de plus en plus sous pression à l'avenir et demeurera un défi de taille. Sur la totalité de 2019, le COC a reçu 82 demandes d'avis dont 80 avaient été traitées au 01/03/2020.

Le COC s'efforce de répondre à ces demandes dans un délai d'un mois. Dans de nombreux cas, la réponse est envoyée plus rapidement, en fonction de la complexité et du degré de difficulté. Certaines demandes nécessitent en effet une analyse très approfondie de la problématique et ne se laissent pas résumer en réponses simples.

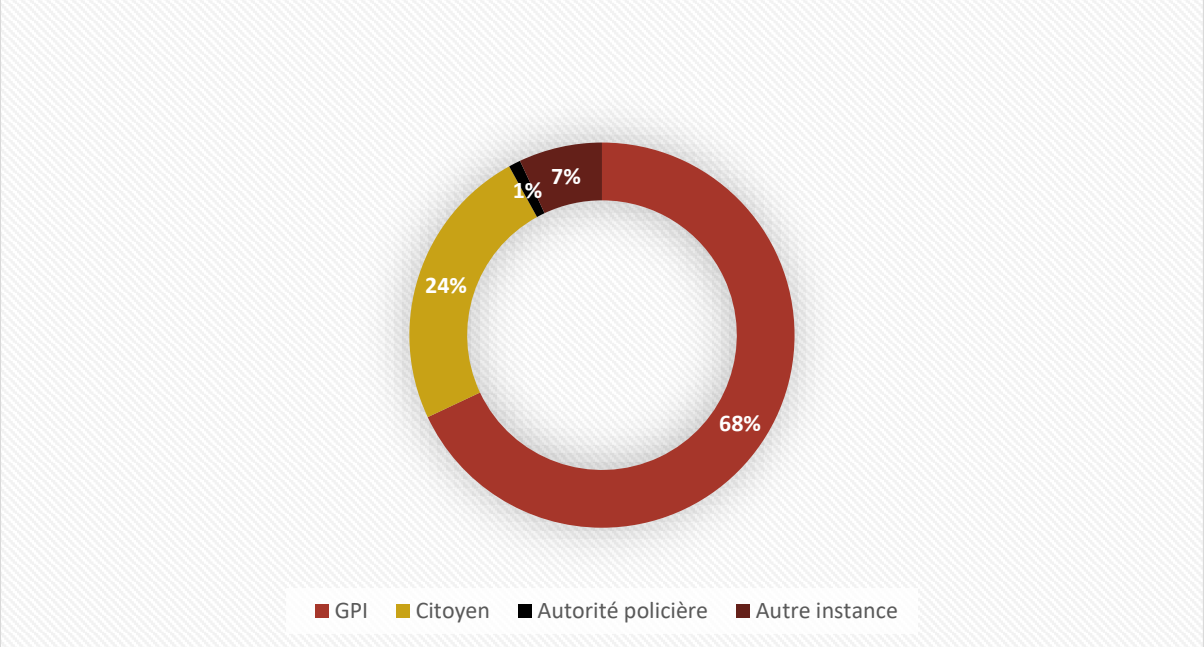
Il se peut enfin qu'une question ou demande donne lieu à une enquête d'office de la part du COC, voire à l'exercice de ses compétences correctrices, comme ce fut notamment le cas pour la question relative à l'utilisation (qui s'est d'ailleurs soldée par une interdiction) des empreintes digitales du personnel dans le contexte du RGPD (par exemple pour le contrôle de l'accès du personnel aux locaux, pour l'utilisation de certains appareils, etc.).

[38] Analyse d'impact relative à la protection des données.

Tableau 4 : Nombre de dossiers de demandes d'informations sur le thème de la protection des données selon l'origine du demandeur

Origine du demandeur	2018[39]	2019	2019 en %
GPI		55 ou 68 %	68
Citoyen		19 ou 23,5 %	23,5
Instance policière		1 ou 1 %	1
Autre instance		6 ou 7,5 %	7,5
Total	**23**	**81**	**100**

Figure 3 : Nombre de dossiers de demandes d'informations sur le thème de la protection des données, selon l'origine du demandeur



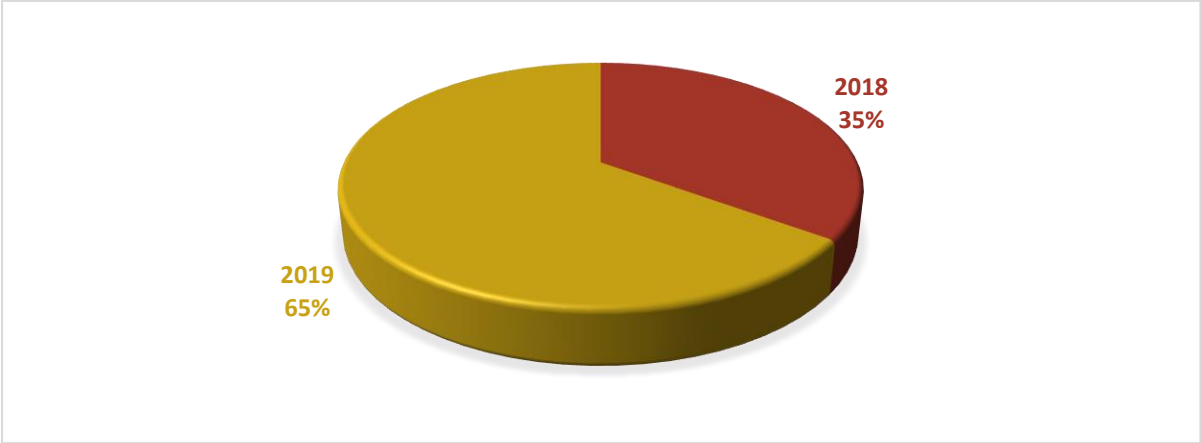
[39] Vu que le programme informatique du COC n'a permis qu'à partir de la fin 2018 de distiller les résultats et orientations finales des dossiers, seuls les chiffres de 2019 peuvent être intégralement fournis. Pour 2018, nous nous limitons au nombre total.

2.3. Protection des données : les demandes d'avis concernant la législation et la réglementation

Tableau 5 : Demandes d'avis au sujet de la législation et de la réglementation en 2018 et 2019

2018	2019	Total
12[40]	22[41]	34

Figure 4 : Nombre de dossiers de demandes d'avis au sujet de la législation et de la réglementation en 2018 et 2019



28. La principale compétence du point de vue politique est et reste la compétence d'avis du COC sur tous les projets de réglementations ayant entièrement ou seulement (très) partiellement trait aux compétences des entités placées sous la surveillance du COC (s'agissant de la compétence autrefois exercée par la Commission de protection de la vie privée/APD). Dans la grande majorité des cas, ces projets (de lois, d'arrêtés royaux ou ministériels, de circulaires, de protocoles, de notes de service internes, de notes de vision, etc.) émanent du niveau fédéral, mais il peut aussi s'agir de normes des états fédérés (le COC a notamment rendu un avis sur le décret flamand sur les maisons de justice).

[40] Après enquête, il a été décidé dans 3 cas de ne pas rendre d'avis parce que le COC estimait que le texte ne relevait pas de ses compétences ni des compétences des entités placées sous sa surveillance.
[41] *Ibidem.*

L'article 59 §1er, 2e alinéa de la LPD prévoit en effet que *« l'autorité de contrôle compétente est consultée dans le cadre de l'élaboration d'une loi, d'un décret ou d'une ordonnance, ou d'une mesure réglementaire fondée sur une telle loi, un tel décret ou une telle ordonnance, qui se rapporte au traitement »*, s'agissant là de la mise en œuvre de l'article 28.2 de la *LED*. S'il subsistait encore dans le cadre de la LVP de 1992 une discussion au sujet du caractère obligatoire de cette consultation préalable, ce n'est plus le cas aujourd'hui. Pour que le COC doive exercer et exerce sa compétence, il est suffisant qu'un sujet donné comporte un seul article régissant la gestion de l'information policière ou ayant trait à d'autres entités relevant de la surveillance du COC. Dans ce dernier cas, l'APD transmettra en principe au demandeur les avis des autorités spécialisées de protection des données (principalement le COC et le Comité R) ainsi que son propre avis, et endossera ainsi le rôle d'autorité de protection des données *'one stop shop'*.[42] Nombre de demandes arrivent en outre encore par le biais de l'APD, qui vérifiera si – et le cas échéant dans quelle mesure – certaines parties d'un projet relèvent de la compétence du COC (ou du Comité R). De nombreux demandeurs ne sont en effet pas (encore) familiarisés avec le nouveau paysage belge de la protection des données.

29. En 2018 et 2019, le COC a reçu 34 demandes d'avis et a effectivement rendu **28 avis**. Ces avis sont en principe publiés sur le site Internet du COC (www.organedecontrole.be), de manière à ce que non seulement le grand public, mais aussi et surtout toutes les parties prenantes (instances administratives et judiciaires, la GPI, le monde académique, les organisations de la société civile, les ONG, etc.) puissent en prendre connaissance. Il serait impossible d'aborder dans le présent rapport les différents aspects de contenu de tous ces avis, de sorte que nous renvoyons le lecteur au site Internet.

[42] En vertu de l'article 54/1, §1er, 2e alinéa de la LAPD.

Nous ne citerons ici que 4 exemples qui, de la perception du COC, sont vraiment cruciaux :

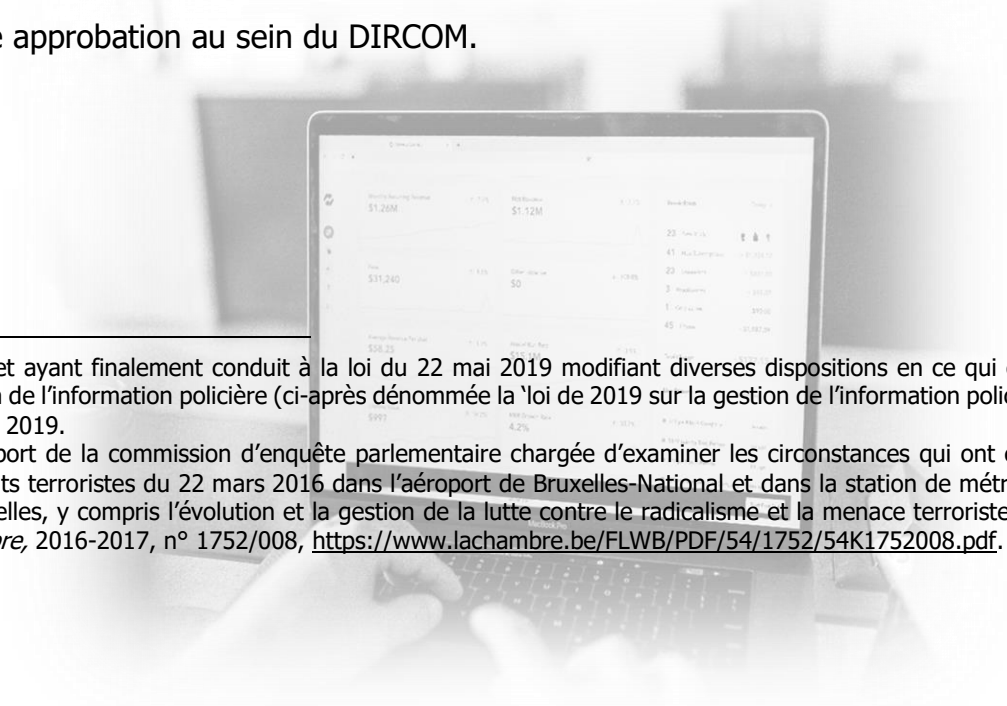
(1) l'avis 9/2018 du 12 décembre 2018 concernant l'*« avant-projet de loi relatif à la gestion de l'information policière et modifiant la loi sur la fonction de police et la loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux »*[43] qui apporte quelques modifications cruciales à la LFP ;

(2) l'avis DA19013 du 17 juin 2019 relatif à un *« avant-projet de loi relative à l'approche administrative communale et portant création d'une Direction Évaluation de l'Intégrité pour les Pouvoirs publics »* qui traite du thème actuel du maintien de l'ordre administratif ;

(3) l'avis DA190019 du 16 décembre 2019 relatif au *« rapport du comité de concertation sur la création d'une banque-carrefour de la sécurité »* qui traite du thème crucial de la création ou non d'une 'banque-carrefour de la sécurité' telle qu'elle a été recommandée par la commission d'enquête parlementaire 'attentats'[44] ;

(4) l'avis DA190011 (rendu conjointement avec le Comité R) du 1er août 2019 concernant un *« projet d'arrêté royal modifiant l'arrêté royal du 21 juillet 2016 relatif à la banque de données commune Terrorist Fighters »* élargissant la banque de données en question à deux nouvelles catégories de personnes.

Ces avis sont préparés et rédigés par un membre du DIRCOM, le cas échéant avec l'aide d'un juriste (et/ou de l'informaticien), et font ensuite l'objet d'une discussion et d'une approbation au sein du DIRCOM.



[43] Projet ayant finalement conduit à la loi du 22 mai 2019 modifiant diverses dispositions en ce qui concerne la gestion de l'information policière (ci-après dénommée la 'loi de 2019 sur la gestion de l'information policière'), M.B. 19 juin 2019.

[44] Rapport de la commission d'enquête parlementaire chargée d'examiner les circonstances qui ont conduit aux attentats terroristes du 22 mars 2016 dans l'aéroport de Bruxelles-National et dans la station de métro Maelbeek à Bruxelles, y compris l'évolution et la gestion de la lutte contre le radicalisme et la menace terroriste, Doc. *Parl. Chambre,* 2016-2017, n° 1752/008, https://www.lachambre.be/FLWB/PDF/54/1752/54K1752008.pdf.

2.4. Protection des données: consultations/traitements illégaux par les membres de la GPI

30. Ces dossiers ont trait à des plaintes de citoyens (ou de fonctionnaires de police) qui estiment ou présument qu'un fonctionnaire de police a consulté indûment leurs données figurant dans les banques de données policières (ou les banques de données tenues à la disposition de la police par le biais de PORTAL).[45] À la mi-2019, il a été convenu avec le Comité P que ce dernier pouvait, dans le cadre d'une première phase de test, transmettre les dossiers de ce type au COC. Il avait à l'époque été question d'une dizaine de dossiers par an. À partir de mai 2019, ces dossiers ont donc été transmis au COC.

Tableau 6 : Nombre de dossiers de plaintes concernant des traitements illicites par des membres de la GPI

Année	Nombre
2019	30

À la date de la clôture du présent rapport d'activité,[46] 14 de ces plaintes avaient été traitées. Le tableau ci-après présente la suite donnée à ces dossiers de plaintes :

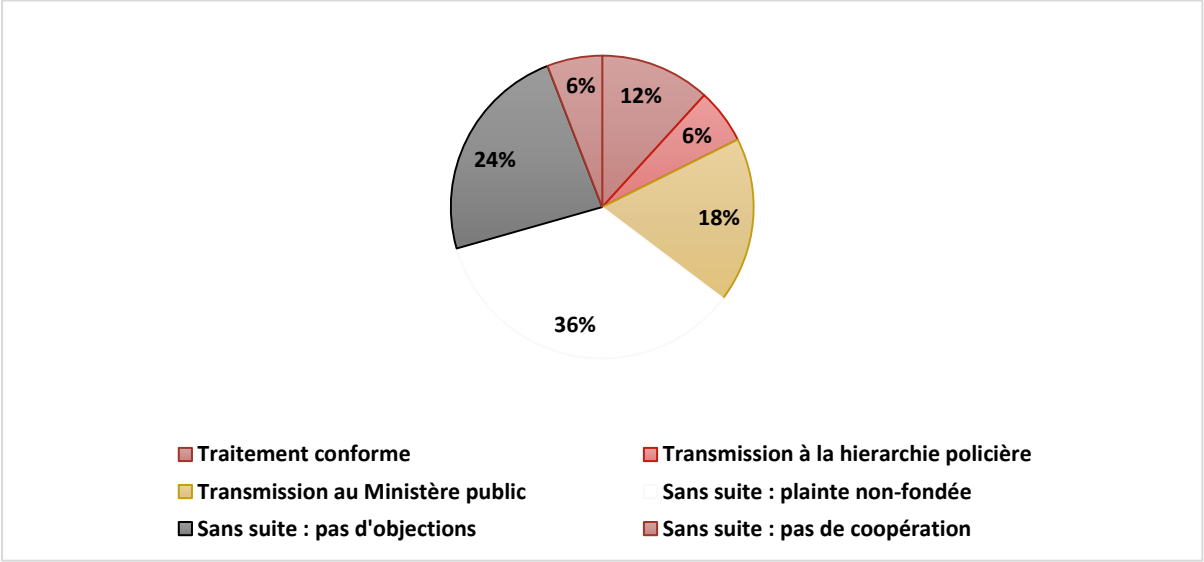
Tableau 7 : Suite donnée par le COC aux dossiers de plaintes

Suite donnée	Nombre
Traitement conforme	2
Transmission à la hiérarchie policière	1
Transmission au ministère public	3
Sans suite : plainte manifestement non fondée	6
Sans suite : pas d'objections	4
Sans suite : pas de coopération	1
Total	**17**

[45] PORTAL est le portail d'accès général réservé aux membres de la GPI. Il s'agit du Registre national (RRN), de la Direction de l'immatriculation des véhicules (DIV) et du registre des armes.
[46] À savoir le 1er avril 2019.

Ici aussi, le nombre total de décisions peut excéder le nombre total de dossiers du fait qu'un même dossier peut s'être soldé par plusieurs suites. Certains aspects de la plainte peuvent par exemple être manifestement non fondés, tandis que d'autres donnent lieu à une transmission au MP ; il arrive aussi que les orientations finales 'traitement conforme' et 'sans suite : pas d'objections' soient données simultanément. La plupart de ces dossiers sont des plaintes contre des fonctionnaires de police concernant des consultations ou des traitements prétendument illicites dans les banques de données policières ; il peut parfois s'agir d'autres aspects, comme une plainte introduite contre la prise d'une photo des documents d'identité d'un suspect au moyen d'un smartphone privé.

Figure 5 : Suite donnée par le COC aux dossiers de plaintes en 2019



31. Depuis mai 2019 (date de la reprise de cette tâche par le COC), 30 dossiers provenant pour la plupart du Comité P ont été ouverts. Il est cependant rapidement apparu que le volume avancé initialement était erroné. Sur une base annuelle, on parle rapidement d'une soixantaine de dossiers, ce qui n'est pas tenable pour le COC vu sa capacité limitée en comparaison des autres autorités de contrôle.

Ces dossiers s'assortissent en effet d'un très fort coefficient de travail que le COC, dont le DOSE qui ne se compose que de 3 membres, ne saurait assumer. De plus, les dossiers de plaintes individuels de ce type ne correspondent ni à l'activité principale ni à la raison d'être du COC, qui souhaite se focaliser avant tout – et a d'ailleurs été initialement constitué pour cette raison – sur les thèmes structurels et organisationnels ayant trait à la gestion de l'information policière. Il est en outre apparu que les plaintes transmises comportaient la plupart du temps des indications de nombreuses autres infractions, voire parfois de délits, pour lesquels le COC n'est de toute façon pas compétent : calomnie/diffamation, violation du secret professionnel, délits informatiques, etc. Autrement dit, des aspects qui ne présentent pour ainsi dire plus aucun rapport avec la compétence du COC en matière de protection des données, mais qui relèvent de la compétence notamment du Comité P. Dans le contexte d'une bonne administration de la justice, il n'est pas indiqué que plusieurs services s'occupent de la même plainte. Début 2020, il a donc été convenu à la demande du COC, après une réunion de concertation avec le Comité P, que chaque institution traiterait à nouveau elle-même (comme par le passé) les plaintes qui lui sont adressées. En principe, tant le Comité P et l'AIG que les services de contrôle interne de la GPI sont en effet compétents pour traiter ces plaintes et dossiers. Le COC, en revanche, est uniquement compétent pour l'aspect de la protection des données.

32. Le COC se limite donc à ses compétences qui ont trait aux infractions à la LPD et portent donc exclusivement sur le traitement/la consultation illicite par un fonctionnaire de police. Le COC ne procède donc ici en tout état de cause qu'à une enquête *prima facie*. Dès qu'un 'suspect' potentiel peut être localisé, le dossier est en principe transmis au contrôle interne de la police. Le COC peut éventuellement aussi le transmettre directement au ministère public compétent (en fonction par exemple de la gravité de l'infraction). Il s'agit en effet aussi toujours de délits (au moins une infraction à l'article 151 du Code pénal et à l'article 222, 1° de la LPD).

À côté de cela et pour terminer, le COC peut aussi recevoir des plaintes visant à dénoncer plus généralement un traitement illicite par un fonctionnaire de police ou par l'organisation policière.

2.5. Protection des données : les enquêtes internationales

33. Le COC et ses membres (du personnel) sont également sollicités pour prendre part à des enquêtes ou visites internationales.

Un commissaire-enquêteur du DOSE a notamment pris part en tant qu'expert belge à la 5e *Joint review of the implementation of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program*[47] à La Haye (le 15 janvier 2019) et ensuite à la visite de terrain à Washington (Etats-Unis) les 31 janvier et 1er février 2019. Ces missions sont pour le membre du personnel un travail d'étude et de participation à l'établissement d'un rapport final. Le rapport de Washington, la *TFTP Review,* peut d'ailleurs être consulté sur le site Internet de la Commission européenne.[48]

En outre, le conseiller en technologies et sécurité de l'information du COC a pris part en tant que membre-expert de la commission d'évaluation à 'l'évaluation Schengen (*SCHEVAL*)' de la Hongrie menée par la Commission européenne du 6 au 11 novembre 2019. Cette mission incluait non seulement la préparation et le travail d'étude requis (pour se familiariser avec les institutions et systèmes informatiques hongrois) mais aussi la visite sur site et ensuite la participation à l'établissement du rapport d'évaluation.

Un membre du DIRCOM a dans le passé (période 2015-2018) également pris part à plusieurs reprises en tant que membre-expert à ces évaluations Schengen, notamment des Pays-Bas, de la Norvège, de la Finlande et de Malte.

[47] Pour plus d'informations à ce sujet, voir https://ec.europa.eu/home-affairs/news/eu-us-cooperation-tackling-terrorist-financing-continues-produce-results_en.

[48] Voir https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20190722_com-2019-342-commission-report_en.pdf.

2.6. Protection des données dans les secteurs et matières spécifiques

2.6.1. *Les inspections BELPIU*

34. La loi du 25 décembre 2016 relative au traitement des données des passagers (la 'loi PNR') met en œuvre les objectifs européens visant la prévention et la lutte contre tant le terrorisme que les délits graves et la criminalité internationale s'inscrivant dans ce contexte. Il a à cette fin été créé au sein du SPF Intérieur une Unité d'information des passagers (BELPIU) qui tient à jour les données des passagers dans une banque de données des passagers dans le but de prévenir et de lutter contre les délits ou menaces définis dans la loi PNR.

Pour tous les passagers qui arrivent en Belgique, partent d'un aéroport belge ou

traversent la Belgique à bord de trains et bus internationaux, toute une série de données à caractère personnel sont enregistrées dans la banque de données des passagers et analysées en fonction d'un nombre restreint de délits ou menaces. Les données des passagers doivent être transmises à la PIU au moins 48 heures avant le départ de la Belgique ou l'arrivée en Belgique par les compagnies aériennes, les transporteurs de passagers et les opérateurs de voyages. Il s'agit globalement de deux catégories de données, à savoir les données dites 'API' ('*Advanced Passenger Information*') ou données d'enregistrement et d'embarquement (numéro de la carte d'identité ou du passeport, nom, prénom et date de naissance, etc.) et les données 'PNR' ('*Passenger Name Records*') ou données de voyage des passagers (nom et adresse, numéro de vol, destination, données de paiement, numéro de siège dans l'avion, heure de départ et d'arrivée, etc.). La PIU a ainsi analysé durant les mois de juillet et août 2019 quelque 5 millions de données de passagers, malgré le fait qu'elle ne reçoit pas encore les données de passagers de toutes les compagnies aériennes, tous les transporteurs de passagers et tous les opérateurs de voyages.

D'ici peu, la PIU disposera donc d'une banque de données colossale regroupant les données de voyage de millions de passagers. Il va ainsi de soi que le traitement des données est soumis à des mécanismes de contrôle interne et externe effectifs et adéquats.

35. Le 27 novembre 2019, l'Organe de contrôle et le Comité R ont mené une visite spontanée et restreinte auprès de la BELPIU. Notons ici que la visite ne faisait pas suite à une plainte (individuelle) ni à l'existence d'indications (concrètes) du non-respect de la législation et de la réglementation par l'UIP visitée.

Vu l'envergure, la nature des données ainsi que la forme du traitement effectué par la PIU, il s'agit d'une violation extrême de la protection de la vie privée.[49] Le traitement des données des passagers est dès lors soumis à des conditions rigoureuses et doit s'assortir des garanties requises. L'angle d'incidence de la visite était donc résolument axé sur le contrôle de la conformité (*'compliance based'*) : le traitement des données des passagers se déroule-t-il dans le respect de la loi et s'assortit-il de l'application d'une norme élevée de sécurité ? Bien qu'il s'agisse d'une visite restreinte, elle était davantage axée sur la sécurité de l'information que sur les aspects juridiques.

[49] Notamment des articles 7 (Respect de la vie privée et familiale) et 8 (Protection des données à caractère personnel) de la Charte des droits fondamentaux de l'Union européenne et de l'article 22 de la Constitution. En marge des données d'identification, l'UIP traite notamment aussi les données de paiement et le comportement de voyage des passagers.

Cet angle d'incidence n'empêche cependant pas le COC et/ou le Comité R de prendre des mesures adéquates lorsque des manquements légaux sont constatés. La visite restreinte se justifiait pour deux raisons. Pour commencer, la PIU n'est opérationnelle que depuis début 2018. Ensuite, les transporteurs de passagers et opérateurs de voyages visés ne sont pas encore tous techniquement connectés avec la PIU. Pour ces raisons, il a été décidé de ne pas encore mener d'enquête approfondie.

La visite se limitait à deux domaines :

(1) Protection informatique et sécurité de l'information.

(2) Proportionnalité du traitement des données, notamment en ce qui concerne :

- la transmission des données PNR à la police fédérale ;

- la procédure de fixation et d'évaluation des critères d'évaluation ;

- les détections ciblées.

La visite s'est déroulée en 2 phases. Durant la 1re phase, les informations et documents nécessaires ont été demandés à la PIU. En fonction du contenu des réponses et des documents, des questions spécifiques ont été formulées en vue de poursuivre l'enquête lors de la visite. Dans un second temps a eu lieu la visite sur place. Celle-ci comportait les volets suivants :

(1) un entretien avec le directeur de l'UIP au sujet de la portée de la visite et des questions additionnelles au sujet des informations et documents transmis au COC ;

(2) le suivi des problèmes mentionnés dans les rapports du DPO dans le cadre des TIC et de la sécurité de l'information ;

(3) une enquête sur la manière dont les critères d'évaluation objectifs sont établis ;

(4) les réquisitions en vue de procéder à des recherches ponctuelles et la dépersonnalisation des données à caractère personnel qui en découlent ;

(5) la journalisation dans le cadre des réquisitions en vue de détections ciblées.

Dans le sillage de cette visite, le COC a formulé un certain nombre de recommandations et de mesures correctrices à l'intention de la BELPIU.

Une version publique du rapport sera mise à disposition sur le site Internet du COC en 2020.

2.6.2. L'Administration générale des douanes et accises

36. Comme nous le disions, le COC a été investi en 2019 d'une nouvelle compétence à l'égard des Douanes (dans la pratique, le service Recherche et le service BELPIU) dans le cadre des réquisitions (demandes) adressées à la BELPIU dans des matières fiscales. L'article 281, §4 de la loi générale sur les douanes et accises du 18 juillet 1977[50] a été à cet égard modifié par la loi du 2 mai 2019 modifiant diverses dispositions relatives au traitement des données des passagers.[51] Cette loi est entrée en vigueur le 4 juin 2019 mais n'a pas encore été appliquée en 2019. Les premiers contacts entre les Douanes et le COC ont néanmoins déjà eu lieu à l'initiative du COC afin d'examiner comment cette disposition devrait être appliquée dans la pratique. Cette disposition prévoit en effet que le COC doit procéder à un contrôle et une vérification *a posteriori* de ces réquisitions en fonction des principes de subsidiarité et de proportionnalité. Dans la pratique, il s'agit généralement de dossiers de fraude aux droits d'accises à travers la contrebande de cigarettes. L'objectif est de convenir en 2020, à travers une forme de protocole, de ce que le COC doit s'attendre à recevoir.

---

[50] *« §4. En recherchant les crimes et délits visés à l'article 8, §1er, 5°, de la loi du 25 décembre 2016 relative au traitement des données des passagers, le conseiller-général désigné pour l'administration en charge des contentieux peut, par une décision écrite et motivée, charger un agent des douanes et accises, de requérir l'UIP afin de communiquer les données des passagers conformément à l'article 27 de la loi du 25 décembre 2016 relative au traitement des données des passagers. La motivation de la décision reflète le caractère proportionnel eu égard à la protection des données à caractère personnel et subsidiaire à tout autre devoir d'enquête. La décision et sa motivation sont notifiées à l'Organe de contrôle de l'information policière visé à l'article 71 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel. L'Organe de contrôle de l'information policière interdit au conseiller-général désigné pour l'administration en charge des contentieux d'exploiter les données recueillies dans des conditions qui ne respectent pas les conditions légales. »*

[51] M.B. 24 mai 2019.

2.6.3. L'Inspection générale de la police pédérale et de la police locale

37. En 2018 et 2019, le COC n'a pas mené d'enquêtes ni de contrôles concernant l'AIG. Il convient de rappeler que la compétence du COC est ici partagée avec l'APD. Le COC est uniquement compétent pour les traitements de données dits 'policiers' de l'AIG (ceux qui relèvent de la *LED* et du titre II de la LPD). Cette institution, qui endosse elle-même un rôle de surveillance, n'a pas été une priorité pour le COC et n'est sans doute pas appelée à le devenir dans un avenir proche. Le rôle de l'AIG n'est d'ailleurs pas vraiment significatif sur le plan des tâches policières opérationnelles. Il va de soi que le COC traite néanmoins les questions éventuelles émanant de l'AIG, de sorte qu'une simplification consisterait évidemment ici aussi à rendre le COC compétent pour les traitements dits 'RGPD' effectués par l'AIG, comme c'est le cas pour la GPI. Il y a en effet lieu d'éviter au maximum qu'un service ou organe relève de plus d'une autorité de protection des données. Une concertation est prévue en 2020 en vue de passer avec l'AIG certaines conventions au sujet des tâches, et pourrait éventuellement déboucher sur l'établissement d'un protocole.

2.7. Les missions MAP : utilisation de caméras par les services de police

2.7.1. Généralités

38. Le COC est avant tout investi d'une mission générale de contrôle à l'égard de toute forme d'utilisation de caméras (voir l'article 46/1 de la LFP et l'article 71, 1° et 3° de la LPD) : visible, invisible (cachée), en un lieu non clos, en un lieu clos accessible au public, en un lieu clos non accessible au public, dans le cadre de la reconnaissance des numéros d'immatriculation (ANPR), avec ou sans caméras ou systèmes intelligents, etc.

Vu l'explosion actuelle de l'utilisation de caméras par la police, il est clair que le COC doit ici aussi établir des priorités claires et ne saurait en aucun cas procéder dans tout le pays à un contrôle proactif de l'utilisation des caméras. Il convient en effet de constater que le public et la presse nourrissent des attentes irréalistes à l'égard des possibilités du COC. Le COC n'est par exemple pas une université ni un organe scientifique en mesure de fournir toutes sortes de statistiques ou chiffres (certainement pas à court ou moyen terme). Il s'agit là avant tout du rôle du (des) responsables du traitement.

En revanche, l'utilisation de caméras par la police (ou certains de ses aspects) est examinée par le COC pour ainsi dire lors de chaque enquête ou visite proactive menée auprès d'une entité de police donnée.

39. Le COC est en outre investi, comme nous le disions, d'un certain nombre de missions qui pourraient être qualifiées de 'missions MAP', autrement dit de quelques missions *sui generis* combinant à la fois des aspects afférents à la gestion de l'information policière et des aspects relatifs à la protection des données.

Il existe en effet des '**M**éthodes **A**dministratives **P**articulières' policières pour lesquelles le COC fonctionne comme une sorte de 'Commission BIM'.[52] Certaines utilisations non visibles de caméras poursuivent en effet une finalité (parfois purement) administrative et ne sont donc pas soumises au contrôle du magistrat compétent, mais bien au contrôle du COC. Concrètement, il s'agit de *« l'utilisation non visible de caméras en raison de circonstances particulières »* (art. 46/4 juncto 46/6 de la LFP) et de *« l'utilisation non visible de caméras dans le cadre de missions spécialisées de protection de personnes »* (art. 46/9 et 46/10 de la LFP).

La problématique principale réside actuellement dans le fait que la notification au COC qui doit être faite par la GPI pour ces utilisations non visibles de caméras n'est pour ainsi dire pas respectée, de sorte que le COC ne dispose pas d'un aperçu (suffisant) de ce type d'utilisation de caméras. Une certaine amélioration est d'ores et déjà perceptible en 2020, mais le problème subsiste. Il s'agit là d'une priorité absolue pour 2020.

2.7.2. Demandes d'information et d'avis concernant l'utilisation de caméras

40. La GPI soumet au COC nombre de questions et demandes concernant l'utilisation de caméras. Entre le 25 mai 2018 (date de l'entrée en vigueur des nouvelles dispositions de la LFP relatives à l'utilisation visible et non visible de caméras) et la fin de 2019, le COC a formulé 32 avis dans le cadre de cette problématique. La grande majorité des demandes émanaient de la police.

[52] Par analogie avec la Commission BIM (Commission administrative chargée du contrôle des méthodes spécifiques et exceptionnelles de recueil des données) dans le cadre des méthodes de renseignements appliquées par les services de renseignement (voir la loi du 30 novembre 1998 organique des services de renseignement et de sécurité).

Tableau 8 : Nombre de demandes d'avis ou d'informations concernant l'utilisation de caméras

Année	Nombre
2019	32

41. Les nouvelles applications ou nouveaux thèmes, comme les caméras dites 'intelligentes' actionnées par certains bruits (initiative de la *ZP Antwerpen* et de la *ZP Limburg Regio Hoofdstad*) qui permettent de déployer les équipes d'intervention de manière plus ciblée ; les questions relatives à l'enregistrement du son par les bodycams ; les questions portant sur les dispositions transitoires et le délai dont la GPI dispose pour mettre ses pictogrammes en conformité avec les nouvelles règles ; la problématique des demandes d'accès aux images des caméras introduites par des personnes concernées ; et les questions concernant la journalisation de la consultation des images, ne sont que quelques-uns des thèmes traités. Toute la question des caméras ANPR, et surtout de la mesure dans laquelle les données ou métadonnées des caméras ANPR peuvent être transmises à des tiers – pouvoirs publics ou acteurs privés – constitue également un thème qui est régulièrement soumis au COC. À cela s'ajoutent les AIPD relatives aux traitements des caméras qui sont soumises pour consultation préalable au COC par les entités de police.

2.7.3. Quelques enquêtes spécifiques

42. En marge des enquêtes de contrôle ou visites planifiées d'avance (voir plus loin) qui sont reprises dans un plan d'action annuel du COC, le COC réserve également une certaine capacité (ou procède à des glissements de cette capacité) pour pouvoir réagir à des évolutions actuelles dont l'importance ne saurait être contestée. Depuis le début du fonctionnement du COC dans sa nouvelle forme en septembre 2018, il a ainsi mené quelques enquêtes/visites qui n'étaient pas planifiées. De telles enquêtes peuvent reposer sur des motifs très divers : communiqués de presse, plaintes, constatations d'office faites dans le cadre d'autres dossiers réactifs, etc. Nous en décrivons ci-après deux exemples (voir aussi www.organedecontrole.be-Publications).

2.7.3.1. Caméras à reconnaissance faciale à BRUNAT

43. Le 10 juillet 2019, l'hebdomadaire Knack a publié une interview avec le Commissaire général de la police fédérale, dans laquelle ce dernier annonçait l'utilisation de la technologie de reconnaissance faciale à l'aéroport de Zaventem. En réaction, le COC a décidé de mener une enquête de contrôle qui incluait notamment une visite sur place en août 2019. L'objectif était de se faire une idée de la technologie utilisée et d'obtenir des informations au sujet du timing prévu, du fondement légal concret, des finalités du traitement, des données à caractère personnel traitées, des mesures prises en matière de sécurité de l'information, de la durée de conservation des données et des banques de données utilisées.

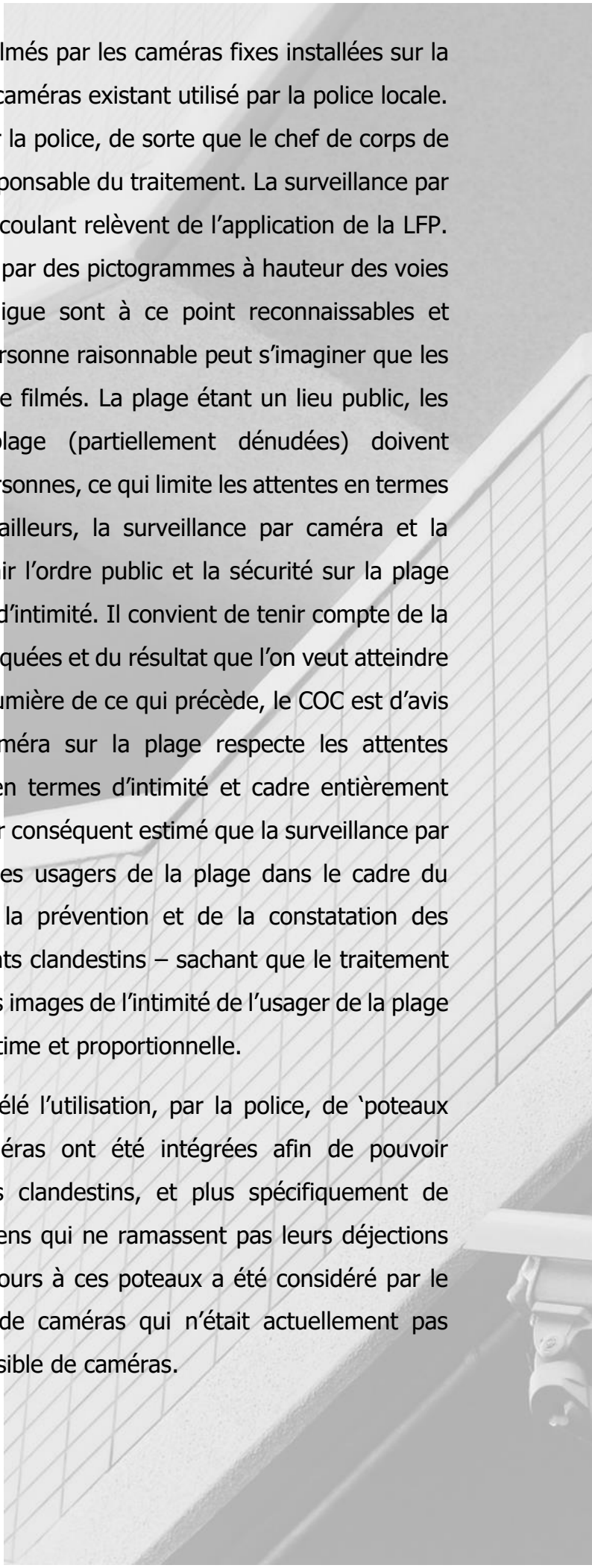
44. Bien que le système ait été présenté comme se trouvant dans une phase de test, il a été constaté lors de la visite qu'il était bel et bien en partie actif. Notamment pour cette raison et après avoir pu établir que le cadre juridique actuel ne permettait pas à la police de procéder à la reconnaissance faciale, le COC a pris en septembre 2019, et en application de l'article 247, 5° de la LPD, une mesure correctrice ordonnant la désactivation temporaire du système. Une version publique du rapport est disponible sur le site Internet du COC.

2.7.3.2. Surveillance par caméra d'une commune de la côte

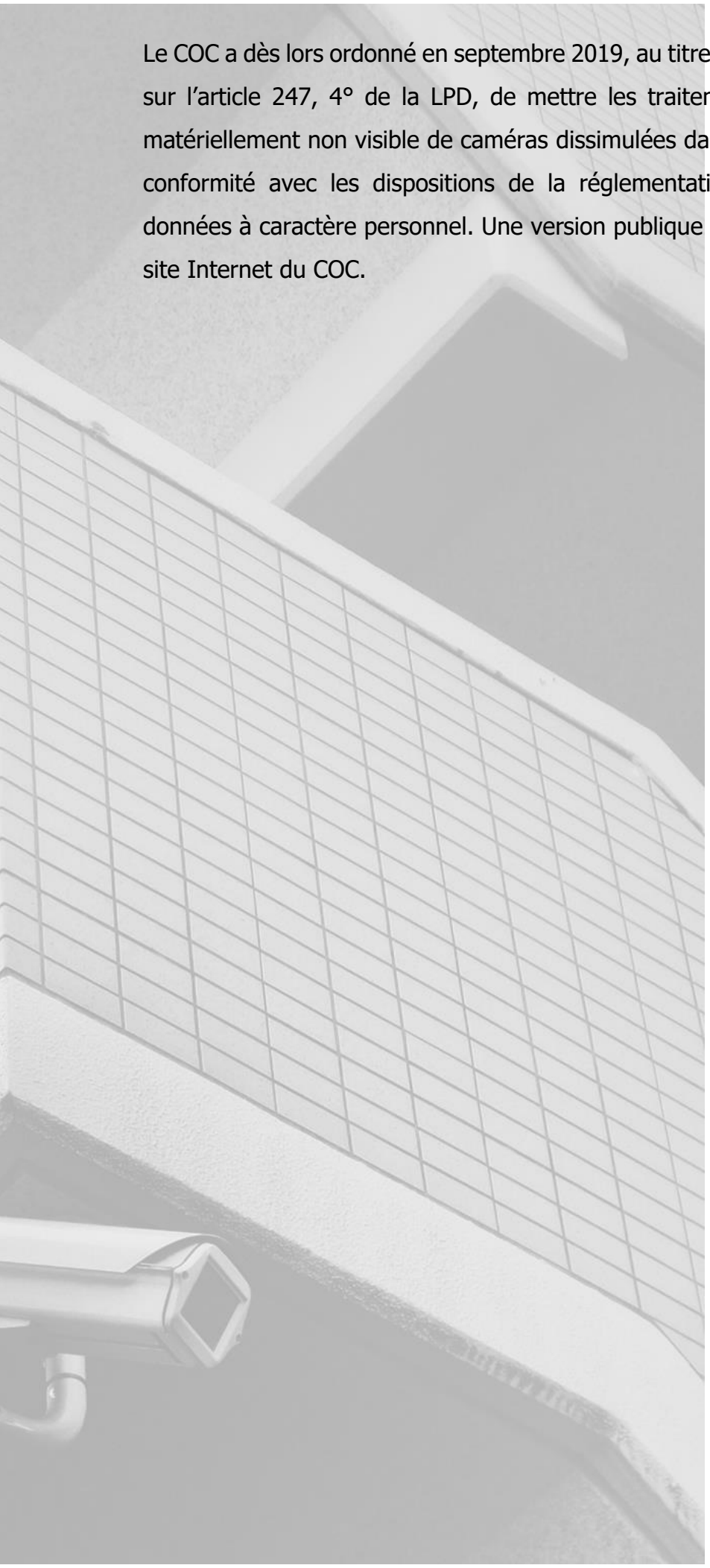
45. Le COC a été saisi d'une plainte concernant le fait que la police locale d'une commune du littoral filme les personnes se trouvant sur la plage. Concrètement, cette utilisation des caméras vise à réprimer les déversements clandestins en général, et en particulier à identifier les propriétaires de chiens qui ne ramassent pas leurs déjections canines. De l'avis du plaignant, l'enregistrement des images constitue une atteinte à l'intimité de certains usagers de la plage. En mai 2019, le DOSE du COC a mené une visite auprès de la zone de police concernée. Les constatations effectuées lors de ce contrôle ont ensuite été analysées à la lumière de la législation et de la réglementation applicables.

46. Les usagers de la plage étaient/sont filmés par les caméras fixes installées sur la digue, lesquelles font partie du réseau de caméras existant utilisé par la police locale. La surveillance par caméra est exercée par la police, de sorte que le chef de corps de la police locale est considéré comme le responsable du traitement. La surveillance par caméra et le traitement de données en découlant relèvent de l'application de la LFP. La surveillance par caméra était annoncée par des pictogrammes à hauteur des voies d'accès. Les caméras installées sur la digue sont à ce point reconnaissables et installées d'une manière telle que toute personne raisonnable peut s'imaginer que les usagers de la plage peuvent eux aussi être filmés. La plage étant un lieu public, les personnes qui se trouvent sur la plage (partiellement dénudées) doivent respecter/accepter la présence d'autres personnes, ce qui limite les attentes en termes d'intimité des usagers de la plage. Par ailleurs, la surveillance par caméra et la présence de la police chargée de maintenir l'ordre public et la sécurité sur la plage limitent également les attentes en termes d'intimité. Il convient de tenir compte de la nature du lieu, des activités qui y sont pratiquées et du résultat que l'on veut atteindre à travers la surveillance par caméra. À la lumière de ce qui précède, le COC est d'avis que cette forme de surveillance par caméra sur la plage respecte les attentes raisonnables des personnes concernées en termes d'intimité et cadre entièrement dans les missions de la police. Le COC a par conséquent estimé que la surveillance par caméra exercée par la police locale sur les usagers de la plage dans le cadre du maintien de l'ordre public ainsi que de la prévention et de la constatation des infractions et délits – dont les déversements clandestins – sachant que le traitement des données est susceptible de générer des images de l'intimité de l'usager de la plage concerné, constitue une mesure licite, légitime et proportionnelle.

47. La visite a cependant également révélé l'utilisation, par la police, de 'poteaux catadioptres' mobiles auxquels des caméras ont été intégrées afin de pouvoir intercepter les auteurs de déversements clandestins, et plus spécifiquement de pouvoir verbaliser les propriétaires de chiens qui ne ramassent pas leurs déjections canines (notamment sur la plage). Le recours à ces poteaux a été considéré par le COC comme une utilisation non visible de caméras qui n'était actuellement pas conforme aux règles sur l'utilisation non visible de caméras.



Le COC a dès lors ordonné en septembre 2019, au titre de mesure correctrice reposant sur l'article 247, 4° de la LPD, de mettre les traitements découlant de l'utilisation matériellement non visible de caméras dissimulées dans des poteaux catadioptres en conformité avec les dispositions de la réglementation régissant le traitement de données à caractère personnel. Une version publique du rapport est disponible sur le site Internet du COC.



2.8. L'exercice de pouvoirs contraignants par le COC

48. Comme nous le disions, le COC dispose contrairement au Comité P ou à l'AIG de pouvoirs de contrainte propres, ce qui signifie qu'il peut forcer les entités de la GPI à poser certains actes/effectuer certains traitements ou à renoncer à certains traitements. Il s'agit des 'compétences correctrices' (art. 247 de la LPD) qui sont aussi désignées sous le terme 'sanctions administratives' – un choix plutôt malheureux – dans la LPD (à l'article 221, §1er).

Le COC est ici investi d'une grande responsabilité, de sorte que chaque exercice de ces pouvoirs s'assortit de la circonspection de mise. Le COC se retrouve ainsi parfois confronté à des choix difficiles. D'une part, il ne peut ignorer les irrégularités constatées ; d'autre part, il tient à perturber le moins possible le fonctionnement de la GPI et veut éviter à tout prix de l'entraver. L'exercice d'équilibre est donc des plus délicats.

Cela signifie que le COC admet pour certaines irrégularités constatées une période de tolérance afin de permettre à la GPI de régulariser la situation. Lorsque l'irrégularité est par contre manifeste, le COC n'a guère d'autre choix que de prendre d'emblée des mesures correctrices, le cas échéant moyennant l'octroi d'un délai pour remédier aux manquements constatés. Voici quelques exemples.

2.8.1. Les mesures correctrices prises

49. Nous avons déjà esquissé plus haut quelques exemples de l'exercice des compétences correctrices. Avant de prendre une mesure correctrice vraiment formelle, le COC prévient l'instance concernée qu'un traitement donné pose problème ou semble illicite. La plupart du temps, les irrégularités sont déjà résolues à ce stade de l'intervention. Dans un certain nombre de cas, le COC ne juge pas opportun de procéder de cette manière plus informelle, et prononce une décision formelle. Ces décisions se déclinent sur toute une gamme pouvant aller d'un avertissement officiel indiquant que le COC est d'avis qu'un traitement est illicite, à la suspension d'un certain flux de données, en passant par une interdiction temporaire ou définitive du traitement.

Les versions publiques des rapports font généralement mention des recommandations et des mesures correctrices, de sorte qu'elles peuvent être consultées par tous les responsables du traitement et par le public.

2.8.2. Les recours judiciaires contre les décisions du COC

50. En 2019, le COC a été impliqué dans le cadre d'un dossier d'accès indirect (voir plus haut) en tant que défendeur dans une procédure devant le Conseil d'état. Le COC est d'avis que le Conseil d'état n'est pas compétent. Le verdict du Conseil d'État est attendu en 2020. Il est en outre crucial de préciser ici que le COC estime qu'il n'existe pas de possibilité de recours contre les décisions prises par le COC dans le cadre de demandes concernant l'accès indirect (qui constituent la majorité des décisions du COC), dans la mesure où le COC exerce dans cette procédure (indirectement) les droits de la personne concernée elle-même. Comme nous le disions, il apparaît cependant que la réponse légalement obligatoire du COC, comme quoi les 'vérifications requises' ont été effectuées, peut engendrer des frustrations et donc potentiellement mener à des procédures judiciaires. Il va de soi qu'une personne concernée a le droit de s'adresser au juge, mais il s'agit alors d'une procédure à l'encontre du responsable du traitement lui-même (la police) et des enregistrements policiers effectués. L'objectif n'est pas d'y impliquer le COC.

La GPI n'a pas intenté depuis septembre 2018 de recours judiciaire contre les mesures correctrices prises.

III. LES ACTIVITES DU COC DANS LE CADRE DE DOSSIERS AXES SUR LA PROTECTION DES DONNEES, LA CONFORMITE, L'EFFICACITE ET L'EFFECTIVITE DE LA GESTION DE L'INFORMATION

3.1. Les visites

3.1.1. Généralités

51. Cette mission relève de l'activité principale du COC depuis sa création en 1998, et encore plus depuis le transfert au pouvoir législatif. Lors de ce transfert en 2014, l'objectif était dès le départ de faire des enquêtes de contrôle (proactives) auprès de la GPI une activité prioritaire. Cette intention n'a pu être réalisée qu'en partie, principalement à cause de la quantité énorme d'avis que le COC a dû rendre au sujet des banques de données particulières déclarées ainsi que de ses activités purement réactives en tant qu'autorité de protection des données. En l'espace de deux ans (entre 2015 et 2017), le COC avait néanmoins mené plusieurs enquêtes de contrôle spontanées importantes. Durant cette *« période antérieure à l'ère de la protection des données »*, l'accent était mis sur les aspects de la licéité, de l'efficacité et de l'efficience de la gestion de l'information. Depuis 2018, la composante cruciale de la protection de la vie privée et des données est venue s'ajouter aux attributions du COC, et force est même de constater que cette composante est devenue de loin la plus substantielle. Selon le COC, il y a 3 grandes explications à ce phénomène, à savoir : (1) l'augmentation exponentielle de l'attention portée à cet aspect depuis l'entrée en vigueur du nouveau cadre européen de protection des données en mai 2018, combinée à une série de nouvelles missions et obligations dont la GPI doit s'acquitter en la matière ; (2) le fait que la GPI a encore un long chemin à parcourir dans ce domaine de sorte que c'est là aussi que se situent les manquements ou points d'amélioration les plus manifestes ; et (3) l'attention accrue pour le thème, tant de la part du grand public que de la presse et du citoyen individuel.

52. Lorsqu'une enquête de contrôle s'assortit d'une ou plusieurs visites sur place détaillées et a une portée très large, on parle d'une 'visite'. En effet, les enquêtes ne comportent pas toutes nécessairement une enquête sur place poussée. Un certain nombre de thèmes sont généralement récurrents dans de telles enquêtes de contrôle d'envergure ou visites. En voici quelques-uns :

(1) contrôle du respect des règles de base de la protection des données (existe-t-il une politique - élaborée par écrit - y a-t-il un délégué à la protection des données, combien de temps peut-il consacrer à ses tâches, quelles initiatives prend-il, dispose-t-on d'un registre des traitements, etc. ?) ;

(2) BNG (qualité de l'alimentation et délais de conservation) ;

(3) application de l'utilisation visible et non visible de caméras ;

(4) banques de données particulières : contenu, sécurisation, liens, etc. ;

(5) utilisation d'équipements IT personnels à des fins opérationnelles ;

(6) traitement de données biométriques à des fins non opérationnelles ;

(7) ICT et sécurité de l'information : politique, architecture, sécurisation, gestion des incidents ;

(8) etc.

Une version publique des rapports des visites est disponible pour consultation sur le site www.organedecontrole.be, sous la rubrique 'Publications-Rapports'.

3.1.2. Quelques visites

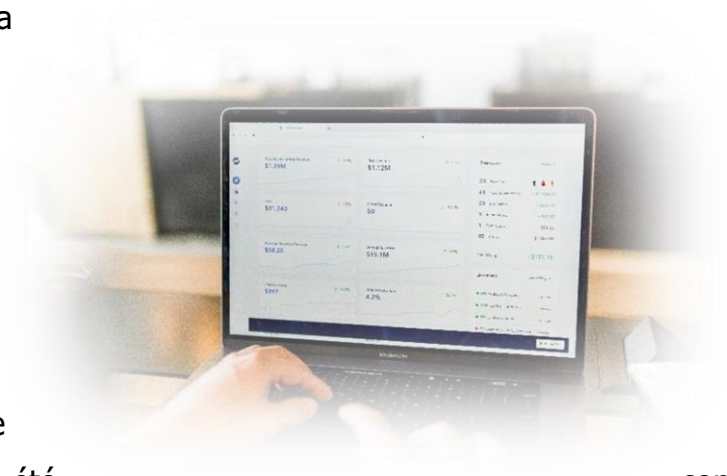
3.1.2.1. ZP Province de Flandre-orientale

53. A la mi-juin 2019, l'Organe de contrôle a mené un contrôle d'envergure auprès d'une zone de police locale de la province de Flandre orientale (ci-après dénommée 'ZP FLO').

Cette visite cadrait dans la mise en œuvre du plan stratégique du COC, qui vise à rendre visite à un certain nombre de zones de police par an en vue d'exercer ses compétences de contrôle et de surveillance. Le contrôle réalisé auprès de la ZP FLO était une visite spontanée et ne faisait donc pas suite à une plainte (individuelle) ni ne découlait de l'existence d'indications (concrètes) de non-respect, par la zone de police contrôlée, de la législation et de la réglementation. Il a été opté pour une visite en largeur. Les conclusions finales et les recommandations et mesures correctrices en découlant n'ayant été formulées qu'en janvier 2020, elles seront brièvement abordées dans le rapport d'activité 2020.[53]

3.1.2.2. ZP Province de Namur

54. A la fin juin 2019, l'Organe de contrôle (COC) a mené une visite d'envergure auprès d'une zone de police locale de la province de Namur. Cette visite ne faisait pas suite elle non plus à une plainte (individuelle) ni ne découlait de l'existence d'indications (concrètes) de non-respect, par la zone de police visitée, de la législation et de la réglementation. Ici aussi, il a été opté pour une visite en largeur. Cela signifie que la visite portait sur plusieurs thèmes sans s'appesantir trop en profondeur sur les différents thèmes. Une attention particulière a été consacrée à l'application du cadre juridique de la protection des données. Étant donné qu'ici aussi, les conclusions finales et les recommandations et mesures correctrices en découlant n'ont été formulées qu'en janvier 2020, elles seront brièvement abordées dans le rapport d'activité 2020.



[53] Le rapport d'activité 2020 doit être transmis au parlement avant le 1er juin 2021 (cf. article 238, 1° de la LPD).

3.1.2.3. L'enquête de contrôle SIS II

55. La réglementation Schengen prévoit que l'autorité de contrôle compétente de chaque état membre effectue tous les 4 ans minimum un contrôle des activités de traitement des données à caractère personnel effectuées sur son territoire dans le cadre du SIS II.[54] Etant donné que la Belgique est un état membre Schengen et que la gestion des signalements Schengen se trouve sous la responsabilité de la GPI belge, il est, depuis l'entrée en vigueur de la LPD, de la compétence du COC (et non plus de l'APD) de procéder aux contrôles de conformité de cette banque de données, ainsi qu'à la vérification de la licéité des traitements effectués dans le cadre du Système d'Information Schengen.[55]

C'est dans ce cadre que l'Organe de contrôle a procédé les 24 et 25 septembre 2019 à une visite de contrôle auprès de la Direction de la Coopération Internationale Policière de la police fédérale (en abrégé 'CGI' Cette visite s'inscrit dans la mise en œuvre du plan stratégique du COC et assure le respect par le COC de ses obligations en matière de législation Schengen. Elle est également à situer dans le contexte de la préparation de l'évaluation 'SCHEVAL' de la Belgique, qui sera réalisée en 2020 sous la direction de la Commission européenne.

Le rapport final n'ayant été délivré qu'en février 2020, il sera abordé plus en détail dans le rapport d'activité de 2020.

[54] Règlement du Parlement européen et du Conseil du 20 décembre 2006 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen de deuxième génération (SIS II), article 44 (ci-après 'Règlement SIS II') et Décision 2007/533/JAI du Conseil du 12 juin 2007 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen de deuxième génération (SIS II), J.O.L. 205, 7 août 2007, article 60 (ci-après 'Décision SIS II').
[55] Décision SIS II, article 60 et Règlement SIS II, article 44.

3.2. Les enquêtes de contrôle

56. Lorsque l'enquête ne s'assortit pas d'une visite sur place d'envergure (c'est-à-dire d'au moins 1 journée entière) ou s'accompagne d'une visite de travail restreinte, le COC parle plutôt d'une 'enquête de contrôle'. Déjà dans les années 2017 et 2018, plusieurs enquêtes de ce type ont été menées. Étant donné qu'à l'époque, le COC n'était pas encore une autorité de protection des données, l'accent était plutôt mis sur la licéité (en général), l'efficacité et l'efficience de la gestion de l'information policière. À partir de septembre 2018, le thème de la protection des données est donc venu s'y ajouter.

3.1.1. Infothèque & FOCUS

57. 'Infothèque' et 'FOCUS' sont deux enquêtes étroitement liées ; la première est antérieure à l'ère de la protection des données, tandis que la deuxième a été initiée alors que le COC était déjà investi de cette mission. L'enquête 'FOCUS' est d'ailleurs loin d'être clôturée, mais est au point mort du fait que le COC n'a pas encore obtenu d'accès à cette application policière/banque de données essentielle cruciale (voir plus loin).

58. Le dossier 'Infothèque', qui a été ouvert dès 2016, était une enquête portant sur une application qui connectait entre elles les banques de données essentielles de dizaines de zones de police locales de manière à permettre de prendre connaissance en temps réel des données contenues dans l'ISLP. Déjà en 2016, le COC avait constaté que cette application initiée par la *ZP Westkust* était illicite, et ce au moins jusqu'à la mi-2019. Même à l'heure actuelle, sa licéité peut donner matière à discussion vu l'absence du cadre indispensable requis pour les interconnexions entre les diverses banques de données policières (voir l'article 44/4, §4 et 5 de la LFP).[56]

[56] *« §4. Les ministres de l'Intérieur et de la Justice, chacun dans le cadre de leurs compétences, déterminent par directive générale et contraignante publiée au Moniteur belge, les modalités relatives à l'interconnexion des banques de données visées à l'article 44/2 entre elles 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. Ces directives déterminent au moins, sur la base du caractère pertinent, adéquat et non excessif, les catégories de banques de données qui peuvent être connectées entre elles, les modalités relatives à l'interconnexion et les règles d'accès des membres des services de police relatives à l'existence d'une information pertinente au sein de ces banques de données interconnectées ou, le cas échéant, aux données elles-mêmes ainsi qu'aux traitements qui en résultent. §5. Les profils et les modalités d'accès visés aux §§ 3 et 4 sont déterminés notamment sur la base : 1° du besoin d'en*

La problématique de l'absence de directives n'a d'ailleurs fait qu'empirer avec les développements, dans le cadre du concept *I-police*, d'applications (notamment l'application 'FOCUS') permettant à un fonctionnaire de police déployé sur le terrain d'accéder immédiatement à partir de sa tablette ou de son smartphone à une multitude d'informations (dont certaines non validées) et de banques de données (dont l'Infothèque). Il ne suffit donc pas dans une législation d'accorder une délégation aux ministres de tutelle, il faut aussi qu'ils l'exercent dans la pratique. Et force est de constater que depuis 2014, c'est souvent là que le bât blesse.

3.1.2. Quelques autres enquêtes de contrôle

59. Une autre enquête digne d'intérêt qui a été menée dès 2016 est celle des 'signalements' (n° 2016/07), qui était une enquête thématique portant sur le respect du suivi des signalements dans la BNG dans le cadre de la circulaire COL 11/2013 ou 'COL INFOFLUX'. Comme la COL 11/2013 impose principalement à la police locale l'obligation d'assurer un suivi des personnes libérées sous conditions, le COC s'est notamment penché sur la manière dont les zones de police tentent de s'acquitter de cette obligation. En résumé, le COC en est arrivé aux constatations suivantes :

(1) Le suivi de ces personnes était/est réglé individuellement à l'échelon de chaque zone de police. La manière dont ce suivi est réglé varie fortement en fonction des circonstances et des moyens disponibles ;

(2) Le retard dont font l'objet les signalements dans la BNG, voire le fait que certaines données ne soient pas enregistrées,[57] ont un certain impact sur la qualité du suivi ;

connaître, en ce compris de la nécessité de croiser ou coordonner les données traitées ; 2° des finalités légales de chaque banque de données 3° des différentes catégories de personnes visées à l'article 44/5 ; 4° de l'évaluation des données ; 5° de l'état de validation des données traitées. Les accès visés aux §§ 3 et 4 doivent être conçus à la base ou par défaut de telle sorte que les données évaluées et validées apparaissent de manière claire et puissent être exploitées prioritairement. Les profils d'accès et l'identification des personnes ayant accès sont tenus à la disposition de l'Organe de contrôle. »

[57] L'Organe de contrôle a par exemple constaté que la peine additionnelle consistant en l'interdiction d'exercer certaines fonctions, professions ou activités (arrêté royal n° 22 du 24.10.1934 relatif à l'interdiction judiciaire faite à certains condamnés et aux faillis d'exercer certaines fonctions, professions ou activités) ne fait plus l'objet d'un signalement dans la BNG, ni donc d'un contrôle. Ce constat pose évidemment un problème sérieux dans le cadre de la lutte contre la criminalité économique, fiscale et financière.

(3) Les zones de police ont, en fonction de leurs moyens, mis au point des instruments pour pouvoir assurer le suivi des mesures ;

(4) Le COC déplore l'absence d'un instrument national, mais aussi le manque de compatibilité des instruments locaux, qui font que les informations ne sont pas généralement disponibles.

60. Dans l'intervalle, force est de constater que les acteurs ont tenu compte du rapport du COC et s'affairent en ce moment activement à déployer une application informatique appelée *I+Belgium* qui permettra d'assurer de manière intégrée le suivi, l'accompagnement et le contrôle des personnes qui font l'objet d'une décision pénale, d'une décision de protection de la jeunesse ou d'une décision d'internement et qui, moyennant le respect de conditions, sont en liberté, ont été remises en liberté ou ont été laissées en liberté. La base juridique à cette fin a d'ailleurs été créée très récemment.[58]

61. Le COC a par ailleurs mené et mène encore de brèves enquêtes portant sur ce que l'on appelle la 'validation centrale' en examinant si les enregistrements dans la BNG étaient corrects et effectués à temps. Depuis septembre 2018 et les nouvelles tâches confiées au COC en tant qu'autorité de protection des données, le COC n'examine cependant plus ces aspects que dans le cadre d'enquêtes de contrôle restreintes ou de visites d'envergure. Le COC ne gère en tout cas plus une application centrale dans ce domaine. Ces aspects ont en effet trait avant tout à la maîtrise de l'organisation interne, et le rôle du COC n'est pas de se substituer à la direction des corps ni au responsable du traitement.

[58] Loi du 5 mai 2019 portant dispositions diverses en matière d'informatisation de la Justice, de modernisation du statut des juges consulaires et relativement à la banque des actes notariés, M.B. 19 juin 2019 et projet d'A.R. pris en exécution de l'article 11, §3 et de l'article 12, §5 de la loi précitée, en préparation et au sujet duquel le COC a été, le 12 octobre 2019, prié par le ministre de la Justice de rendre un avis.

3.3. Les avis concernant les banques de données particulières

62. Entre 2016 et la fin juin 2019, le COC a consacré une partie importante de son temps à rendre les avis prescrits par la loi sur les banques de données particulières que la GPI devait à l'époque encore déclarer à l'Organe de contrôle (voir l'article 44/11/3 de la LFP de l'époque).[59] En l'espace de 3 ans, l'Organe de contrôle a rendu des avis au sujet de quelques 800 banques de données particulières. Ces avis étaient tantôt favorables ou défavorables, tantôt favorables sous conditions. Comme leur nom l'indique, ils demeuraient cependant des 'avis' qui étaient/sont suivis ou non par les services de police concernés. Cette déclaration permettait quoi qu'il en soit au COC de disposer d'un aperçu très fiable du paysage policier des banques de données particulières, ce qui est malheureusement moins évident aujourd'hui.

[59] Cet article a en effet été modifié dans l'intervalle par la loi du 22 mai 2019 modifiant diverses dispositions en ce qui concerne la gestion de l'information policière, M.B. 19 juin 2019, 61992 (entrée en vigueur le 29 juin 2019).

3.4. Le contrôle des banques de données communes terrorisme et extrémisme

CONTROLE EN 2017

63. Dans le sillage des attentats perpétrés à Bruxelles, la loi du 27 avril 2016 relative à des mesures complémentaires en matière de lutte contre le terrorisme[60] a modifié la loi sur la fonction de police (LFP) élaborant ainsi une base légale pour la création des banques de données communes (en abrégé 'BDC'). L'article 44/6 de la LFP confie le contrôle du traitement des informations et des données à caractère personnel enregistrées dans la BDC au COC et au Comité permanent R agissant conjointement. Les deux instances doivent en outre, préalablement à la création d'une BDC, rendre un avis conjointement sur la base d'une 'déclaration préalable' introduite par les responsables du traitement (les Ministres de l'Intérieur et de la Justice). Les deux institutions ont conclu en décembre 2017 un protocole d'accord en vue d'un exercice coordonné de ces 2 compétences.

Dans le cadre de leur mission de contrôle conjointe, le COC et le Comité permanent R ont décidé d'examiner en 2017 les éléments suivants :

(1) le contenu de la fiche de renseignements et de la carte d'information de chaque FTF sur la base de paramètres légaux et réglementaires ;

(2) le contrôle des actions de l'OCAM en ce qui concerne la validation initiale en tant que FTF et les traitements ultérieurs ;

(3) le contrôle des consultations des fiches de renseignements et des cartes d'information par les services de base et les services partenaires ;

(4) le contrôle de la manière dont les bourgmestres sont informés de la carte d'information (il peut s'agir de plusieurs bourgmestres par entité) ;

[60] M.B. 9 mai 2016.

(5) l'identification des utilisateurs de la BDC FTF, le nombre d'accès directs/consultations directes, l'exercice (ou non) d'un contrôle de la licéité des accès directs/consultations directes, l'existence (ou non) d'un système de validation et l'existence d'éventuels incidents de sécurité ;

(6) l'existence d'une actualisation du mode d'emploi de la banque de données ;

(7) un examen des traitements des 2 journées sélectionnées ;

(8) la désignation d'un consultant en matière de sécurité et de protection de la vie privée.

Les recommandations nécessaires ont été formulées concernant les points qui précèdent, tant à l'OCAM qu'aux ministres responsables et aux autres services de base et partenaires.

Dans le cadre de leur enquête portant sur la BDC FTF, le COC et le Comité permanent R ont constaté le traitement d'entités qui étaient reprises dans la *Joint Information Box* (*JIB*), à savoir la liste (gérée par l'OCAM) des personnes et organisations jouant un rôle clé dans le processus de radicalisation. Un nouveau traitement a en outre été introduit sous le dénominateur *home-grown terrorist fighters* (*HTF*). Ce traitement vise le recensement des personnes animées de motivations terroristes qui, contrairement aux *foreign terrorist fighters*, n'ont pas l'intention (ni dans le passé ni à l'avenir) de se rendre dans une zone de conflit djihadiste. Ces nouveaux traitements ont été introduits à la demande expresse des Ministres de la Justice et de l'Intérieur. Sans vouloir remettre en doute l'opportunité ni l'utilité opérationnelle de tels traitements additionnels, le COC et le Comité permanent R ont attiré l'attention sur le fait que ces traitements avaient été instaurés sans arrêté royal et sans avis préalable du Comité permanent R ni du COC. Le COC et le Comité permanent R ont interpellé les Ministres de la Justice et de l'Intérieur à ce sujet.

CONTROLE EN 2018

En 2018,[61] cette BDC a été transformée : elle s'appelle désormais banque de données commune *terrorist fighters* (BDC TF) et inclut également, en marge de la catégorie générale (existante) des *foreign terrorist fighters*, une nouvelle catégorie constituée de *homegrown terrorist fighters*. Il a par ailleurs été créé en 2018[62] une BDC distincte pour les 'propagandistes de haine' (la BDC PH).

Le COC et le Comité permanent R ont en 2018 procédé à un contrôle conjoint de la mise en œuvre de certaines recommandations qu'ils avaient formulées en 2017 (voir plus haut). Il a en outre été décidé de soumettre à un contrôle la manière dont l'information était transmise aux bourgmestres et aux tiers respectivement par les chefs de corps de la police locale et les services de base. Les recommandations nécessaires ont été formulées concernant les points qui précèdent, tant à l'OCAM qu'aux ministres responsables et aux autres services partenaires.

CONTROLE EN 2019

L'*arrêté royal du 20 décembre 2019 modifiant l'arrêté royal du 21 juillet 2016 relatif à la banque de données commune Terrorist Fighters et l'arrêté royal du 23 avril 2018 relatif à la banque de données commune Propagandistes de haine et portant exécution de certaines dispositions de la section 1re bis « De la gestion des informations » du chapitre IV de la loi sur la fonction de police* a apporté d'autres modifications à la BDC TF. Outre un certain nombre de modifications techniques, il crée notamment 2 nouvelles catégories de personnes dans la BDC TF, à savoir les *« Extrémistes Potentiellement Violents »* et les *« Personnes condamnées pour terrorisme ».*

[61] A.R. du 23 avril 2018 modifiant l'arrêté royal du 21 juillet 2016 et modifiant la banque de données commune *Foreign Terrorist Fighters* vers la banque de données commune *Terrorist Fighters*, M.B. 30 mai 2018 (A.R. TF).
[62] A.R. du 23 avril 2018 relatif à la banque de données commune Propagandistes de haine et portant exécution de certaines dispositions de la section 1re bis *« De la gestion des informations »* du chapitre IV de la loi sur la fonction de police (A.R. HP).

Pour l'année 2019, le COC et le Comité permanent R ont décidé d'axer le contrôle conjoint d'une part, sur le suivi de certaines recommandations qui avaient été formulées dans les rapports des années précédentes et d'autre part, sur la consultation d'un certain nombre de services (de base et partenaires) concernant les contrôles de licéité et les procédures internes visant un déroulement fluide du traitement des informations contenues dans la BDC TF. Il a en outre également été procédé à une analyse plus détaillée de la coordination du traitement des informations contenues dans la BDC TF, en prêtant notamment attention au rôle du DPO de la BDC TF qui avait été désigné peu de temps auparavant. Le nombre croissant de services qui ont accès à la BDC TF a dans ce contexte été pris en compte également.

Le COC et le Comité permanent R ont vérifié les recommandations suivantes qui avaient été formulées dans le sillage de contrôles conjoints antérieurs :

(1) la désignation d'un délégué à la protection des données ;

(2) la mise en œuvre d'un mécanisme pour la notification des incidents de sécurité ;

(3) la mise en œuvre de développements informatiques complémentaires ;

(4) un contrôle spontané des *fichiers de journalisation* (pour un nombre restreint de services) ;

(5) l'exception à l'obligation d'enregistrer des informations policières dans la BDC TF en vertu d'un embargo imposé par un magistrat compétent.

Au moment de la rédaction du présent rapport annuel, ce rapport n'est pas encore définitif. Il sera donc abordé dans le rapport annuel 2020.

3.5. Les demandes d'information et d'avis concernant la gestion de l'information policière

64. Le COC reçoit également de la part des services contrôlés des questions et demandes qui sont sans rapport avec le thème de la protection des données, voire qui ne présentent aucun lien avec la gestion de l'information policière opérationnelle. C'est d'ailleurs logique vu que le COC est également compétent pour les matières relevant du RGPD. Voici quelques exemples à titre d'illustration :

(1) le COC a rendu le 6 juin 2018 un avis en vertu de l'article 44/11, §2 de la LFP en réponse à une question du directeur général de la Direction générale de la gestion des ressources et de l'information de la police fédérale portant sur la licéité de la désignation d'un membre du personnel CALOG en tant que directeur général de la DGR ;

(2) un avis a été rendu concernant la compétence du personnel CALOG à l'égard des traitements dans les banques de données policières, à commencer par la consultation de la BNG ;

(3) un point de vue a été adopté sur la question de l'accès des SICAD de la police fédérale (dans la pratique, les carrefours d'information d'arrondissement ou CIA) à la banque de données essentielle ISLP de la police locale.

Une dizaine d'avis ont ainsi été rendus, à la demande soit des services de police, soit d'un citoyen ou d'une autre autorité.

IV. LES ACTIVITES POLITIQUES DU COC

4.1. Les forums de concertation nationaux

65. Le COC prend part à nombre de forums de concertation nationaux, meetings, réunions, etc., soit de manière ponctuelle, soit sur une base structurelle. Il s'agit d'une concertation qui peut être informelle ou formelle, avec par exemple des ministres en charge de la police et leurs cabinets, les administrations concernées, les autres autorités administratives ou judiciaires, etc. concernant les initiatives projetées, ou encore de rencontres stratégiques et opérationnelles avec d'autres autorités de protection des données ou instances de contrôle, d'une concertation avec les corps de police, leurs chefs de corps ou DPO, etc. Concrètement, des concertations ont par exemple eu lieu avec :

(1) la *Vlaamse Vereniging voor Steden en Gemeenten (VVSG)*, l'Union des villes et communes de Flandre : à la demande de la VVSG, le COC prend part au groupe de travail *'Gegevensuitwisseling politie-lokale besturen'* qui se consacre à l'échange de données entre la police et les administrations locales ;

(2) l'Office des étrangers, concernant le traitement des demandes 'Article 24 du Règlement SIS II' (les *'entry bans'*) ;

(3) la police fédérale, tant avec le commissaire général qu'avec un certain nombre de ses services, dont la DRI[63] et le CG/ISPO[64] ;

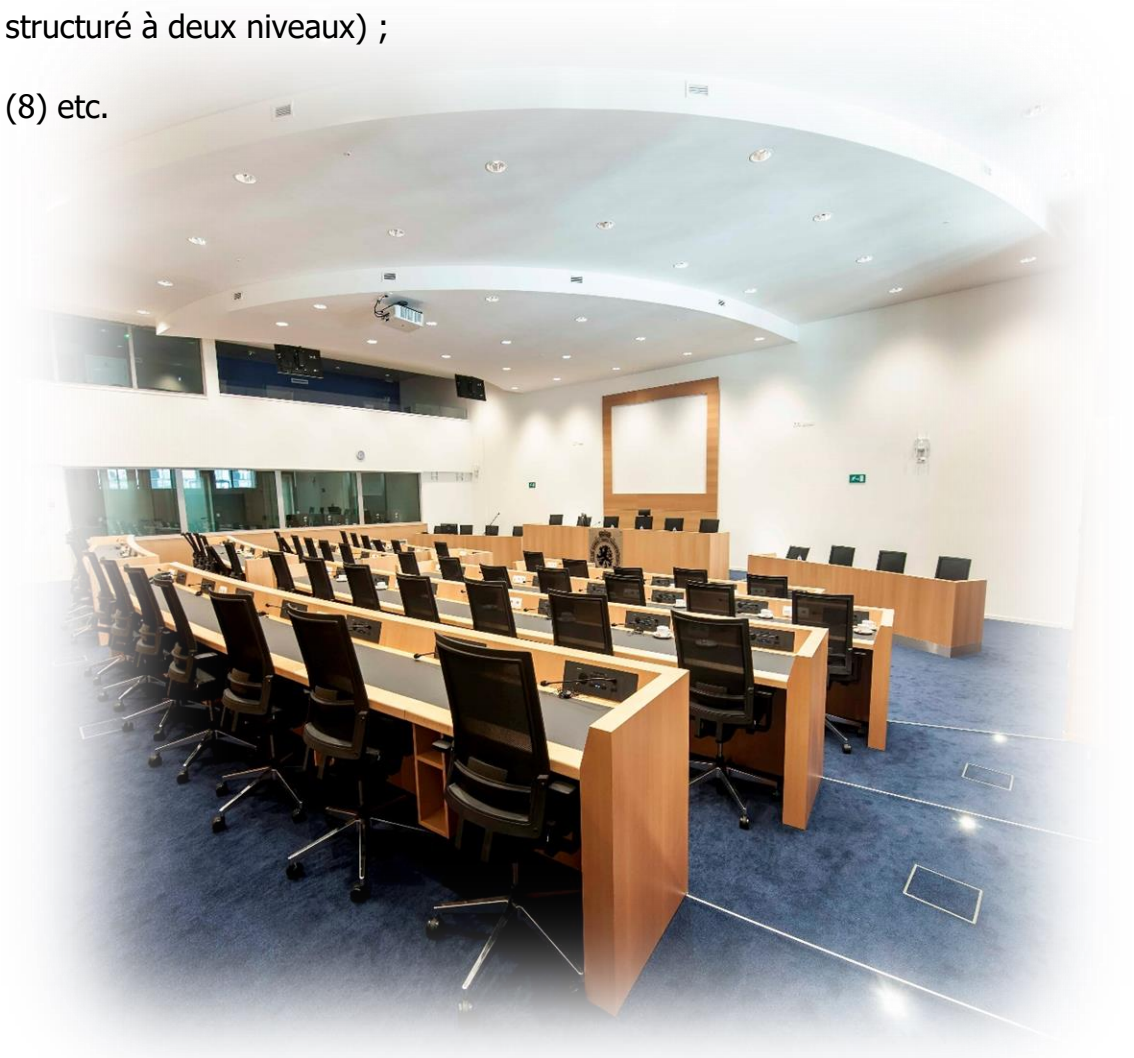
(4) l'APD, le Comité R et/ou le Comité P, concernant diverses matières communes ;

(5) la Ligue des Droits Humains, à la demande de cette dernière, concernant l'organisation et la politique du COC ;

(6) UNIA, à la demande de cette dernière, concernant l'organisation et la politique du COC ;

(7) le nouveau « Comité Information et ICT », à l'occasion d'une réunion de lancement (cf. art. 8*sexies* de la loi organisant un service de police intégré, structuré à deux niveaux) ;

(8) etc.



[63] La DRI est la *« Direction de l'information policière et des moyens ICT »*, qui fait partie de la *« Direction générale de la gestion des ressources et de l'information »* (DGR).
[64] Il s'agit de l'acronyme désignant le « Commissariat général/*Information Security & Privacy Office* ».

4.2. Les forums de concertation internationaux

66. En sa qualité d'autorité de protection des données compétente, le COC représente la Belgique au sein de quelques forums de concertation internationaux. Il s'agit par exemple : de l'*Europol Cooperation Board* ; du *SIS II Supervision Coordination Group* ; et du *BTLE* (*Borders, Transport and Law Enforcement*), un sous-groupe de travail de l'*European Data Protection Board* (le 'Comité européen de la protection des données' qui réunit les 27 autorités de protection des données des états membres et l'EDPS).[65] En fonction de la matière à traiter, le COC prend part à ces forums seul ou conjointement avec l'APD. Un suivi correct des thèmes traités au sein de ces assemblées monopolise une capacité considérable. Le COC tente dans la mesure du possible d'y apporter activement son concours.

Le COC s'efforce en effet d'investir du temps dans ces assemblées car elles traitent de nombreux thèmes internationaux cruciaux, qui peuvent parfois avoir des répercussions et revêtir de l'importance au niveau national, comme l'*EU-US privacy shield*, la problématique de la rétention des données, l'obtention de preuves électroniques (*'e-evidence'*) au-delà des frontières, etc.

En 2019, le COC a ainsi assisté à 10 réunions, précédées de la préparation requise et accompagnées d'un suivi courant et permanent (approbation de comptes rendus, contributions aux positions communes, échange d'arguments, etc.).

[65] L'*European Data Protection Supervisor*, l'EU-DPA, https://edps.europa.eu.

4.3. Communication externe et participation à des évènements

4.3.1. Contacts avec la presse

67. En 2019, le COC s'est mis à entretenir ou à avoir des contacts réactifs avec la presse. Un membre-conseiller a été chargé de la fonction de porte-parole de la presse tant du côté francophone que du côté néerlandophone. La désignation d'un porte-parole de la presse est non seulement une composante logique de toute organisation à vocation sociétale mais aussi la mise en œuvre du devoir d'information prévu à l'article 240, 1° de la LPD qui impose au COC l'obligation de *« favorise*(r) *la sensibilisation du public et sa compréhension des risques, des règles, des garanties et des droits relatifs au traitement des données à caractère personnel … »*.

Les articles au sujet de l'arrêt de l'utilisation du système de reconnaissance faciale à l'aéroport de Bruxelles-National (par exemple dans les quotidiens flamands *De Standaard,*[66] *Het Laatste Nieuws,*[67] etc.), du contrôle exercé par le COC sur les banques de données particulières (par exemple dans le quotidien 'L'Avenir'[68]) ou de la problématique des consultations illicites de la part de fonctionnaires de police (par exemple dans le quotidien 'L'Avenir'[69]) ne sont que quelques exemples des communications du COC à l'intention de la presse. Le COC constate par ailleurs que sa notoriété et sa reconnaissance auprès de la presse se renforcent et qu'il reçoit de plus en plus d'appels de journalistes. On peut s'attendre à ce que cette tendance ne fasse que s'accentuer en 2020.

---

[66] Voir https://www.standaard.be/cnt/dmf20190920_04618911.
[67] Voir https://www.hln.be/nieuws/binnenland/federale-politie-moet-gezichtsherkenning-op-zaventem-stopzetten-project-is-in-strijd-met-wet~aeaa5daa.
[68] Voir https://www.lavenir.net/cnt/dmf20180918_01228062/le-gardien-des-800-banques-de-donnees.
[69] Voir https://www.lavenir.net/cnt/dmf20181128_01263466/ces-policiers-qui-vous-epient-illegalement.

Cet aspect implique également une charge de travail non négligeable pour le membre concerné puisque la presse est active 24 heures sur 24 et 7 jours sur 7. Néanmoins, la désignation d'un porte-parole de la presse distinct n'est de toute façon pas une option réaliste pour le COC à l'heure actuelle, ni à temps plein ni même à temps partiel.

L'objectif est aussi de mener dans la mesure du possible à partir de 2020, une communication proactive, par exemple en diffusant des communiqués de presse sur des thèmes intéressants ou actuels.

4.3.2. Participation à des journées d'étude et formations

68. Les membres et le personnel du COC font principalement l'objet de sollicitations réactives en vue de prendre part à toutes sortes de formations, journées d'étude ou colloques organisés par des tiers. Le COC tente d'accéder le plus souvent possible à ces demandes, et ce pour diverses raisons. De telles participations sont en effet l'occasion de tâter le terrain pour savoir ce qui s'y fait et s'y dit, de comprendre les questions et problèmes qui se posent et surtout de diffuser à l'échelle la plus large possible, la vision et les points de vue du COC, de manière à ce que les instances contrôlées – et avant tout la GPI – se profilent et opèrent de plus en plus de manière conforme. La mission de sensibilisation du COC exige en effet le déploiement aussi intensif que possible, d'efforts en ce sens. Par ailleurs, le COC est également investi en vertu de l'article 240, 2° de la LPD de l'obligation d'*« encourage(r) la sensibilisation des responsables du traitement et des sous-traitants aux obligations légales à l'égard des traitements de données à caractère personnel. »*

Pour illustrer ce propos par quelques exemples, le COC a notamment apporté son concours aux formations suivantes :

(1) ANPA (Académie Nationale de Police), formation des aspirants commissaires de police (sessions pour les francophones et sessions pour les néerlandophones) ;

(2) Formation spécifique organisée pour tous les DPO de la GPI par le service CG/ISPO de la police fédérale (sessions pour les francophones et sessions pour les néerlandophones) ;

(3) Formation interne à l'intention du personnel de l'Autorité de protection des données (session consacrée à l'application du titre II de la LPD) ;

(4) Concertation sur le thème de la sécurité de l'information organisée par la *ZP Kouter* et réunissant les zones de police suivantes de Flandre occidentale : *ZP Oostende, ZP Brugge, ZP Spoorkin, ZP Kouter, ZP De Haan/Bredene et ZP Middelkerke* ;

(5) Formation dispensée à tous les membres du personnel de la ZP Condroz-Famenne (2 jours) ;

(6) Rencontre/entretien sur demande avec les candidats commissaires principaux dans le cadre des épreuves organisées en vue de l'obtention du brevet de direction (thème : les accords de coopération regroupant plusieurs agences, comme l'ARIEC, les *Family Justice Centers*, le Carrefour d'Information Maritime, etc.) ;

(7) Présentation à l'occasion du 'salon du RGPD' ;

(8) Etc.

69. Le DIRCOM envoie par ailleurs aussi lui-même ses membres et son personnel à des formations pertinentes. La matière que traite le COC est complexe, constituée de composantes nationales et internationales, régie par une réglementation qui comporte de nombreuses 'zones grises' et évolue rapidement (ne serait-ce que du fait de l'évolution fulgurante de l'ICT). Rester au fait de toutes les nouveautés tient donc à la fois de la nécessité et du défi. Quelques exemples :

(1) Formation auprès de la DRI de la police fédérale, portant sur l'infrastructure de l'ICT de la GPI ;

(2) Participation à la séance d'information 'Protection des données à caractère personnel au moyen de la cryptographie avancée' - SMALS ;

(3) Conférence du Professeur B. Preneel (KU Leuven) sur le thème de la cryptographie, au siège de l'Autorité de protection des données ;

(4) Formation de maintenance et webmaster pour le nouveau site Internet du COC ;

(5) Participation de juristes du COC aux *Case Handling Workshops* organisés en 2019 par l'EDPS. Ces ateliers visent l'échange, entre les différentes autorités nationales de protection des données et avec l'autorité de protection des données de l'UE, d'expériences et de bonnes pratiques dans le domaine des inspections, des audits, des contrôles et des visites ;

(6) Diverses formations organisées par l'ERA (*Europäische Rechtsakademie*, Trèves) ayant notamment pour thèmes Europol, *Freedom & Security*, *Privacy & Dataprotection ECtHr and CJEU case-law*, etc. ;

(7) Formation Themis *capita selecta* de la KU Leuven sur le droit pénal et la procédure pénale ;

(8) Formation *blockchain* de l'Institut de formation judiciaire ;

(9) Congrès *European Society of Criminology*, Université de Gand ;

(10) Présentation de *papers* sur différents thèmes ayant trait à la police dans le cadre de l'obtention du brevet de direction de commissaire principal ;

(11) Journées d'étude et colloques organisés par le *Centre for Policing and Security* ;

(12) Etc.

4.3.3. Site Internet

70. Le lancement d'un site Internet n'a pas été une mince affaire dès lors que le COC lui-même ne dispose en la matière que de très peu d'expertise propre, voire aucune. Les membres et le personnel se sont donc dans une large mesure acquittés eux-mêmes du travail avec le support restreint d'un prestataire de services externe. Le second semestre de 2019 y a été consacré et s'est finalement soldé par le lancement en ligne à la fin 2019. Le site est accessible à l'adresse URL www.organedecontrole.be ou www.controleorgaan.be, et le rôle de webmaster est endossé par la (seule) secrétaire de direction, qui suit régulièrement des formations à cette fin.

4.3.4. Consultations du COC par des externes

71. Le COC est régulièrement consulté par des parties externes, par exemple par des étudiants qui veulent faire leur stage auprès du COC, pour des interviews dans le cadre de travaux de fin d'études de bacheliers ou de masters ou encore de *papers*, ou pour des interviews dans le cadre d'enquêtes menées par la Commission européenne (par exemple au sujet de la mise en œuvre de la directive API). Ces parties externes peuvent aussi être des fonctionnaires de police dans le cadre de cycles de politique ou de brevets divers, ou d'autres acteurs intéressés. Un autre exemple sont les visites de délégations étrangères. Le COC a ainsi reçu une délégation japonaise, composée d'un procureur et du premier secrétaire de la Mission du Japon auprès de l'Union européenne, qui souhaitait obtenir davantage d'explications sur le rôle d'une autorité de protection des données policières.

V. PARTENARIATS ET COMPETENCES PARTAGEES

72. Le législateur fédéral a prévu dans la LCA et la LPD quatre autorités fédérales de protection des données ayant chacune leurs propres compétences : l'Autorité de protection des données, l'Organe de contrôle de l'information policière, le Comité permanent R et le Comité permanent P.

L'article 54/1 de la LCA prévoit en outre en son paragraphe premier que ces autorités doivent collaborer ensemble, entre autres en ce qui concerne le traitement des plaintes, les avis et les recommandations qui affectent les compétences de deux ou plusieurs autorités de contrôle. Le traitement conjoint des plaintes, des avis et des recommandations se fait sur la base du principe du guichet unique qui doit être assumé par l'APD. Le deuxième paragraphe stipule ensuite qu'*« afin de réaliser la coopération visée au premier paragraphe, les autorités de contrôle concluent un protocole de coopération. »*

L'APD, le COC et les deux Comités permanents souhaitent mettre en œuvre le 2e paragraphe susmentionné en établissant un protocole de coopération.

Un texte de base a été rédigé à la fin 2019 par le COC et l'APD, et les négociations se poursuivent en 2020.

73. Le COC a en outre eu par exemple une collaboration ponctuelle avec le Comité P dans le dossier du 'screening de festivaliers' dans le cadre duquel le COC a apporté son concours à l'enquête du Comité P. Le réalisme nous force à reconnaître que la capacité du COC ne lui permet pas de procéder fréquemment de la sorte vu qu'il est déjà submergé par ses propres tâches.

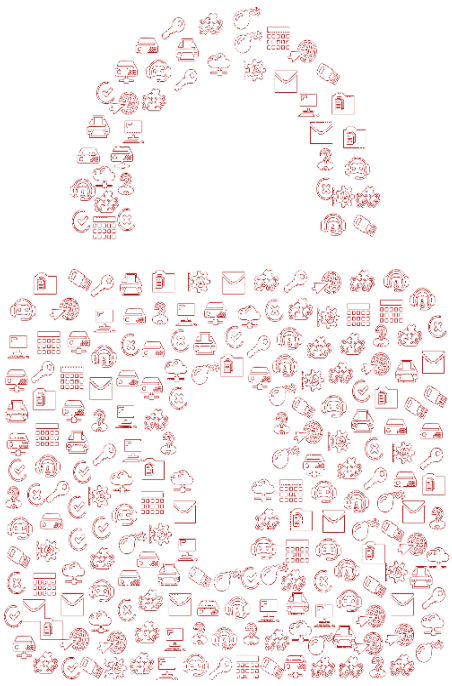
En ce qui concerne les plaintes, il a été convenu ce qui suit : sauf s'il est manifeste que le COC ou le Comité P est investi d'une compétence exclusive, chaque institution traite les plaintes qui lui sont adressées (voir plus haut). Le Comité P continue cependant de communiquer au COC et de mettre à sa disposition, les plaintes contre des policiers concernant des consultations illégitime ou des traitement illégitimes dans des banques de données policières.

74. Avec le Comité permanent R sont organisés des contrôles annuels conjoints portant sur les banques de données communes terrorisme et extrémisme tandis qu'une collaboration est envisagée dans le cadre de la fonction de contrôle de la protection des données auprès de la BELPIU. Les premiers contacts à cette fin ont été établis en 2019, avec une première visite conjointe qui a permis de faire connaissance et une visite restreinte rendue à l'Unité d'information des passagers.

75. Le COC tente aussi de collaborer avec d'autres organes et/ou institutions si tous les partenaires participants y trouvent des avantages. Le COC a ainsi passé en 2019 des conventions avec l'Office des étrangers au sujet du traitement des demandes 'Article 24 du Règlement SIS II' (dossiers *'entry ban'*) qui sont introduites pour la grande majorité des ressortissants albanais. Cette collaboration a permis de remarquer que de telles demandes étaient souvent soumises simultanément aux deux institutions (et même à d'autres autorités de protection des données des états membres de l'UE), donnant donc lieu à une double enquête. Des conventions de travail concrètes ont été passées à ce sujet afin de permettre une rationalisation.

VI. CONCLUSION ET PERSPECTIVES FUTURES

76. Une **première conclusion** consiste à dire que le COC, à travers sa relance du 5 septembre 2018, a dans la pratique pris un tout nouveau départ et est parvenu en dépit de son envergure restreinte à se faire rapidement une place dans le paysage de la protection des données et de la police. Il a, surtout au début, dû faire l'impasse sur certains aspects par manque de capacité, mais il est peu à peu parvenu à déployer ses activités dans nombre de ses domaines. Un autre constat frappant réside dans le fait que le volet de la protection des données constitue à l'heure actuelle plus de 75 % au moins de ses activités.



77. Une **deuxième conclusion** est que le COC jouit déjà d'une grande confiance de la part des autres acteurs, qu'il s'agisse des citoyens/personnes concernées ou des responsables du traitement. Le nombre et le type de dossiers auxquels il a été fait allusion au fil du présent rapport d'activité le prouvent. Cette confiance existe aussi auprès des autorités de police – et des services de police – comme en témoignent les dizaines de demandes d'avis qui sont adressées au COC et qui portent souvent – mais certainement pas exclusivement – sur des aspects relatifs à la protection des données.

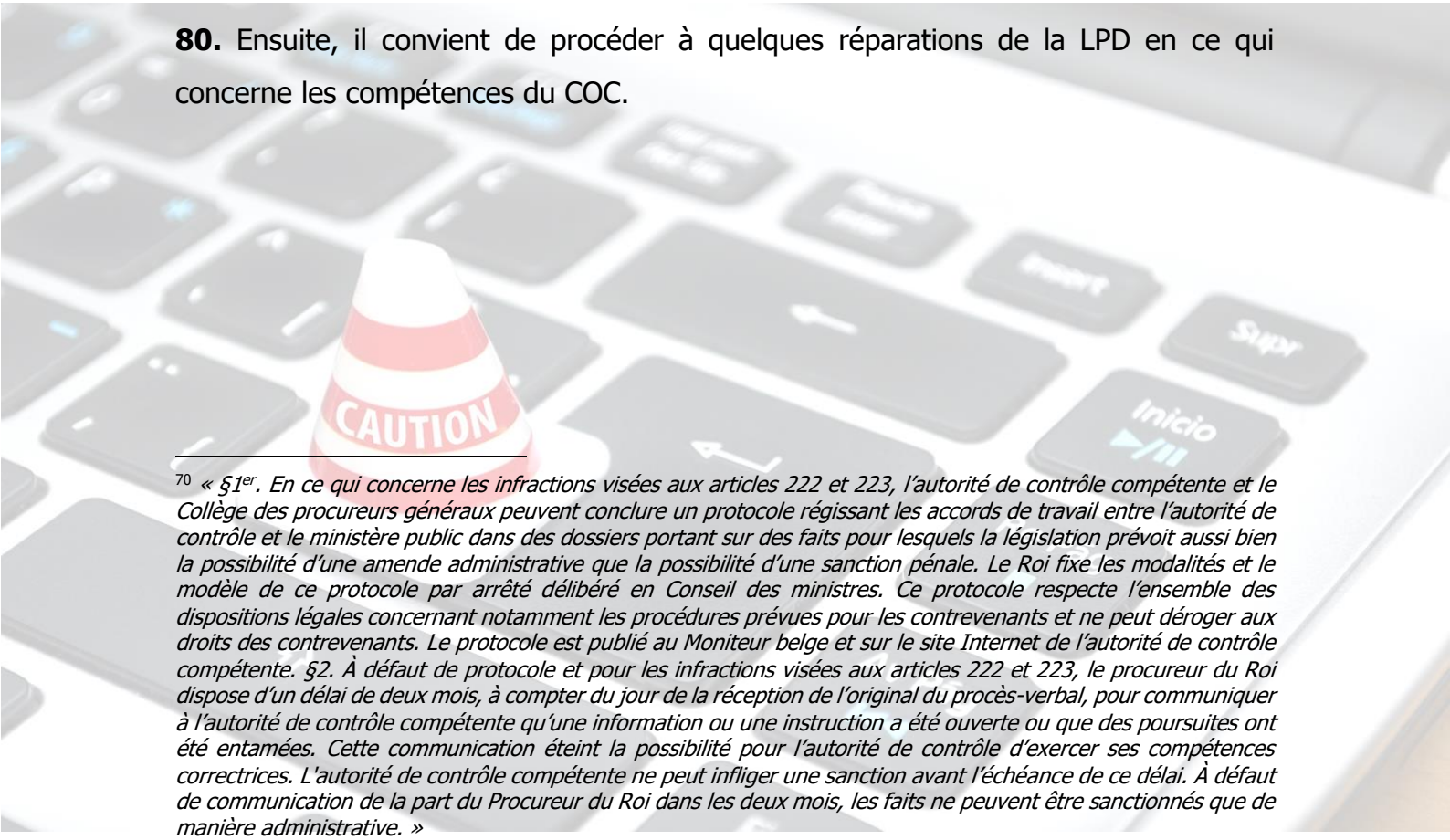
Une **troisième conclusion** réside dans le constat que le COC n'hésite pas à exercer ses compétences correctrices – et donc ses pouvoirs de contrainte – et tente de pallier ainsi au vide classique qui affecte le droit à la protection de la vie privée et des données, à savoir l'absence de véritable mécanisme de *law enforcement* ou de maintien. Le COC tente d'y remédier dans sa matière en exerçant au besoin et de manière proportionnelle ses pouvoirs de contrainte (qui, pour toute clarté, ne permettent pas à l'heure actuelle d'infliger une amende administrative).

De manière proportionnelle, le COC ne veut évidemment pas rendre le travail de la police impossible à travers un exercice aveugle ou trop peu nuancé de ses compétences correctrices. À cet égard, il s'agit souvent d'un exercice d'équilibre délicat.

78. Pour ce qui est de l'avenir, le COC a encore un travail important à accomplir. La conclusion de protocoles d'accord constitue l'une des priorités absolues pour 2020. L'article 229 de la LPD prévoit en outre la possibilité pour le COC de conclure un protocole d'accord pour mettre en place le maintien le plus adéquat, et donc de créer une sorte de régime *« una via ».*[70] Vu les déficiences du maintien pénal de cette matière, il s'agit là pour le COC d'une piste à explorer.

79. Le COC nourrit également l'ambition d'initier encore plus d'enquêtes d'office et proactives sur le terrain, mais est à cet égard limité par la capacité dont il dispose. Les premières expériences révèlent qu'une visite globale d'une police locale, par exemple, monopolise énormément de capacité, en particulier si elle revêt une certaine envergure. Il est clair que le COC ne pourrait pas réaliser 10 de ces enquêtes par an.

80. Ensuite, il convient de procéder à quelques réparations de la LPD en ce qui concerne les compétences du COC.



[70] *« §1er. En ce qui concerne les infractions visées aux articles 222 et 223, l'autorité de contrôle compétente et le Collège des procureurs généraux peuvent conclure un protocole régissant les accords de travail entre l'autorité de contrôle et le ministère public dans des dossiers portant sur des faits pour lesquels la législation prévoit aussi bien la possibilité d'une amende administrative que la possibilité d'une sanction pénale. Le Roi fixe les modalités et le modèle de ce protocole par arrêté délibéré en Conseil des ministres. Ce protocole respecte l'ensemble des dispositions légales concernant notamment les procédures prévues pour les contrevenants et ne peut déroger aux droits des contrevenants. Le protocole est publié au Moniteur belge et sur le site Internet de l'autorité de contrôle compétente. §2. À défaut de protocole et pour les infractions visées aux articles 222 et 223, le procureur du Roi dispose d'un délai de deux mois, à compter du jour de la réception de l'original du procès-verbal, pour communiquer à l'autorité de contrôle compétente qu'une information ou une instruction a été ouverte ou que des poursuites ont été entamées. Cette communication éteint la possibilité pour l'autorité de contrôle d'exercer ses compétences correctrices. L'autorité de contrôle compétente ne peut infliger une sanction avant l'échéance de ce délai. À défaut de communication de la part du Procureur du Roi dans les deux mois, les faits ne peuvent être sanctionnés que de manière administrative. »*

La LPD a été adoptée très rapidement par le Parlement et présente quelques manquements. Le COC formule à cet égard les suggestions suivantes.

(a) <u>Les autorités compétentes :</u> En ce qui concerne les services relevant du COC, quelques imperfections pourraient être éliminées, à savoir :

(a.1) en rendant le COC compétent pour les Douanes dans leur ensemble sans plus opérer de ventilation entre l'APD et le COC ; le COC s'est récemment vu confier une nouvelle compétence d'évaluation à l'égard des réquisitions adressées par les Douanes à la BELPIU.[71] Autrement dit, le COC doit de toute façon se forger de l'expertise dans ce domaine (d'autant qu'il s'agit des compétences fiscales des Douanes). Il serait plus cohérent de ne prévoir qu'une seule autorité de protection des données pour les Douanes également ;

(a.2) on pourrait aussi remettre en question le fait que la Cellule de Traitement des Informations Financières (CTIF) ait l'APD comme autorité de protection des données ; la CTIF a en effet dans une large mesure une fonction répressive, une matière avec laquelle le COC est bien mieux familiarisé que l'APD ;

(a.3) en désignant le COC en tant qu'autorité de protection des données compétente pour le service d'enquêtes du Comité P, comme le proposaient les premières versions de la LPD ; aucune explication rationnelle ne justifie de soustraire le service susmentionné, qui est en réalité un service de police (certes spécifique), au contrôle du COC, qui en sa qualité d'autorité de protection des données est compétent non seulement pour la police intégrée mais aussi pour l'AIG.

[71] Voir plus haut le point 10, note de bas de page 27.

De cette manière, tous les services de police (spécifiques) auraient la même autorité de protection des données. L'APD doit par exemple actuellement se pencher sur une demande portant sur les traitements effectués par le service d'enquêtes P, alors qu'elle préférerait – et c'est compréhensible – se retirer entièrement de la 'matière policière'.

(b) <u>Les compétences correctrices et autres :</u> Il convient d'apporter quelques éclaircissements au sujet des compétences du COC lui-même qui ont trait :

- à ses compétences correctrices ;

- à sa compétence d'agir à l'encontre de fonctionnaires de police individuels ;

- à sa compétence à l'égard des écoles de police ;

- à la possibilité – après consultation du magistrat compétent – de prendre également des mesures correctrices dans des enquêtes préliminaires en cours ;

- à l'accès direct incontestable du COC à toutes les banques de données auxquelles la police intégrée a accès (au même titre que les autres entités relevant de la compétence du COC) ;

- aux possibilités dont dispose le COC de fournir ou non des informations complémentaires à la personne concernée dans le cadre d'une demande d'accès indirect (donc davantage que la communication actuelle selon laquelle le COC a effectué les *« vérifications requises »*) ;

- à l'idée de ne pas imposer le système de l'accès indirect à une personne concernée pour l'exercice de ses droits portant sur des images enregistrées par des caméras (vu que ce n'est pas réalisable dans la pratique pour le COC) ;

- à la question de savoir contre quelles décisions du COC un moyen de droit peut être utilisé, etc.

(c) <u>L'astreinte administrative :</u> Un autre point d'attention réside dans la nécessité de disposer d'une forme de moyen de pression, qui pourrait par exemple être l'astreinte administrative. Le COC n'est pas d'emblée demandeur de pouvoir infliger des amendes administratives, mais préfère tout de même se réserver cette possibilité.

Si un service de police ne veut pas se conformer à une mesure correctrice (qu'il soit en cela soutenu ou non, voire commandé par ses autorités de police), la seule possibilité dont le COC dispose en réalité actuellement est celle de transmettre le dossier au parquet. On peut donc se demander si ce parquet, qui doit collaborer au quotidien avec ce service de police, sera enclin à faire pression sur ce service, voire à intenter des poursuites pénales à son encontre. Le COC est plutôt sceptique à ce sujet. Étant donné que l'exclusion de l'amende administrative pour les administrations publiques (voir l'article 221, §2 de la LPD) fait l'objet d'un recours en annulation devant la Cour constitutionnelle,[72] il convient d'attendre de voir si la Cour ne va pas d'emblée fournir la réponse et la solution.

(d) <u>L'accès direct aux banques de données policières :</u> Une grande préoccupation est et reste l'accès direct du COC et de ses membres (du personnel) à <u>toutes</u> les banques de données policières. À l'heure actuelle, le COC a accès par le biais de PORTAL à la BNG et à quelques autres banques de données pouvant être consultées au moyen de l'application KIK.[73] Cependant, il existe en dehors de cela encore toute une série de banques de données que le COC n'est pas en mesure de consulter directement et qui sont cruciales (à commencer par les banques de données essentielles). La concertation avec la GPI est à cet égard plutôt laborieuse. Cette dernière part en effet encore du principe qu'il doit à chaque fois y avoir une base légale ou réglementaire spécifique justifiant que le COC obtienne cet accès.

[72] Recours en annulation de l'article 221, §2 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, intenté par l'ASBL « Fédération des Entreprises de Belgique », numéro de rôle 7135 (FR), M.B. 9 avril 2019.
[73] KIK est une forme d'application de recherche avec laquelle différentes banques de données policières peuvent être consultées.

Le COC n'est pas d'accord avec ce point de vue, qui lui complique considérablement la tâche dans sa mission de contrôle. Le COC adhère au point de vue univoque selon lequel il doit disposer d'un accès – et aussi d'un accès direct – à toutes les banques de données auxquelles la police a accès, ce qui tient plutôt de l'évidence pour un organe de contrôle de la police, ou du moins le devrait. De plus, la base légale régissant cette question existe déjà à l'article 244, §1er de la LPD : *« L'Organe de contrôle, ses membres et les membres du service d'enquête ont un accès illimité à toutes informations et données traitées par les services visés par l'article 26, 7°, a) … et en particulier … »* (soulignement propre). Cette disposition est très large et inclut aussi les banques de données dont la police n'est pas le responsable du traitement (ni le préposé du responsable du traitement). La consultation d'une 'banque de données externe' par la police est en effet également un 'traitement'. Vu la formulation de l'article 244, §1er de la LPD, il semble clair sur le plan juridique que le COC doit non seulement y avoir accès mais aussi, pour autant évidemment que ce soit techniquement possible, qu'il doit s'agir d'un accès direct. À titre additionnel, il convient de faire référence également aux dispositions pertinentes tant du RGPD que de la *LED*, qui prévoient que des *« pouvoirs effectifs »* doivent être conférés à l'autorité de contrôle (soulignement propre). On peut à cet égard citer l'article 47.1 de la directive : *« Chaque État membre prévoit, par la loi, que chaque autorité de contrôle dispose de pouvoirs d'enquête effectifs. Ces pouvoirs comprennent au moins celui d'obtenir du responsable du traitement ou du sous-traitant l'accès à toutes les données à caractère personnel qui sont traitées et à toutes les informations nécessaires à l'exercice de ses missions. »* (soulignement propre). Le COC veut couper court à toute discussion en la matière en prévoyant une disposition légale explicite.

(e) Les moyens de droit contre les décisions du COC : Un défi de taille réside dans l'évolution sur le plan des possibilités de recours auprès du pouvoir judiciaire contre les décisions du COC. Aussi longtemps que les recours se limitent à quelques cas par an, cela ne posera pas un problème majeur ; si par contre les recours se multiplient, il faudra inévitablement prévoir des renforts.

La crainte de procès ne saurait par ailleurs retenir et ne retiendra jamais le COC de prendre des mesures correctrices ou, plus généralement, de statuer avec fermeté. Pour ce qui est des dossiers 'accès indirect', il faudrait préciser qu'un recours devant le juge ne peut jamais être introduit à l'encontre de la décision du COC lui-même ni à l'encontre du COC en tant qu'institution, mais peut uniquement être introduit à l'encontre du responsable du traitement (voir plus haut).

81. Pour conclure, nous pouvons dire que la protection de la vie privée et la protection des données ont auprès de la police pris une dimension nouvelle et gagné en importance depuis mai 2018. Pour la GPI, ce domaine et cette dimension sont donc une donnée nouvelle, de sorte qu'une certaine période de tolérance et d'adaptation est acceptable. Le COC est disposé dans ce contexte à assister, soutenir et conseiller tous les acteurs. Il ne prendra des mesures correctrices et ne recourra à l'astreinte qu'en tant qu'*ultimum remedium*, mais il n'hésitera pas à le faire si cela s'avère nécessaire. Néanmoins, le COC privilégiera toujours dans la mesure du possible une approche axée sur la médiation et la solution.

La commission parlementaire 'attentats'[74] qui a fait appel au COC dans le cadre de ses travaux, a fait entre autres la recommandation suivante en ce qui concerne '*la réglementation*': « *Le COC doit par ailleurs pouvoir contrôler la sécurité globale de la gestion de l'information et non plus seulement certains aspects de celle-ci* » et a en ce faisant, a pointé l'importance des activités du COC. Le COC effectuera donc cette tâche de la façon la plus efficiente possible en 2020 et tentera même de l'approfondir.

Rapport d'activités des années 2016 à 2019, approuvé par l'Organe de contrôle de l'information policière, le 25 mai 2020.

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

[74] Commission parlementaire chargée d'examiner les circonstances qui ont conduit aux attentats terroristes du 22 mars 2016 dans l'aéroport de Bruxelles-National et dans la station de métro Maelbeek à Bruxelles, y compris l'évolution et la gestion de la lutte contre le radicalisme et la menace terroriste, *La Chambre*, 2016-2017, DOC 54, n° 1752/008, p. 252.

ANNEXE: L'ORGANE DE CONTROLE EN CHIFFRES[75]

DOSSIERS	ANNEE	NOMBRE
Demandes d'accès indirect	2019	392
Demandes d'information et avis protection des données	2019	81
Demande d'information et avis gestion de l'information policière	2019	1
Avis loi ou réglementation	2019	22
Plaintes pour consultation ou traitement illégitimes	2019	30
Avis sur l'utilisation de caméras	2019	32
Enquêtes de contrôle caméras	2019	2
Visites d'envergure zone de police/entités PF	2019	2
Enquête de contrôle SIS II	2019	1
Enquête de contrôle BELPIU	2019	1
Enquête de contrôle BDC Terrorisme	2019	1
TOTAL	**2019**	**565**

[75] Il est bien sûr à noter que l'investissement, à la fois en termes de capacité et de temps, dans des visites ou contrôles circonstanciés, n'est pas comparable avec celui d'un avis. Il faut donc comprendre que les différentes sortes d'enquêtes et d'avis ne sont pas ou du moins très difficilement, comparables en ce qui concerne la charge de travail.

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