Éditeur responsable :

Frank Schuermans – Président a.i. de l'Organe de contrôle de l'information policière

Adresse : Rue de Louvain 48 – 1000 Bruxelles

E-mail : info@organedecontrole.be

Illustrations :

(1) Images du Parlement fédéral et des environs – de Kurt Van Den Bossche – Droits réservés à la Chambre des Représentants

(2) Images de membres de la police – Droits réservés à la police

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

TABLE DES MATIÈRES

A. Préambule du comité de direction

B. Cadre légal

C. Vision et mission

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

1. INTRODUCTION

1.1. Compétences et missions

1.1.1. Quatre missions prioritaires

1.1.2. Compétences

1.1.3. Organisation et composition

1.1.4. Quelques chiffres clés relatifs à l'organisation interne

2. LES ACTIVITÉS RELEVANT PRINCIPALEMENT DE LA PROTECTION DES DONNÉES

2.1. Les demandes d'accès indirect (AI)

2.2. Les demandes d'informations et d'avis

2.3. Avis au sujet de la législation et de la réglementation

2.4. Les plaintes

2.5. Les brèches de sécurité (databreach)

2.6. Les enquêtes internationales

2.7. Protection des données dans des secteurs et matières spécifiques

2.7.1. Contrôle spécial : les contrôles BELPIU

2.7.2. Contrôle spécial : les réquisitions fiscales de l'AGD&A à la BELPIU

2.7.3. L'Inspection générale de la police fédérale et de la police locale

2.8. Utilisation de caméras par les services de police

2.8.1. Généralités

2.8.2. Demandes d'informations et d'avis concernant l'utilisation de caméras

2.8.3. Quelques enquêtes spécifiques

2.9. L'exercice des compétences correctrices

2.9.1. Les mesures correctrices prises

2.9.2. Les recours judiciaires contre les décisions du COC

3. LES ACTIVITÉS RELEVANT PRINCIPALEMENT DU CONTRÔLE

3.1. Les enquêtes de contrôle menées auprès de la GPI

3.1.1. Généralités

3.1.2. Aperçu des principales enquêtes de contrôle

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

3.3. Le contrôle des statistiques de la BNG en tant que fondement pour la rétention de données

4. LES ACTIVITÉS POLITIQUES

4.1. Forums de concertation nationaux

4.2. Forums de concertation internationaux

4.3. Communication externe et participation à des événements

4.3.1. Contacts avec la presse

4.3.2. Participation à des journées d'étude et formations

4.3.3. Site Internet

4.3.4. Consultations du COC par des étudiants et d'autres externes

5. PARTENARIATS ET COMPÉTENCES PARTAGÉES

6. CONCLUSION ET PERSPECTIVES D'AVENIR

ANNEXE : L'ORGANE DE CONTRÔLE EN CHIFFRES

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

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 de données 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*

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* (voir aussi UIP)

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 comité de direction

1. Le présent rapport d'activité présente un aperçu des activités de l'Organe de contrôle de l'information policière ou COC[1] en 2022. 2022 est la quatrième année de fonctionnement complète du COC, qui, dans le sillage de la mise en place du nouveau cadre européen et national en matière de protection de la vie privée et des données[2], en septembre 2018, s'est durant cette période résolument positionné dans le paysage du contrôle de la police intégrée belge (GPI).

2. Un rapport d'activité est toujours l'occasion de procéder à une brève rétrospective, a fortiori dès lors que 2022 a été la dernière année du fonctionnement du comité de direction (DIRCOM) dans sa composition initiale. Au 01.02.2023, le président Philippe Arnould a en effet pris sa retraite. L'efficacité de la collaboration entre les membres du DIRCOM est cruciale pour toute organisation, et encore plus pour une organisation à petite échelle comme le COC qui, tout comme ses collaborateurs, doit disposer à la fois de l'expertise technique requise, d'une bonne connaissance des dossiers et d'aptitudes en matière de gestion des ressources humaines.

3. Créé en tant qu'organe spécifique chargé en priorité de contrôler l'efficacité et l'efficience de la gestion de l'information policière, le COC se trouvait entre 1998 et 2014 sous l'autorité conjointe des ministres de l'Intérieur et de la Justice. En 2014, le COC a été transféré au pouvoir législatif pour finalement exercer à partir du 05.09.2018 une mission additionnelle en tant qu'autorité de protection des données spécialisée en charge (entre autres) de la GPI.

---

[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 »), d'une part, 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 »), d'autre part.

B. Cadre légal

4. Le cadre légal se compose d'une part 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 de la législation nationale fondamentale comme la LPD (loi relative à la protection des données), la LFP (loi sur la fonction de police) et dans une moindre mesure 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 police intégrée (GPI) et pour les autres services soumis au contrôle du COC, le sont également pour le COC. Les dispositions les plus importantes sont celles que l'on retrouve à l'article 4 §2, 4e alinéa de la LCA, à l'article 71 et aux titres II et VII de la LPD et dans la LFP (articles 25/1 à 25/8 inclus, 44/1 à 44/11/13 inclus et 46/1 à 46/14 inclus).

5. Par souci de clarté, nous rappelons que le COC n'est pas uniquement une autorité de protection des données, mais aussi une instance de contrôle régulière en charge notamment de la gestion de l'information policière dans son ensemble.

C. Vision et mission

6. Le COC aspire dans sa mission/vision 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[3], de la BELPIU[4] et de l'AGD&A[5].

Il adopte une attitude constructive en commençant par assister et sensibiliser les institutions contrôlées. Ce n'est qu'en dernier recours qu'il procédera éventuellement à une intervention contraignante à travers la prise d'une «mesure correctrice» (voir plus loin).

[3] L'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).
[4] 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.
[5] L'Administration générale des Douanes et Accises du Service public fédéral Finances.

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

1. INTRODUCTION

1.1. Compétences et missions

1.1.1. Quatre missions prioritaires

7. Les compétences et missions du COC incluent dans les grandes lignes:

(1) la surveillance de l'application du titre 2 de la LPD à l'égard de la GPI, de l'AIG et de la BELPIU, autrement dit tous les traitements ayant trait à l'exécution des missions opérationnelles;

(2) la surveillance de l'application du RGPD et du titre 1er de la LPD par la GPI, à savoir tous les traitements (ayant trait à la protection de la vie privée) dans le cadre de l'exécution des missions non opérationnelles (par exemple les traitements HRM[6]);

(3) le contrôle du traitement de l'information et des données à caractère personnel visées aux articles 44/1 à 44/11/14 de la LFP, y compris celles introduites dans toutes les banques de données policières;

(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 l'utilisation visible et non visible de caméras par la GPI;

(b) à la loi du 25 décembre 2016 relative au traitement des données des passagers (contrôle du fonctionnement de la BELPIU);

(c) à la compétence du COC à l'égard des Douanes en ce qui concerne les réquisitions adressées par ce service à la BELPIU dans des matières fiscales;

[6] *Human Ressources Management.*

(d) à la législation sur la rétention des données, selon laquelle le COC est chargé, en vertu de l'article 126/3 §1er, 8e alinéa de la loi du 13 juin 2005 relative aux communications électroniques (ci-après 'la LCE'), de la validation (ou non) des statistiques relatives au nombre de faits punissables et au délai de conservation pour chaque arrondissement judiciaire et chaque zone de police;

(e) à l'article 42 §3, 2e et 3e alinéa de la LFP, en vertu duquel le COC est également chargé du contrôle des requêtes de la Cellule Personnes disparues de la police fédérale en vue de la consultation des données relatives aux communications électroniques impliquant la personne disparue.

8. Lorsque nous parlons dans la suite de ce rapport d'activités ***«relevant principalement»*** de la protection des données ou d'activités ***«relevant principalement»*** du contrôle, nous entendons par là que chacune de ces deux catégories d'activités inclut également des aspects de l'autre dimension. Autrement dit, même lorsqu'une activité relève principalement de la protection des données, elle comporte également toujours des éléments ayant trait à l'efficacité, à l'efficience et à la conformité à d'autres droits fondamentaux ou prescriptions légales. À l'inverse, lorsque l'accent est mis sur la mission de contrôle, le respect de la vie privée et la protection des données constitue tout de même un volet crucial de l'activité.

1.1.2. Compétences

9. Les compétences du COC sont les missions classiques d'un organe de surveillance ou de contrôle. Une série de réparations s'imposent néanmoins du fait que le COC est également une autorité de protection des données. Ces adaptations requises ont été communiquées par le COC en mai 2021 dans le cadre de l'évaluation de la LPD prévue à l'article 286[7] qui a été réalisée par le secrétaire d'État chargé de la protection de la vie privée. Toutefois, la réparation requise de la LPD n'a toujours pas été réalisée à l'heure où nous clôturons la rédaction de ce rapport d'activité. De l'avis du COC, cette

[7] L'article 286 prévoit une évaluation de la LPD dans le courant de la troisième année à compter de son entrée en vigueur. La LPD étant entrée en vigueur le 5 septembre 2018, son évaluation devait donc intervenir dans le courant de 2021.

loi de réparation est en tout état de cause indispensable pour lui permettre d'optimaliser son fonctionnement, et donc aussi la surveillance de la GPI et des autres instances contrôlées.

1.1.3. Organisation et composition

10. Le COC se compose d'un comité de direction (DIRCOM) composé de trois membres, dont deux magistrats et un expert. À cela s'ajoute un «service d'enquête» (DOSE[8]) composé de 2 membres provenant de la GPI et de 1 expert. Vient enfin un «service de soutien» («secrétariat») composé de 1 juriste, 1 informaticien et 1 assistant de direction. Le COC peut en outre recruter contractuellement[9] jusqu'à maximum 30 % de son effectif total (sur un cadre de 9 ETP), ce qu'il s'efforce toujours de faire de manière à porter l'effectif au maximum de 11 ETP s'il est au complet. Cela dit, il est rare que l'effectif soit au complet. Il convient notamment de signaler à cet égard la vacance, depuis le 1er août 2022, de l'unique fonction d'informaticien, à laquelle il n'a toujours pas pu être pourvu à l'heure où nous clôturons le présent rapport. Le COC a dans l'intervalle fait 3 tentatives de recrutement mais se heurte à la pénurie cuisante de profils de ce type sur le marché de l'emploi, à laquelle s'ajoutent les exigences rigoureuses que le COC est tenu d'imposer de par son position étatique et du fait qu'il ne dispose que d'un seul poste d'informaticien (ce qui implique par exemple que le candidat recruté doit obligatoirement être trilingue).

Toute la politique PLIF[10] doit également être assurée par les membres du DIRCOM, moyennant il est vrai un soutien de la part de Persopoint. Contrairement aux autres institutions parlementaires collatérales, le COC ne dispose pas non plus d'une administration, si ce n'est un(e) assistant(e) de direction.

Le centre de services commun 'INCENTRIS' projeté par la Chambre en 2021 ne sera finalement **pas** créé, de sorte que la charge de travail du COC en matière de PLIF demeure inchangée.

---

[8] **D**ienst **O**nderzoeken/**S**ervice d'**E**nquête.
[9] 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.
[10] Personnel, Logistique, Informatique et Finances.

1.1.4. Quelques chiffres clés relatifs à l'organisation interne

11. 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 des autres institutions ayant droit à une dotation. Il convient de souligner également qu'il est rare que le cadre complet de 11 ETP puisse être maintenu. En 2022, le COC a par exemple dû se passer d'informaticien pendant une demi-année (après le départ de ce dernier pour le *Belgian Cyber Security Centre*[11]) et a aussi perdu deux juristes, une fonction pour laquelle il s'écoule toujours au moins quelques mois avant qu'un remplaçant ne soit trouvé. De plus, la technicité et les exigences de la fonction sont telles, même pour un juriste, qu'il faut au moins 6 mois pour pouvoir véritablement fonctionner correctement.

Le DIRCOM a tenu 47 réunions formelles en 2022 (avec procès-verbal), en plus des consultations informelles quotidiennes. En principe, il y a aussi une réunion plénière chaque semaine avec tous les membres du personnel, au cours de laquelle peuvent être abordés aussi bien des sujets opérationnels que des thèmes dits PLIF.

12. Le COC disposait en 2022 d'un budget de dépenses approuvé de 1.618 KEUR, pour lequel il a perçu une dotation de 1.314 KEUR. La dotation est exclusivement utilisée pour s'acquitter des charges salariales, de sorte que toutes les autres dépenses de fonctionnement et d'investissement doivent être financées au moyen des réserves qui ont été accumulées au fil des années précédentes grâce à la politique parcimonieuse menée par le COC (et du fait qu'il n'a pas été pourvu aux remplacements ou qu'il y a été pourvu tardivement). Nous avions déjà indiqué dans notre rapport d'activité précédent que cette situation ne serait plus viable à partir de 2023 et que la dotation devra donc davantage couvrir les dépenses réelles. Il en a été tenu compte pour 2023, à travers l'approbation d'un budget de dépenses de 2.047 KEUR et l'octroi d'une dotation de 1.860 KEUR. Une grande partie des charges de fonctionnement n'est cependant toujours pas couverte par la dotation, de sorte que l'excédent de ces dépenses devra toujours être financé au moyen des réserves existantes. Il semble d'ailleurs que des réserves aient été accumulées en 2022

[11] Un départ qui nous a amenés à constater que le COC n'est pas en mesure de rivaliser avec d'autres institutions (même parlementaires) en termes de conditions salariales.

également du fait qu'il n'a pas pu être pourvu à temps aux fonctions devenues vacantes. En comparaison des autres autorités de contrôle, le COC n'en demeure pas moins la moins bien lotie avec sa dotation des plus modestes.

2. LES ACTIVITÉS RELEVANT PRINCIPALEMENT DE LA PROTECTION DES DONNÉES

2.1. Les demandes d'accès indirect (AI)

13. Les demandes formulées par 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 – mieux connues sous l'appellation 'dossiers article 42 de la LPD'[12] ou 'dossiers AI'[13] – constituent une part de plus en plus prépondérante des activités réactives quotidiennes du COC, au point qu'elles ont en 2022 affecté pour la première fois de manière significative les missions de contrôle proactives du COC. Contrairement aux autres pays de l'UE, qui disposent pour la police d'un système d'accès direct, ces dossiers sont en Belgique traités par le COC.

14. Chaque dossier d'accès indirect requiert un effort substantiel de la part des gestionnaires de dossiers, à savoir les membres du DIRCOM, les membres du DOSE et les juristes du COC. Le volume de travail est en effet tel que pour ainsi dire tous les membres et membres du personnel du COC sont obligés de se consacrer au traitement de ces demandes.

15. Le nombre de demandes a connu une augmentation exponentielle au fil des ans. Sachant que la Commission de la protection de la vie privée de l'époque traitait en moyenne entre 100 et 150 dossiers par an, le volume a atteint un nouveau pic en 2022 avec **555 dossiers**.

---

[12] 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).

[13] « AI » signifiant « Accès indirect ».

<u>Tableau 1 :</u> Évolution du nombre de demandes d'accès indirect adressées au COC

Année	Nombre de dossiers AI
2018	333
2019	392
2020	283
2021	546
2022	555

16. Des **555** dossiers AI qui ont été introduits en 2022, **<u>520</u> avaient déjà été traités** lors de l'établissement des statistiques à la fin mars 2023. **Autrement dit, cela signifie qu'un peu plus de 93 % des demandes avaient été clôturées avec réponse à la personne concernée lors de leur inclusion dans les statistiques.**

<u>Tableau 2 :</u> Délai de traitement moyen et médiane

Année	Délai de traitement moyen en jours	Médiane en jours
2019	193,86	147
2020	85,63	58
2021	63,35	43
2022	51,65	39

Le <u>délai de traitement moyen</u>[14] était de **51,65 jours en 2022 (médiane : 39 jours)**, ce qui prouve que les délais de traitement diminuent toujours et que des gains d'efficacité sont donc toujours enregistrés au niveau du traitement de ces dossiers. Les gestionnaires de dossiers du COC acquièrent de plus en plus de connaissances et les accès aux banques de données policières se multiplient. En 2022, un accès à toutes les banques de données CAD de tous les CIC a été mis en place, tandis que les accès aux banques de données de base ISLP et FEEDIS ont été étendus. La seule limitation rencontrée ici par le COC a été le maximum technique de 25 unités par personne. Le COC a par ailleurs misé sur un accès aux informations policières conditionné par un code d'utilisateur restrictif. Le COC s'efforce en outre toujours de mettre en place une

[14] Le nombre de jours qui s'écoulent entre la date de la demande (généralement introduite par e-mail) et la date de la décision finale.

approche coordonnée qui serait confiée au DPO de l'entité de police la mieux placée ou du CG/ISPO de le police fédérale, partant du principe que la responsabilité doit incomber à la partie qui en est légalement investie, à savoir le responsable du traitement (fonctionnel ou opérationnel).

Si nous faisons abstraction des dossiers d'étrangers dont la majorité peuvent assez rapidement être transmis à l'Office des Étrangers, nous obtenons pour l'année 2022 un délai de traitement moyen de 67,5 jours (médiane 47) pour les dossiers standard[15] d'accès indirect.

Vu le fort coefficient de travail, le nombre toujours élevé de dossiers en 2022 depuis le début des activités d'autorité de protection des données du COC (avec un cadre demeuré inchangé), le fait que le COC dépend de la rapidité et de la priorité avec lesquelles la GPI fournit au COC les évaluations qu'il lui demande et les questions parfois complexes qui se posent, notamment en raison de la structure morcelée de la police belge, le COC considère ce chiffre de 2022 comme très performant, tout comme en 2021[16].

17. De ces 520 dossiers traités, 308 avaient trait à la Banque de données nationale générale (BNG), autrement dit 59,23 %.

Voici les résultats et/ou l'orientation finale des dossiers traités :

(1) maintien du (des) enregistrement(s) : 97, soit 18,65 %
(2) archivage/effacement du (des) enregistrement(s) : 109, soit 21 %
(3) rectification du (des) enregistrement(s) : 67, soit 13 %
(4) (plus) aucune coopération de la part de la personne concernée[17] : 126, soit 24,23 %
(5) il n'y avait pas d'enregistrement dans la BNG : 59, soit 11,34 %
(6) la demande était purement une demande d'informations : 16, soit 0,03 %
(7) la demande n'était pas recevable : 13, soit 0,025 %

[15] Nous entendons essentiellement par là des dossiers de Belges ou de personnes d'une autre nationalité qui habitent ou résident en Belgique.
[16] Ce chiffre n'est en tout cas plus comparable aux longs délais de traitement de la Commission de la protection de la vie privée de l'époque.
[17] 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.

(8) le délai de conservation était dépassé : 86, soit 16,5 %

Le nombre total d'orientations, à savoir 573, est supérieur au nombre total des 520 dossiers BNG clôturés en mars 2022 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 aussi par un maintien de l'enregistrement.

Tableau 3 : Décisions finales concrètes du COC dans le cadre des demandes d'accès indirect ayant trait à la BNG

Résultat	**2019**	**2019 en %**	**2020**	**2020 en %**	**2021**	**2021 en %**	**2022**	**2022 en %**
Maintien de l'enregistrement	59	**33 %**	48	**22,75 %**	65	**11,9 %**	**97**	**18,65 %**
Rectification	15	**8,5 %**	31	**14,69 %**	92	**18,58 %**	**67**	**13 %**
Archivage/effacement	49	**28 %**	78	**36,97 %**	155	**31,3 %**	**109**	**21 %**
Total	**123**		**144**		**312**		**273**	

Si nous prenons uniquement les dossiers dans lesquels le COC a émis une **évaluation ou décision concrète**[18], **nous constatons qu'environ 33,8 % des dossiers BNG traités en 2022 (176 dossiers sur 520) se sont soldés par un archivage/effacement complet ou partiel des enregistrements effectués par la police dans la BNG**. **Il s'agit d'une diminution marquée par rapport aux années précédentes**, que l'on doit aux premières réalisations techniques d'un archivage automatisé généralisé (voir plus loin).

Tableau 4 : Décisions d'archivage/d'effacement des enregistrements dans la BNG

Année	**Archivage ou effacement**
2019	52 %
2020	75,69 %
2021	79 %
2022	33,8 %

[18] Il s'agit donc des dossiers dans lesquels le COC a vraiment émis une évaluation concrète, à savoir les dossiers qui se sont soldés par un maintien de l'enregistrement, une rectification ou un effacement complet.

18. Ce pourcentage a donc en effet diminué, mais il doit néanmoins continuer à inciter tous les dirigeants de la GPI à la réflexion et à l'action, s'agissant là d'un appel que nous avions déjà lancé dans nos précédents rapports d'activité. **La qualité (l'exactitude et la précision) des banques de données policières laisse encore (trop) à désirer, ce qui a des retombées potentiellement très préjudiciables pour le citoyen. Celui-ci peut en effet être directement ou indirectement préjudicié par des traitements de données incorrects, dépassés ou autrement impropres.** Directement, parce que le traitement dont le citoyen fait l'objet (fouille, arrestation, approche policière, lien avec les banques de données techniques ANPR, etc.) ne saurait être correct dès lors qu'il repose sur des informations erronées. Et indirectement, du fait qu'il est ainsi injustement fait obstacle ou mis un terme à l'accès à certains métiers: les (candidats) fonctionnaires de police, les agents de sécurité, les militaires, les travailleurs du secteur de la sécurité privée, les travailleurs d'une centrale nucléaire et autres sont tous jugés notamment sur leurs «antécédents policiers». On peut aussi penser à l'approche administrative communale qui sera mise en place dans un avenir proche et qui fera en sorte que ces antécédents policiers seront également pris en compte pour décider du refus, de la suspension ou de la révocation de permis d'établissement ou d'exploitation ou de la fermeture d'établissements[19].

Il est frappant de constater que le COC a reçu 27 demandes d'accès indirect de la part de **membres ou de candidats membres de la GPI**, un nombre qui représente **5 %** des demandes. En 2021, il s'agissait encore de 52 demandes, de sorte qu'une baisse substantielle était perceptible en 2022.

Dans le sillage de la matérialisation de la directive relative à l'interconnexion de banques de données[20] dans des applications comme FOCUS et du déploiement potentiel du système *police/search ISLP* accessible par le biais de FOCUS, la question se pose par ailleurs de savoir dans quelle mesure un effacement et/ou une rectification dans la BNG se répercute(nt) également dans les autres banques de données

[19] Voir à ce sujet l'avis DA220002 du 8 novembre 2022 de l'Organe de contrôle relatif à un avant-projet de loi relative à l'approche administrative communale, à la mise en place d'une enquête d'intégrité communale et portant création d'une Direction chargée de l'Évaluation de l'Intégrité pour les Pouvoirs publics (voir aussi Doc. Parl. *Chambre*, 2022-2023, DOC 55 3125/001).
20 Directive contraignante commune des Ministres de la Justice et de l'Intérieur relative aux 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, M.B. 04-08-2021.

policières comme ISLP ou les banques de données particulières. Il existe un risque réel qu'un enregistrement effacé ou archivé dans la BNG figure tout de même encore dans une autre banque de données policière comme FOCUS et/ou le système *police search/ISLP*, voire dans des banques de données non policières comme SIDIS[21], ce qui ne saurait évidemment être le but.

Le déploiement de l'archivage automatique de la BNG – annoncé depuis de nombreuses années et légalement obligatoire depuis 2017 – s'est poursuivi en 2022 mais n'est toujours pas finalisé au moment de la clôture du présent rapport d'activité (mai 2023).

Tableau 5 : Nombre de dossiers clôturés en 2022, ventilés en fonction du type de banque de données policière auquel la demande avait trait[22]

Type de banque de données	2019	2020	2021	2022
BNG	171	211	315	308
Banque de données de base	-	6	14	18
Banque de données particulière	-	2	6	3
Banque de données technique	-	2	4	0
SIS II	68	41	202	197
BDC T&E[23]	0	1	1	1
Autre[24]	1	6	10	8
Europol	7	7	1	5
Interpol	3	13	12	5
Total	250[25]	289[26]	564[27]	545[28]

19. Un dossier d'accès indirect induit un très fort coefficient de travail et inclut plusieurs étapes: analyse de la demande, consultation de diverses banques de

[21] La banque de données de l'administration pénitentiaire.
[22] Un tiret (-) signifie que cette catégorie n'était pas encore reprise séparément dans les chiffres de 2019.
[23] Banque de données commune Terrorisme et Extrémisme.
[24] Le type « Autre » peut par exemple couvrir les banques de données pour lesquelles la GPI n'est pas le responsable du traitement, comme le Registre national ou le répertoire des véhicules.
[25] Ce total de 250 est supérieur au nombre de dossiers clôturés (234) du fait qu'une requête peut avoir trait à plusieurs banques de données policières.
[26] Ce total de 289 est supérieur au nombre de dossiers clôturés (259) du fait qu'une requête peut avoir trait à plusieurs banques de données policières.
[27] Ce total de 564 est supérieur au nombre de dossiers clôturés (495) du fait qu'une requête peut avoir trait à plusieurs banques de données policières.
[28] Ce total de 545 est supérieur au nombre de dossiers clôturés (520) du fait qu'une requête peut avoir trait à plusieurs banques de données policières.

données policières, envoi à la GPI d'une demande d'évaluation[29]de la pertinence (permanente) ou de la légalité[30] d'un ou plusieurs enregistrements, concertation éventuelle avec la GPI (et/ou le parquet), correction/ventilation éventuelle ou archivage des données à la demande du COC, contrôle par le COC des rectifications ou effacements promis ou annoncés par la GPI, communication avec le plaignant/déclarant ou son avocat, etc. …

Du fait que la GPI choisit – notamment en raison du morcellement de l'organisation policière – de répartir la responsabilité des enregistrements entre les différentes entités de police concernées (allant dans la pratique de deux à plus de dix entités), une coordination entre toutes les entités responsables concernées s'impose dans un nombre croissant de dossiers pour diverses raisons, dont la cohérence entre les différents points de vue et la maîtrise du délai de traitement des demandes.

Il va néanmoins de soi qu'il n'appartient **pas** à l'Organe de contrôle en sa qualité d'autorité de protection de données de mettre en place une telle coordination au sein de la police **intégrée**, s'agissant là par excellence d'une responsabilité opérationnelle de la police.

Pour cette raison, le COC a commencé dans le courant de 2021 à travailler dans certains dossiers dont la complexité l'exige avec un seul 'coordinateur de la protection des données' désigné par le COC ou par la GPI, et ce pour des motifs structurels (tels que définis aux articles 99 à 105 inclus de la LPI) ou pour des motifs fonctionnels de contenu (responsabilité d'un fait revêtant un caractère absorbant, d'une enquête en cours ou de mesures à prendre en cours). Cette nouvelle approche du COC depuis 2021 a été encore plus assidûment appliquée en 2022. Si elle permet d'une part un plus grand respect du droit à la protection des données, elle contribue d'autre part à donner à certains dossiers des nouvelles ou différentes orientations tactiques opérationnelles. Il convient néanmoins de souligner que la part de ces 'indications du COC' dans le nombre total de demandes reste limitée à moins de 10 %.

[29] Une demande peut en effet avoir trait à plusieurs enregistrements réalisés par différents services de police.
[30] Lorsque le délai de conservation maximal a été dépassé (par ex. un enregistrement d'un vol simple peut être conservé durant maximum 10 ans, sauf en cas d'« absorption »), la pertinence ne joue même plus aucun rôle et les enregistrements doivent être archivés.

20. C'est notamment sur la base de ces dossiers que le COC a dû à nouveau constater en 2022 que la BNG contient encore trop d'inexactitudes et/ou d'erreurs, alors qu'il s'agit justement de la banque de données qui contient uniquement des données dites **validées**[31], et notamment :

- des délais de conservation (largement) dépassés ;

- une qualification erronée conférée aux faits ;

- des motifs d'enregistrement erronés ou caducs ;

- des rapports d'information dont le délai de conservation est dépassé ou qui n'ont plus aucune pertinence ;

- des signalements qui restent ouverts sans aucune valeur ajoutée ni évaluation intermédiaire ;

- l'absence de suite judiciaire en exécution de l'article 646 du Code d'instruction criminelle et de l'article 44/5 §6 de la LFP ;

- etc. …

21. Les dossiers d'accès indirect peuvent être l'occasion pour le COC de se pencher sur des problèmes, des questions ou des thèmes qui relèvent plutôt des principes ou qui reviennent fréquemment. Par ailleurs, il est important de répéter qu'une personne concernée n'a à notre avis pas la possibilité, dans le cadre d'un dossier AI, d'opposer un moyen de droit au COC, qui **doit** en vertu de la loi clôturer chaque dossier par la communication sibylline au citoyen que le COC a procédé aux *« vérifications nécessaires »*. Le COC n'est donc pas autorisé à communiquer quoi que ce soit du contenu ni formuler de motivation dans un sens ou dans l'autre. Le COC ne fait donc que se substituer à la personne concernée dans l'exercice de ses droits. Une personne concernée dispose néanmoins d'un recours contre le responsable du traitement (les ministres de l'Intérieur et/ou de la Justice et/ou le chef de corps). Comme nous le disions dans le rapport d'activité de 2021, cette question de principe est toujours en cours d'évaluation par la Cour de Justice de l'Union européenne à Luxembourg – avec

[31] Terme renvoyant à un processus interne d'évaluation de l'exactitude et de la précision des informations et données à caractère personnel saisies, dans lequel plusieurs personnes sont impliquées.

l'investissement de capacité substantiel que l'on sait de la part des membres (du personnel) du COC –, dans le sillage de deux questions préjudicielles soumises par la Cour d'appel de Bruxelles à travers son arrêt du 9 mai 2022 rendu dans le dossier D.D. et *Ligue des Droits Humains* contre le COC :

1. «*Les articles 47 et 8, §3 de la Charte des droits fondamentaux de l'Union européenne imposent-il de prévoir un recours juridictionnel à l'encontre de l'autorité de contrôle indépendante telle que l'Organe de contrôle de l'information policière lorsqu'elle exerce les droits de la personne concernée à l'égard du responsable du traitement*»
2. «*L'article 17 de la Directive 2016/680 est-il conforme aux articles 47 et 8, §3 de la Charte des droits fondamentaux de l'Union européenne tels qu'ils sont interprétés par la Cour de justice en ce qu'il oblige l'autorité de contrôle – qui exerce les droits de la personne concernée envers le responsable de traitement – qu'à informer cette personne « qu'elle a procédé à toutes le vérifications nécessaires ou à un examen » et « de son droit de former un recours juridictionnel » alors que pareille information ne permet aucun contrôle a posteriori sur l'action et l'appréciation de l'autorité de contrôle au regard des données de la personne concernée et des obligations qui pèsent sur le responsable de traitement ?*»

Ces questions préjudicielles soumettent en tout état de cause à l'appréciation de la Cour de Justice de l'Union européenne la question de la conformité ou non à la Charte des droits fondamentaux de l'Union européenne du système belge de l'accès indirect, lequel constitue un cas unique au sein de l'Union européenne[32]. Le verdict est attendu pour le second semestre de 2023.

2.2. Les demandes d'informations et d'avis

22. Par ailleurs, le COC a continué en 2022 à être consulté par des citoyens et par des professionnels – faisant la plupart du temps partie de la police, mais pas toujours

[32] Ce système a été introduit en 2018 et a été maintenu jusqu'à ce jour – en dépit de tous les signaux indiquant qu'il engendre sur le plan juridique de nombreux problèmes et frustrations – en raison des pressions exercées en ce sens par la GPI, qui est jusqu'ici suivie sans réserve dans ce raisonnement par les ministres de tutelle compétents.

– 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 la communication, par la police, d'informations policières à des tiers (par exemple le partage ou non des données à caractère personnel des parties impliquées dans un accident de la route, la communication ou non des données à caractère personnel d'auteurs d'infractions SAC-1[33]à la commune, la communication ou non de données à caractère personnel aux gardiens de la paix, etc. …). D'autres questions avaient trait notamment aux compétences du délégué à la protection des données (DPO), à la problématique des *screening* de toutes sortes, à la responsabilité des sous-traitants, à la publication ou non d'une AIPD, au fait de filmer des fonctionnaires de police, à la saisie ou non des infractions SAC-1[34] dans la BNG, aux compétences des agents de sécurité privés, à la qualification pénale correcte des violations du droit à la protection des données, à l'utilisation de données de test ou de données réelles, aux traitements dits 'SAC-5'[35], etc. … Des directives internes et/ou les ordres de service sont également soumis à l'avis du COC.

Une question peut parfois amener le COC à émettre un avis d'initiative devant le constat qu'une même thématique revient régulièrement à la surface. Ces avis d'initiative ont pour objectif de fournir à la GPI des directives et un cadre (juridique) sur certains thèmes (épineux). Les avis ne sont pas tous rendus publics. Certains sont (1) soit uniquement transmis à la ou aux parties prenantes[36], (2) soit diffusés exclusivement en interne au sein de la GPI sous la forme d'une publication sur l'intranet. En 2022, le COC a ainsi publié notamment les avis suivants sur le *Sharepoint* de la GPI :

- Avis DD210082 du 12.01.2022 relatif à la communication, par la police, des données du répertoire des véhicules (banque de données de la DIV) aux

[33] À savoir les infractions purement administratives (qui ne font donc plus l'objet de sanctions pénales, mais uniquement d'amendes administratives).
[34] À savoir les infractions purement administratives (qui ne font donc plus l'objet de sanctions pénales, mais uniquement d'amendes administratives).
[35] À savoir les excès de vitesse mineurs (dans une zone 30 ou en agglomération), qui peuvent également être traités par les communes mais qui sont tout de même encore constatés par la police.
[36] Par exemple l'avis DD220024 du 11.03.2022 relatif au contrôle, par la police, des membres des familles d'accueil de ressortissants ukrainiens expatriés (traduction libre).

communes afin de permettre à ces dernières de procéder à la perception d'une rétribution dans le cadre du stationnement limité dans le temps[37];

- Avis DD220075 du 08.11.2022 relatif au recours à des agents de sécurité privés à l'accueil des bâtiments de police[38].

Force est toutefois de constater que l'Organe de contrôle ne dispose pas d'une capacité suffisante pour s'acquitter pleinement de cette mission documentaire pour la GPI. Souvent, les avis sont uniquement transmis au demandeur sans être mis à la disposition de toute la GPI sous une forme adaptée (c'est-à-dire traduits[39], anonymisés, etc. …), par manque de capacité.

Les questions spécifiques relatives aux traitements par caméra seront abordées plus loin. Une demande d'avis peut aussi toujours donner lieu à l'ouverture d'une enquête (et/ou d'un avis) d'initiative, voire à l'exercice de compétences correctrices.

23. Le COC doit très régulièrement rappeler à la police qu'il lui est impossible d'être 'le juriste' et/ou 'le spécialiste de la protection de la vie privée' de tous les membres la GPI. Pour cette raison, il est important que la GPI fasse d'abord intervenir ses canaux internes et son propre délégué à la protection des données. Les entorses à ce principe sont encore fréquentes.

L'afflux constant de questions prouve d'autre part que la GPI considère le COC comme le centre d'expertise par excellence en la matière. La capacité nécessaire pour apporter une réponse de qualité à ces demandes reste cependant un défi de taille. **87 demandes d'avis (<u>pas</u> sur l'utilisation de caméras) ont été introduites en 2022, dont 82 étaient clôturées en avril 2023.** À titre de comparaison, ces demandes étaient au nombre de 81 en 2019, de 79 en 2020 et de 82 en 2021. En 2022, le COC a donc reçu le plus grand nombre de demandes d'avis jusqu'à ce jour.

Le COC intervient aussi souvent de manière informelle (avis téléphonique, réunions Teams, réponses directes par e-mail sans enregistrement dans le système de gestion

[37] Traduction Libre.
[38] Traduction Libre.
[39] Le COC n'a pas de traducteurs internes et doit donc sous-traiter toutes les traductions à un prestataire externe et ensuite les contrôler, ce qui constitue également un obstacle en termes de budget et de capacité.

des dossiers du COC, etc. …). En 2022, 82 e-mails ont ainsi été traités et au moins 5 réunions ont eu lieu.

24. Pour 2022, le délai de traitement moyen est de 30,8 jours et est donc très comparable à celui de 2019, 2020 et 2021 (respectivement 28,46, 29,76 et 27,83 jours). Le COC a dès le départ pris comme principe un délai de réponse de 1 mois, mais répond aussi plus rapidement lorsque c'est possible. Tout dépend de la complexité de la demande. Étant donné que certains avis gonflent artificiellement le délai de traitement moyen, il est intéressant de préciser que la **médiane est respectivement de 4 (2019), 7,5 (2020), 8 (2021) et 11,5 (2022) jours**. **Nombre de demandes d'avis obtiennent donc une réponse dans la semaine ou dans les deux semaines**.

Tableau 6 : Nombre de dossiers de demandes d'informations sur le thème de la protection des données, selon l'origine du demandeur

Origine du demandeur	2019	2019 en %	2020	2020 en %	2021	2021 en %	2022	2022 en %
GPI	55	67,9	48	60,76	43	52,44	60	73,5
Citoyen	19	23,46	17	21,52	15	18,29	11	13,25
Instance policière	1	1,23	4	5,06	3	3,66	6	7,2
Autre instance	6	7,41	2	2,53	5	6,10	4	4,8
Parlementaire	-	-	1	1,27	-	-	-	-
Enquête d'office du COC	-	-	7	8,86	1	1,22	1	1,25
Avocat	-	-	-	-	3	3,66	-	-
Total	**81**	**100**	**79**[40]	**100**	**73**[41]	**100**	**82**	**100**

[40] Le nombre de demandes d'avis est légèrement supérieur au nombre d'avis étant donné que certains avis ont été sollicités par plusieurs demandeurs (par exemple par une autorité de police et par un service de police).
[41] Le nombre de demandes d'avis est légèrement supérieur au nombre d'avis étant donné que certains avis ont été sollicités par plusieurs demandeurs (par exemple par une autorité de police et par un service de police).

2.3. Avis au sujet de la législation et de la réglementation

Tableau 7 : Demandes sur la législation et de la réglementation entre 2018 et 2022 incluse

2018	2019	2020	2021	2022	Total
12[42]	22[43]	15	33	**39**	121

25. L'importante compétence d'avis sur les projets de réglementations (lois, arrêtés royaux, directives, …) ayant entièrement ou partiellement trait aux compétences du COC relève dans la grande majorité des cas des autorités fédérales (parlement ou gouvernement), mais peuvent aussi être des projets des entités fédérées (décrets, ordonnances, arrêtés des gouvernements fédérés, …).

26. Un point d'attention réside toujours dans le fait que les entités fédérées n'ont souvent pas le réflexe de solliciter également l'avis du COC lorsque les règles et la pratique de la gestion de l'information policière sont directement ou indirectement impactées. Le problème est encore plus cuisant lorsque les entités fédérées ne sollicitent pas non plus l'avis de l'APD et entravent ainsi le bon fonctionnement du mécanisme du guichet unique[44]. En 2022, ce problème s'est surtout posé pour des projets de réglementations des autorités flamandes, de sorte que le COC et souvent aussi la police elle-même découvrent seulement par la suite que de nouvelles réglementations flamandes ayant un impact sur le fonctionnement de la police et sur la gestion de l'information policière ont été adoptées.

27. En 2022, le COC a reçu **39 demandes d'avis** et a effectivement rendu **24 avis**. Pour les 15 autres demandes, il a été conclu après examen du texte qu'il n'était pas possible ou pas nécessaire de rendre un avis, (1) soit parce que le COC n'est pas compétent, (2) soit parce que par essence, le texte en question ne modifie en rien les règles en matière de gestion de l'information policière, (3) soit en raison du manque

[42] 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.
[43] *Ibidem.*
[44] Voir l'article 54/1 §1er, 2e alinéa de la LCA, en vertu duquel l'APD, dès que le demandeur coche sur le *« formulaire de demande d'avis relatif à un projet de texte normatif »* qu'il doit compléter, et plus précisément dans la partie II *« Vérification de la compétence de l'APD et objet de la demande »*, au point 4 *« Le projet concerne ou implique un (des) traitement(s) de données à caractère personnel effectué(s) par une ou plusieurs autorités ci-dessous »*, la case *« Services de police »* et/ou la case *« Inspection générale de la police fédérale et de la police locale »*, transmet le projet au COC pour qu'il puisse vérifier s'il peut ou doit rendre un avis.

de capacité du COC combiné au constat d'un impact plutôt marginal sur le fonctionnement de la police et la gestion de l'information policière. Vingt et une (21) demandes d'avis ont été transmises par l'APD dans le cadre du principe du guichet unique. 10 d'entre elles émanaient des entités fédérées, ce qui démontre la nécessité pour les entités fédérées de transmettre (également) leurs projets de réglementations pour avis à l'APD. Les 18 autres demandes ont été reçues directement de l'autorité sollicitant l'avis.

Au niveau de ces dossiers également, nous continuons à observer une **hausse du nombre de demandes d'avis et du nombre d'avis effectivement rendus**. Depuis 2018 et le lancement du COC en tant qu'autorité de protection des données, 2022 a été jusqu'ici l'année la plus chargée pour ce type de dossiers.

28. 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 (les instances administratives et judiciaires, la GPI, le monde académique, les organisations de la société civile, les ONG, etc. …) puissent en prendre connaissance. Parmi les thèmes importants qui ont ainsi été abordés, nous épinglerons l'approche administrative communale, l'interdiction d'accès aux domaines récréatifs, la liste des organes pouvant recevoir des informations et données à caractère personnel policières (cf. art. 44/11/9 de la LFP), la rétention des données, le système d'information Schengen (*SIS*) et le système d'entrée/de sortie (*Entry Exit System* ou *EES*), le Traité de Police Benelux de 2018, les traitements par caméra (dont la loi de réparation sur les *bodycams*), la publicité de l'administration, les traitements journalistiques, le DPO et le Registre des traitements de la GPI, etc. …

29. Ces avis sont préparés et rédigés par un membre du DIRCOM (le cas échéant avec l'aide d'un juriste ou un membre du DOSE/juriste), et font ensuite l'objet d'une discussion et d'une approbation au sein du DIRCOM. Les avis doivent être rendus dans un délai de 60 jours, ou de 15 jours en cas d'urgence. Un problème persistant est la transmission parfois tardive de la demande par l'APD dans le cadre du principe du guichet unique, qui fait que le COC ne dispose en réalité que rarement du délai de 60 jours.

2.4. Les plaintes

30. Les dossiers de plaintes peuvent être de deux types. Dans la majorité des cas, ils ont trait à des traitements prétendument illicites de la part de membres de la GPI. Ces plaintes sont introduites par des citoyens (ou par des membres de la GPI) qui présument qu'un membre de la GPI a consulté abusivement leurs données figurant dans les banques de données policières ou dans les banques de données tenues à disposition par le biais de PORTAL[45], ou a effectué d'autres traitements illicites.

Trois dossiers de plaintes ont été transmis par le Comité permanent P.

En 2022, le COC a aussi reçu pour la première fois une série de plaintes pouvant avoir trait à des thèmes divers mais portant toutes sur des traitements de données prétendument illicites. En 2021, le COC a ainsi reçu également 14 autres plaintes qui avaient trait par exemple à un traitement illicite dans le cadre de l'utilisation de caméras, à l'absence de notification d'une fuite de données, à l'utilisation d'un drone, au fait qu'un membre du personnel n'ait pas pu exercer son droit d'accès à son dossier personnel, etc. …

Tableau 8 : Nombre de dossiers de plaintes

Année	Traitement illicite par un membre de la GPI	Autre	TOTAL
2019	30	0	**30**
2020	26	14	**40**
2021	16	12	**28**
2022	23	6	**29**

Le nombre total de dossiers de plaintes semble se stabiliser aux alentours d'une trentaine par an. Le tableau ci-après présente la suite donnée à ces dossiers de plaintes par le COC:

[45] PORTAL est le portail d'accès général réservé aux membres de la GPI. Il s'agit du Registre national (RRN), du répertoire des véhicules (DIV) et du registre des armes.

<u>Tableau 9 :</u> Suite donnée par le COC aux dossiers de plaintes

Suite donnée	2020	2021	2022
Sans suite : COC pas compétent	5	4	6
Sans suite : plainte irrecevable[46]	3	3	4
Sans suite : pas d'objections	11	1	1
Sans suite : plainte manifestement non fondée	4	0	2
Sans suite : pas de coopération du plaignant	10	8	7
Sans suite : autre service déjà en charge du traitement	3	1	3
Sans suite : traitement non opportun[47]	4	1	2
Traitement conforme	3	4	7
Ordre de traitement conforme	0	2	0
Sous-traitant réprimandé	0	1	0
Avertissement au sous-traitant	2	0	0
Ordre de rectification	1	0	0
Ordre d'effacement	1	0	0
Ordre de limitation du traitement définitive	0	0	0
Transmission à la hiérarchie policière	7	0	4
Transmission au ministère public	3	0	1
Procès-verbal dressé	4	1	2
Mesure interne prise par la GPI	0	1	1
Ouverture d'une enquête disciplinaire	5	1	2
Total	**66**	**28**	**42**

31. Le traitement des plaintes est venu s'ajouter aux missions du COC depuis sa réforme en une autorité de protection des données. Vu le fort coefficient de travail de ces dossiers, la capacité limitée du Service d'Enquête (3 ETP) et les compétences du COC, nous nous limitons explicitement aux éventuels traitements illicites de données (généralement des consultations) par un fonctionnaire de police. Le COC procède dans ce contexte à une enquête *prima facie*. Dès qu'un 'suspect' potentiel peut être localisé dans le temps/l'espace, le dossier est en principe – à moins qu'il ne nécessite un

[46] Par exemple parce qu'il s'est finalement avéré que la plainte n'était pas dirigée contre un fonctionnaire de police.
[47] Par exemple en raison d'une enquête disciplinaire ou pénale en cours dans laquelle le COC ne souhaite pas s'immiscer.

traitement par le COC lui-même – transmis au chef de corps/directeur. Le COC peut aussi le transmettre directement au ministère public compétent[48](en fonction par exemple de la gravité de l'infraction), mais cela n'arrive pas souvent étant donné que le COC a en principe – et doit d'ailleurs avoir – confiance en la qualité du traitement policière interne.

32. Il n'empêche que le COC vérifie toujours quelle décision finale le corps prend, et que ce suivi est absolument nécessaire. Le COC a en effet dû constater à plusieurs reprises – et c'est alarmant – que la GPI entretient en ce qui concerne l'alimentation de la BNG dans le sillage de consultations illicites des banques de données par des fonctionnaires de police certains usages ou habitudes dérogatoires et illicites avantageant les auteurs de ces irrégularités. Il arrive ainsi qu'il ne soit tout simplement pas établi de procès-verbal, ou qu'un procès-verbal soit établi mais pas saisi dans la BNG, ou encore qu'un procès-verbal soit saisi formellement dans la BNG mais soit particulièrement difficile à retrouver[49]. Il s'agit là d'un exemple d'une culture plus répandue au sein de la police qui consiste à se montrer sévère envers les citoyens, mais à faire manifestement preuve de davantage de clémence à l'égard des comportements déviants ou tout simplement illicites (et/ou punissables) des membres du corps de police.

33. Le délai de traitement moyen des dossiers de plaintes a diminué de 238,6 jours en 2019 (médiane : 230 jours) à 96,66 jours (médiane : 46,5 jours) en 2020, 74 jours (médiane : 46,5 jours) en 2021 et 73,08 jours (médiane : 49 jours) en 2022. Ici aussi, la réduction/stabilisation des délais de traitement se poursuit donc. Des 29 plaintes reçues en 2022, 25 avaient été traitées en avril 2023.

2.5. Les brèches de sécurité (databreach)

34. En 2022, 25 brèches de sécurité ont été notifiées au COC par des entités de la GPI. Il s'agit du nombre le plus élevé recensé depuis le lancement de l'Organe de

[48] Il s'agit en effet également toujours d'infractions (et au moins d'une infraction à l'article 151 du Code pénal et à l'article 222, 1° de la LPD).
[49] Pour les initiés à la technique de la BNG : c'est ce qui se produit lorsque les liens requis ne sont pas établis entre les entités 'fait/DOS' et 'personne'.

contrôle en tant qu'autorité de protection des données. Il doit s'agir d'infractions dites 'CIA', à savoir des infractions ayant des retombées sur la Confidentialité (C), l'Intégrité (I) et *l'Availability* (A, la disponibilité) des données à caractère personnel.

Ces dossiers peuvent être complexes, de sorte que le COC ne dispose de toute façon pas de la capacité suffisante pour examiner les infractions sur le fond étant donné qu'il ne dispose que d'un seul ETP informaticien. En 2022, le COC s'est retrouvé sans informaticien à partir du 1er août. Le COC examine uniquement si l'infraction a été correctement traitée et si toutes les mesures requises ont été prises avant et après la survenance de l'infraction pour empêcher que de telles infractions se reproduisent encore et pour limiter le plus possible les effets préjudiciables.

Concrètement, il s'agit de cas de *hacking*, de *ransomware*, de perte d'un appareil ou de documents sur papier, d'e-mails envoyés au mauvais destinataire, d'e-mails contenant des informations ou pièces jointes qui n'auraient pas dû s'y trouver, de phishing ciblé, de diffusion non autorisée (de photos, d'images, …), de divulgation en ligne d'informations non publiques (informations de l'intranet), d'accès trop étendus ou non autorisés, de mots de passe compromis, d'abus de droits d'accès, de transferts de données non autorisés, etc. …

Tableau 10 : Nombre brèches de sécurité notifiées

2018	2019	2020	2021	2022	Total
6	17	17	20	**25**	85

2.6. Les enquêtes internationales

35. Le COC est souvent sollicité pour prendre part à des enquêtes ou visites internationales. Vu notre capacité limitée, le DIRCOM a décidé comme il l'avait déjà fait en 2020 et 2021 de ne pas prendre part à des enquêtes internationales en 2022. Vu qu'il existe en revanche au niveau de l'UE, et en particulier pour les évaluations SCHEVAL, un manque permanent de candidats pour composer les équipes internationales requises, le COC prendra part à au moins 1 évaluation SCHEVAL en 2023, à savoir celle de la Lettonie.

2.7. Protection des données dans des secteurs et matières spécifiques

2.7.1. Contrôle spécial : les contrôles BELPIU

36. Dans le cadre de l'application de la loi du 25 décembre 2016 relative au traitement des données des passagers (la 'loi PNR') et de la mission de contrôle du COC, il a été procédé en 2022 à une visite et à un contrôle spécial auprès de l'Unité Belge d'informations de passagers (l'UIP of *BELPIU*).

Il a été décidé d'axer le contrôle sur l'efficacité du traitement des données des passagers. Le COC s'est pour ce faire limité à la police intégrée (GPI) étant donné qu'il est uniquement compétent pour les traitements policiers de l'UIP.

La Commission européenne s'est déjà livrée à un exercice de révision de la directive PNR[50]. Un exercice similaire sera réalisé à l'échelle de la Belgique pour la loi PNR. Pour cette raison, le contrôle s'est concentré sur la question de la plus-value de la banque de données des passagers en comparaison d'autres méthodes d'enquête, et de la proportionnalité du traitement de données à grande échelle compte tenu de l'ingérence profonde qu'il implique dans la vie privée.

Le contrôle et l'enquête ont en l'occurrence été limités à trois domaines:

1. point de la situation et suivi d'une partie du rapport de contrôle de 2020, dont l'établissement des profils;
2. l'efficacité et la proportionnalité de la banque de données des passagers (la question centrale de l'enquête);
3. les requêtes ciblées et les demandes de recherche ciblée.

37. Dans le cadre du suivi du rapport de contrôle de 2020, le COC constate que l'UIP a dans l'intervalle donné suite aux recommandations dudit rapport. Il ressort par ailleurs des procédures internes de l'UIP que celle-ci prête attention à la protection

[50] Rapport de la Commission au Parlement européen et au Conseil sur le réexamen de la directive (EU) 2016/681 https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2020:0305:FIN:FR:PDF

des données et veille à offrir des garanties additionnelles en vue de la minimalisation des données.

L'enquête menée par l'Organe de contrôle quant à l'efficacité de la banque de données des passagers met clairement au jour un certain nombre de problèmes susceptibles de miner l'efficacité du système PNR. Il arrive notamment que les *matches* (*hits* validés) soient transmises trop tard ou soient reçues trop tard par le service de police intervenant, que les données de passagers transmises ne soient pas toujours exactes, et que moins d'interventions policières soient effectuées en raison de la politique d'action actuelle d'une entité de police donnée.

Cela a d'une part un impact sur l'efficacité de la finalité poursuivie par la banque de données des passagers, à savoir la lutte contre le terrorisme et les formes graves de criminalité. D'autre part, cela conduit dans certains cas à des situations dans lesquelles des personnes font à tort l'objet d'une enquête qui ne les concerne en réalité pas, ou sont à tort interceptées par la douane ou par la GPI à l'aéroport. La cause des problèmes constatés est généralement extérieure à l'UIP. Pour une part, ces problèmes sont en effet également dus à la qualité des données enregistrées dans la Banque de données nationale générale (BNG), une problématique que l'Organe de contrôle a déjà épinglée à plusieurs reprises.

Il est difficile à ce stade d'apporter une réponse objective à la question de savoir si la banque de données des passagers a une plus-value mesurable dans des informations pénales. S'il est vrai que l'on pourrait répondre par l'affirmative à cette question en se basant sur le rapport annuel de l'UIP, notamment sur la base des *hits* (générés à partir de profils) et des résultats communiqués à l'UIP par les destinataires des *hits*, il n'est pas possible actuellement de formuler une réponse claire en ce qui concerne l'efficacité de ce système dans le cadre de l'investigation, par la police, des phénomènes de terrorisme et des formes graves de criminalité. Les éléments représentatifs (chiffres) ne sont en effet pas suffisants, principalement en raison de l'absence d'informations concernant l'utilisation des données PNR dans le processus de traitement de l'information ou de l'instruction judiciaire.

Compte tenu des éléments qui précèdent, il convient donc de procéder à une évaluation politique de l'efficacité de la banque de données des passagers. Il y a lieu de renvoyer ici au récent arrêt du 21 juin 2022 de la Cour de Justice de l'Union européenne (arrêt de la Cour dans l'affaire C-817/19, *Ligue des droits humains*), dans lequel la Cour indique notamment que les droits fondamentaux exigent que les compétences de traitement prévues par la directive PNR ne peuvent être exercées que dans la mesure où c'est strictement nécessaire. Lorsqu'un État membre ne fait pas face à une menace terroriste qui s'avère réelle et actuelle ou prévisible, le droit de l'Union s'oppose à la législation nationale en vertu de laquelle les données PNR doivent être transmises et traitées pour les déplacements effectués au sein de l'Union européenne en avion et avec d'autres formes de transport. Cet arrêt nécessitera en tout état de cause une révision approfondie de la réglementation belge ainsi que du fonctionnement de l'UIP.

Enfin, l'Organe de contrôle constate que les membres détachés des services de police endossent une double fonction et accomplissent donc aussi des devoirs d'information et d'enquête et établissent des procès-verbaux et/ou des rapports confidentiels. Or, il s'agit là d'un traitement policier qui semble aller plus loin que la compétence du fonctionnaire de police détaché auprès de l'UIP telle qu'elle est strictement réglementée par la loi PNR, et qui doit donc de l'avis du COC être considéré comme problématique d'un point de vue juridique. Le COC appelle donc le législateur à apporter la clarté nécessaire dans la loi PNR, compte tenu de la délimitation des finalités de la directive PNR.

2.7.2. Contrôle spécial : les réquisitions fiscales de l'AGD&A à la BELPIU

38. Le COC a été investi en 2019 d'une nouvelle compétence à l'égard du service Recherche des Douanes dans le cadre des réquisitions adressées à la BELPIU dans des matières fiscales. L'article 281 §4[51]de la loi générale sur les douanes et accises du

[51] « *§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.

18 juillet 1977 prévoit 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 jusqu'ici toujours de dossiers de fraude aux droits d'accises à travers la contrebande de cigarettes. La réquisition et la motivation doivent être portées à la connaissance de l'Organe de contrôle. L'Organe de contrôle interdit au conseiller général d'utiliser les données collectées dans des circonstances non conformes aux conditions légales. En 2022, seule 1 demande de recherche ciblée a été adressée au COC. Pour la première fois, le COC n'a **pas** constaté l'absence de motivation de l'utilisation de toutes les données des passagers demandées.

2.7.3. L'Inspection générale de la police fédérale et de la police locale

39. En 2022, le COC n'a pas mené d'enquêtes spécifiques concernant l'AIG. La compétence du COC est ici partagée avec l'APD en ce sens que le COC est uniquement compétent pour les traitements de données opérationnels policiers de l'AIG (ceux qui relèvent de la *LED* et du titre 2 de la LPD). Cette institution, qui endosse elle-même un rôle de surveillance, n'a jusqu'ici pas été une priorité pour le COC et n'est, pour des raisons de capacité, sans doute pas près de le devenir à l'avenir.

2.8. Utilisation de caméras par les services de police

2.8.1. Généralités

40. Le COC est investi d'une mission 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), tant visible que non visible (cachée).

Vu l'explosion 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. En revanche, l'utilisation de caméras est souvent examinée par le COC lors de chaque contrôle proactif – une catégorie de

---

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. »

contrôles dont la fréquence a malheureusement diminué en 2022 (voir plus loin) – effectué auprès d'une entité de police donnée.

41. Une problématique réelle demeure en 2022 également le fait que depuis l'entrée en vigueur de la LPD le 5 septembre 2018, le devoir de notification au COC qui est prévu de la part de la police pour les utilisations non visibles de caméras semble n'être pour ainsi dire pas respecté, de sorte que le COC ne dispose pas d'un aperçu (suffisant) de ce type d'utilisation de caméras. Le COC soupçonne dès lors l'existence d'un *dark number* substantiel pour l'utilisation non visible de caméras à des fins administratives.

Le fait qu'à peine trois (3) notifications aient été effectuées[52], c'est-à-dire autant qu'en 2021, combiné à l'absence d'enregistrement dans le registre des traitements REGPOL, **peut tout simplement être qualifié de problématique**. Cette remarque, qui avait déjà été formulée dans le rapport d'activité de 2021, n'a manifestement pas enjoint la GPI ni l'autorité de tutelle à une quelconque action ou réflexion. Ce constat est illustratif d'un phénomène plutôt récurrent selon lequel la police se croit apparemment autorisée à ignorer certaines prescriptions légales (voir aussi la remarque formulée au point 32).

2.8.2. Demandes d'informations et d'avis concernant l'utilisation de caméras

42. Nombre de questions et demandes concernant l'utilisation de caméras sont (principalement) soumises par la GPI au COC. Entre le 25 mai 2018 (date de l'entrée en vigueur des nouvelles dispositions relatives à l'utilisation de caméras) et la fin 2022, le COC a reçu 134 demandes d'avis concernant cette thématique.

[52] Concrètement par les zones de police Brugge, Noorderkempen et Tournaisis.

<u>Tableau 11 :</u> Nombre de demandes d'avis ou d'informations concernant l'utilisation de caméras

Année	**Nombre**
2019	**32**
2020	**29**
2021	**29**
2022	**32**
TOTAL	**134**

43. Parmi les thèmes abordés figurent les questions relatives à l'utilisation de *bodycams*, au partage d'images de caméras avec par exemple des communes, à l'utilisation de drones, à la compétence des Conseils communaux, à l'utilisation de caméras lors de fouilles, à la surveillance par caméra dans les cellules et dans les bâtiments de police, à l'utilisation de caméras dans les fourgons cellulaires, etc. …

44. À cela s'ajoutent – également à fort coefficient de travail – les analyses d'impact relatives à la protection des données ou ***AIPD***[53] qui ont trait à des traitements par caméra et qui sont soumises au COC par les entités de police pour consultation préalable.

45. En 2022, un total de **28 AIPD** ont été soumises pour analyse au COC dans le cadre de l'utilisation de caméras par la police. Deux l'ont été en exécution d'une mesure correctrice imposée, dont une avait trait à une banque de données technique locale. En principe, chaque dossier ne contient qu'une seule analyse, mais peut aussi en comporter plusieurs lorsqu'une zone de police transmet par exemple plusieurs AIPD à la fois (par exemple une pour l'utilisation de caméras mobiles et une pour l'utilisation de caméras fixes).

Il arrive parfois qu'une analyse soit précédée d'une concertation (en *Teams*) entre le COC et le service de police afin de pouvoir mieux la préparer. Plusieurs AIPD qui s'assortissaient initialement d'un score ou d'une évaluation moins favorable ont été parcourues avec le DPO afin de contextualiser les remarques du COC, même s'il n'était pas nécessaire de soumettre une deuxième version au COC. Ces sessions de *coaching*

[53] En anglais *DPIA* pour *Data Protection Impact Assesment*.

du COC ont été organisées principalement sous la forme d'appels *Teams*, en présence ou non de juristes ou de l'informaticien du COC. Étant donné qu'il s'agit en principe d'analyses *prima facie*, l'attention se focalisait essentiellement sur des aspects juridiques fonctionnels, et moins sur les détails relatifs aux aspects des technologies de l'information et de la communication (aussi en raison de la capacité limitée du COC dans cette matière). Le délai de traitement moyen d'une analyse *prima facie* était en 2022 de **84,22 jours** (médiane: **42 jours**), du fait qu'un dossier n'est pas toujours clôturé immédiatement à l'issue de la première analyse vu ce que nous expliquions plus haut au sujet du *coaching*. Il est à noter qu'une seule AIPD a à nouveau dû être considérée comme inacceptable après une seconde analyse, ce qui signifie qu'il est toujours dûment tenu compte des remarques formulées par le COC et que certaines des zones de police qui établissent l'AIPD manifestent une nette volonté d'optimaliser la qualité.

Tableau 12 : Nombre d'AIPD soumises pour avis au COC concernant l'utilisation de caméras

Année	**Nombre**
2019	**27**
2020	**10**
2021	**33**
2022	**28**

Tableau 13 : Nombre d'AIPD[54]soumises pour avis au COC selon le type d'utilisation de caméras

AIPD par type de caméra	**2021**	**2022**
Caméras ANPR (fixes, fixes temporaires, mobiles), combinées ou non avec une banque de données technique	8	5
Bodycams	11	6
Drones	3	2
Caméras fixes ou caméras fixes temporaires	11	15
Total	33	**28**

[54] En anglais *DPIA* pour *Data Protection Impact Assesment*.

Tableau 14 : Évaluation *prima facie* des AIPD soumises en 2022

Résultats des analyses *prima facie*	**2020**	**2021**	**2022**
Acceptable *prima facie*	1	0	0
Acceptable *prima facie* avec remarques	5	12	13
Acceptable *prima facie* avec conditions contraignantes	1	8	6
Inacceptable *prima facie*	2	7	1
Second avis du COC – acceptable	0	3	0
Second avis du COC – acceptable avec remarques	1	3	0
Second avis du COC – inacceptable			1
Total	10	33	21[55]

46. La méthodologie pratiquée depuis la mi-2020 par le COC consiste à analyser les AIPD soumises par les services de police eux-mêmes pour vérifier qu'elles répondent à un certain nombre de critères en fonction du type de caméra, éventuellement en fournissant une explication en fonction de la présence ou de l'absence de ces critères. Le cas échéant, des remarques additionnelles sont ajoutées. La décision prise par le COC reflète ainsi le résultat d'une analyse *prima facie* et ne constitue donc pas (encore) un avis formel au sens de l'article 59 de la LPD. Sur la base de cette analyse, le service de police décide ensuite d'amender ou non l'AIPD et/ou d'ajuster le traitement projeté. Il peut en découler un second avis *prima facie*. S'il n'est pas satisfait aux conditions contraignantes imposées par le COC ou s'il est procédé au traitement en dépit de son caractère inacceptable, le COC émettra un avis formel sur la base de l'article 59 de la LPD. Cela n'a encore jamais été le cas jusqu'ici.

2.8.3. Quelques enquêtes spécifiques

47. 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 mais qui se sont en 2022 retrouvées fortement sous pression en raison du volume croissant de travail réactif, le COC tente également de réserver une certaine capacité (ou procède à des glissements de cette capacité) pour pouvoir réagir à des évolutions actuelles. En **2019**, il y a par

[55] Sept (7) AIPD soumises étaient encore en cours de traitement au moment de la clôture du présent rapport d'activité.

exemple eu l'enquête avec mesure correctrice menée au sujet de l'utilisation de caméras permettant la reconnaissance faciale (*FRT*[56]) à l'aéroport de Bruxelles-National par la police fédérale, à laquelle le COC a mis un terme. En **2020**, il s'agissait notamment (1) d'une enquête concernant l'utilisation de drones par la ZP CARMA[57]et d'un avis relatif au cadre légal et à l'utilisation de *bodycams*[58]. En **2021**, il s'agissait de plusieurs contrôles spéciaux axés sur le thème de l'utilisation de caméras par la police, dont les rapports/avis ont toutefois été publiés seulement en **2022**. Il s'agissait (1) d'une enquête de contrôle à l'échelle de la GPI concernant l'utilisation de drones, à savoir le *«Contrôle thématique et avis d'initiative DIO20009-1 du 15 mars 2022 relatifs à l'utilisation, par la police intégrée, de caméras montées sur des drones»*, dont l'objectif était de fournir à la GPI et aux instances de police des recommandations concernant l'utilisation de drones[59]. Il convient ensuite de citer le *«Rapport de contrôle et de visite du 29 mars 2022*[60]*concernant l'enregistrement et/ou l'écoute, par la police, de la concertation confidentielle entre le suspect et l'avocat»*, dans le cadre duquel le COC a, en 2021 et durant une partie de 2022, réalisé à la demande des ministres compétents pour la police une enquête à l'échelle de la GPI concernant la surveillance audiovisuelle de la concertation confidentielle au moyen de caméras. Le rapport comporte une série de constatations et formule un certain nombre de recommandations devant établir clairement dans quelles circonstances et sous quelles conditions une surveillance par caméra peut ou non être exercée à des fins de sécurité pendant la concertation confidentielle. Dans le sillage de ce rapport, le Collège des procureurs généraux a diffusé une circulaire mettant en œuvre ces recommandations du COC[61].

---

[56] *Facial Recognition Technology*.
[57] Rapport avec mesure correctrice DIO20009 du 23 décembre 2020 concernant la visite effectuée auprès de la zone de police CARMA par l'Organe de contrôle de l'information policière dans le cadre de l'utilisation de drones en vue du contrôle du respect des mesures visant à limiter la propagation du Coronavirus - COVID-19, www.organedecontrole.be.
[58] Rapport et avis CON190008 du 8 mai 2020 suite aux constatations dans le cadre d'une enquête sur l'utilisation de *bodycams*, www.organedecontrole.be.
[59] www.organedecontrole.be/publications/rapports.
[60] Rapport de contrôle et de visite DIO21002 du 29 mars 2022 de l'Organe de contrôle de l'information policière concernant l'enregistrement et/ou l'écoute, par la police, de la concertation confidentielle entre le suspect et l'avocat, www.organedecontrole.be.
[61] Circulaire 9/2022 du 11 juillet 2022 – Addenda 6 à la circulaire 8/2011 relative à l'organisation de l'assistance d'un avocat dès la première audition dans le cadre de la procédure pénale belge – L'enregistrement et/ou l'écoute par la police de la concertation confidentielle entre le suspect et l'avocat, www.om-mp.be.

2.9. L'exercice des compétences correctrices

48. Le COC peut ordonner à la GPI de poser certains actes/d'effectuer certains traitements ou de renoncer (à l'avenir) à certains traitements. Il s'agit des 'compétences correctrices' (article 247 de la LPD) par lesquelles le COC se distingue de toutes les autres autorités de contrôle compétentes pour la police. Vu leur impact sur le fonctionnement opérationnel des services, l'exercice de ces compétences s'entoure de la circonspection de mise. D'une part, le COC 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. Cet exercice d'équilibre est à la fois difficile et délicat.

Cela signifie que le COC applique pour certaines irrégularités constatées une politique de tolérance. 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. L'expérience nous apprend que la GPI, après une simple communication indiquant que le COC peut agir et agira le cas échéant de manière correctrice, se conforme dans la grande majorité des cas aux remarques du COC, rendant ainsi inutile une mesure correctrice formelle.

2.9.1. Les mesures correctrices prises

49. Les mesures correctrices se déclinent sur toute une gamme pouvant aller d'une réprimande à une interdiction temporaire ou définitive du traitement, en passant par un avertissement officiel indiquant qu'un traitement est illicite ou la suspension d'un certain flux de données.

En 2022 également, le COC a formulé à la fois des **requêtes**, des **recommandations** et des **mesures correctrices**. Les **requêtes** sont plutôt des suggestions que le COC émet pour optimaliser le fonctionnement (par exemple des bonnes pratiques), tandis que les **recommandations** revêtent, comme le nom l'indique, un caractère un peu plus contraignant (sans pour autant être vraiment contraignantes du point de vue juridique) et s'assortissent généralement d'un délai de mise en œuvre fixé par le COC. Quant aux **mesures correctrices**, elles sont le moyen prévu par la LPD pour permettre au COC d'agir de manière contraignante.

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

Tableau 15 : ***Décisions prises dans les enquêtes de contrôle***

Décisions prises dans les enquêtes de contrôle	**2020**	**2021**	**2022**
Requêtes[62]	1	36	7
Recommandations	80	33	7
Mesures correctrices	26	32	9
TOTAL	107	101	23

50. La diminution du nombre de décisions prises dans des enquêtes de contrôle en 2022 est due à plusieurs causes, dont :

- la pression croissante des activités réactives, à savoir:
    - l'augmentation du nombre d'avis concernant des projets de réglementations;
    - le grand nombre d'avis/d'AIPD ayant trait à l'utilisation de caméras (dont certains d'une envergure substantielle, notamment concernant *PoliceSearch*@GPI). On constate dans ce contexte qu'il est parfois fait appel (abusivement) au COC pour trancher des discussions internes à la GPI (par ex. la collecte de données par l'Inspection générale dans le cadre du contrôle de l'application de la directive MFO-2, le fait de n'effacer ou de n'archiver des données que lorsque le COC en donne 'l'ordre', le fait d'utiliser le COC comme 'juriste' pour contester des questions ayant trait à la tutelle budgétaire administrative, etc. …);
    - les demandes adressées au COC en vue de participer à des formations de la GPI;

[62] La pratique consistant à demander aussi tout simplement certaines réalisations n'a été vraiment lancée qu'en 2021, ce qui explique le nombre réduit en 2020.

    - l'augmentation persistante et le volume important des dossiers d'accès indirect;
    - les nouvelles missions comme la validation des statistiques de la BNG en matière de rétention des données (voir plus loin) (2 semaines entières à raison de 5 ETP);
    - les difficultés de recrutement rencontrées par le COC;
    - la capacité monopolisée par le suivi des requêtes, recommandations et mesures correctrices formulées dans le passé;
- la capacité de toute façon limitée du COC, dont les membres et les membres du personnel peuvent aussi être absents en cas de congé, de maladie, de difficultés à trouver un remplaçant[63], etc. …
- Conformité informelle afin que le COC n'ait pas à prendre des mesures correctrices formelles.

[63] Le COC a ainsi dû se passer d'informaticien pendant une demi-année en 2022.

Un examen des mesures correctrices prises en 2022 révèle la répartition suivante :

Tableau 16 : ***Types de mesures correctrices prises dans les enquêtes de contrôle***

Mesures correctrices prises dans les enquêtes de contrôle[64]	**2020**	**2021**	**2022**
Avertissement	3	2	1
Réprimande	1	0	1
Ordre de mettre le traitement en conformité avec les règles en matière de protection des données	21	26	6
Interdiction du traitement	1	1	8
Limitation définitive du traitement	-	1	0
Limitation temporaire du traitement	-	1	0
Total	26	31	16

[64] Il convient de souligner que le COC prend évidemment aussi des mesures correctrices dans le cadre des autres types de dossiers, comme les demandes d'accès indirect et les plaintes. Les statistiques y afférentes sont reprises plus haut dans le présent rapport d'activité.

2.9.2. Les recours judiciaires contre les décisions du COC

51. En **2021**, un jugement a été prononcé par le Président du Tribunal de première instance de Bruxelles (procédure en référé) dans deux dossiers dans lesquels le COC avait été cité en tant que défendeur.

Tant dans l'ordonnance du 17 mai 2021[65] que dans celle du 10 décembre 2021[66], prises chacune par un Président différent, la vision du COC a été suivie et les diverses demandes ont donc été rejetées.

En **2022**, la chambre francophone de la Cour d'appel de Bruxelles a posé à travers son arrêt du 9 mai 2022 rendu dans le premier dossier (ordonnance du 17.05.2021) deux questions préjudicielles à la Cour de Justice de l'Union européenne (voir le point 21), qui fera – espérons-le – pour l'avenir la clarté sur cette problématique. Le COC s'attend tout de même à ce que la Cour de Justice se livre à un examen critique du système belge de l'accès indirect pour le citoyen – unique au sein de l'UE et par ailleurs obligatoire. Dans le deuxième dossier (ordonnance du 10.12.2021), la 1re chambre francophone de la Cour d'appel de Bruxelles a rejeté dans son arrêt du 3 octobre 2022 la demande initiale comme irrecevable en l'absence d'intérêt, donnant ainsi gain de

[65] Président du Tribunal de première instance de Bruxelles, 17 mai 2021, dans le dossier ASBL *Ligue des Droits Humains* et D.D. contre l'Organe de contrôle, *non publiée*.
[66] Président du Tribunal de première instance de Bruxelles, 10 décembre 2021, dans le dossier Y.K. contre l'Organe de contrôle, *non publiée*.

cause au COC[67].

Il s'agissait dans les deux cas d'une discussion de principe sur la question de savoir s'il existe un moyen de droit (suffisant) contre le COC ou son verdict dans le cadre des demandes d'accès indirect (voir plus haut). L'Organe de contrôle se substitue en effet dans cette procédure à la personne concernée pour exercer (indirectement) ses droits, de sorte qu'il ne prend pas véritablement une 'décision'. La réponse légalement obligatoire du COC (selon laquelle il a été procédé aux *« vérifications nécessaires »*) constitue régulièrement une source de frustration et peut donc potentiellement mener à des procédures judiciaires, comme cela a donc été le cas à deux reprises. La personne concernée a évidemment le droit d'intenter une action en justice, mais dans ce cas contre le responsable du traitement légal (ou fonctionnel) lui-même (à savoir les ministres compétents pour la police et/ou les chefs de corps de la police fédérale ou le dirigeant de la police fédérale) et les enregistrements policiers qu'il a effectués.

52. En **2022**, la Cour d'appel d'Anvers a statué dans son arrêt du 12 décembre sur le recours introduit en 2021 par la zone de police Regio Turnhout contre certaines mesures correctrices (pas toutes) que le COC avait imposées à l'issue d'un contrôle technique effectué dans cette zone de police frontalière. Il s'agit toujours de la seule fois qu'une entité de police a contesté en justice une mesure correctrice du COC. Le COC n'a pas obtenu gain de cause dans ce dossier et les trois mesures correctrices (dont seulement une était cependant encore effectivement en vigueur) ont été annulées par la Cour d'appel d'Anvers.

Le COC s'est pourvu en cassation contre cet arrêt en 2022. De l'avis du COC, l'arrêt de la Cour d'appel d'Anvers, en plus d'être peu convaincant dans ses motifs, confronte également le COC à de graves problèmes de fonctionnement. La Cour reproche au COC d'avoir ignoré dans sa décision les droits de la défense, le principe de diligence et le principe de *fairplay*. Elle en arrive à cette conclusion dès lors qu'elle impose une séparation rigoureuse entre la fonction d'investigation et la fonction de décision des différents organes du COC (s'inspirant à cet égard sans aucun doute des allusions permanentes à l'APD) et qu'elle reproche par essence aux membres du DIRCOM

[67] Bruxelles, 3 octobre 2022, en cause de Y.K. contre l'Organe de contrôle, *non publié*.

d'avoir pris part à la phase d'investigation avant d'avoir décidé des mesures correctrices.

Si cette vision n'est d'une part prescrite par aucune disposition légale, constitutionnelle ou conventionnelle, elle revient d'autre part surtout à une négation des termes clairs de la loi, qui confère bel et bien les pleins pouvoirs d'investigation et de décision aux membres du COC (autrement dit, aux membres du DIRCOM). Il suffit de lire le Chapitre III du Titre 7 de la LPD pour constater qu'il n'est pas établi de distinction entre les pouvoirs d'investigation des membres et ceux du Service d'Enquête. Il est incompréhensible que la Cour ignore ces articles de loi. La séparation qu'elle exige n'est prescrite nulle part dans la LPD, ni même suggérée; même les travaux préparatoires de la LPD n'en font aucune mention. Si la Cour de cassation suit la position de la Cour d'appel, il ne restera plus qu'à réécrire les articles de la LPD relatifs à l'Organe de contrôle et à augmenter sensiblement la capacité du COC …

3. LES ACTIVITÉS RELEVANT PRINCIPALEMENT DU CONTRÔLE

3.1. Les enquêtes de contrôle menées auprès de la GPI

3.1.1. Généralités

53. Cette mission relève de l'activité principale du COC depuis sa création en 1998. L'accent était dans ce contexte mis à la fois sur les aspects de la licéité, de l'efficacité et de l'efficience de la gestion de l'information et sur la composante de la protection de la vie privée et des données. Il convient de faire remarquer que les enquêtes de contrôle initiées les années précédentes monopolisent toujours de la capacité en 2022 étant donné que le COC est évidemment aussi tenu d'assurer un suivi des requêtes, des recommandations et surtout des mesures correctrices qu'il a formulées et pour lesquelles il a très souvent fixé un certain délai de mise en œuvre. Ce suivi requiert lui aussi immanquablement de la capacité. Les enquêtes de contrôle sont généralement initiées d'office mais peuvent aussi découler d'une demande des instances administratives ou judiciaires.

54. Le COC catégorise comme suit les enquêtes de contrôle :

- un **contrôle global** est un contrôle qui s'assortit d'une ou plusieurs visites approfondies sur place et d'une portée très large ;

- un **contrôle technique** est un contrôle qui se concentre sur la licéité, l'exhaustivité et l'exactitude des enregistrements/traitements effectués dans les banques de données policières et qui porte surtout sur l'efficacité opérationnelle et l'exactitude des enregistrements effectués dans les banques de données. Il peut aussi arriver qu'un contrôle technique ait trait à un problème plutôt ponctuel ;
- un **contrôle thématique** consiste à mener une enquête sur un thème déterminé qui peut inclure à la fois de la *desk research* et des visites sur place ;
- un **contrôle restreint** porte sur un seul ou sur quelques aspects (partiels) d'un traitement de données policier ou non policier ;

- un **contrôle international** désigne les enquêtes internationales auxquelles le COC apporte son concours ;
- un **contrôle spécial** est un contrôle portant sur des matières particulières, comme les contrôles annuels des banques de données communes terrorisme et extrémisme ou les enquêtes *BELPIU*.

Un contrôle technique se penche notamment en détail sur les thèmes suivants :

- banques de données particulières ;
- contrôle et utilisation des fichiers de journalisation ;
- BNG et option 35[68] ;
- triptyque[69] ;
- utilisation de caméras ;
- fonctionnement *ANPR* ;
- …

55. Parmi les thèmes récurrents de telles enquêtes de contrôle, on retrouve notamment:

(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 et autres banques de données policières (qualité de l'alimentation, respect des délais de conservation, communication à des tiers, …);

(3) utilisation visible et non visible (cachée) de caméras;

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

(5) utilisation d'équipements IT personnels à des fins opérationnelles, ou d'équipements professionnels à des fins privées;

[68] On entend par « option 35 » le transfert normal des données de l'*ISLP* vers la Banque Nationale Générale (BNG).
[69] Le triptyque consiste à relever les empreintes digitales et palmaires, à prendre des photos et à établir le signalement individuel afin de permettre l'identification d'une personne.

(6) traitement de données biométriques ou d'autres catégories particulières de données, ou utilisation de nouvelles technologies;

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

(8) etc. …

La version publique[70]des rapports est disponible pour consultation sur le site www.organedecontrole.be, dans la rubrique Publications.

3.1.2. Aperçu des principales enquêtes de contrôle

56. Certaines enquêtes de contrôle peuvent durer relativement longtemps du fait que le COC consacre du temps à leur suivi, et aussi parce que la police sollicite régulièrement un report d'exécution. L'objectif est de clôturer le suivi dans l'année, mais il s'avère que ce n'est pas toujours possible.

57. Voici un aperçu des enquêtes de contrôle **initiées** en 2022 :

- Contrôle thématique relatif à la coopération policière entre la Belgique et la Turquie – Enquête sur les flux de données policières entre les services de police et les autorités turques pour des finalités opérationnelles (CON22008).
- Contrôle restreint relatif aux processus suivis par la police intégrée, structurée à deux niveaux (GPI) pour l'enregistrement en BNG de mesures faisant suite à une condamnation pour infraction routière (CON22007).
- Contrôle thématique relatif à L'enregistrement et l'exploitation en BNG par les services de police intégrée, structurée à deux niveaux (GPI) de données et informations relatives à des faits de fraude à l'identité dans le cadre de l'exercice de leurs missions de police administrative et de police judiciaire (CON22006).

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

- Contrôle restreint auprès de la zone de police Bruxelles-Ouest concernant la saisie dans la BNG des infractions à la législation visant à limiter la propagation du coronavirus commises par des membres du personnel (CON22005).
- Contrôle thématique relatif au *Real Time Intelligence Centre* du CIC de Flandre orientale et à l'application d'OSINT police administrative (CON22003).
- Contrôle thématique relatif à l'exécution de l'enquête de moralité dans le cadre du recrutement et de la sélection de candidats pour le cadre opérationnel et administratif et logistique de la police intégrée, structurée à deux niveaux (GPI) (CON22002).
- Contrôle restreint auprès de la zone de police de Zwijndrecht concernant une brèche de sécurité (DIO22010).
- Contrôle restreint relatif à la mise en œuvre de projets pilotes dans le cadre de la problématique de l'utilisation du GSM au volant (DIO22009).
- Contrôle restreint relatif au signalement en BNG de mesures relatives au prélèvement ADN à la suite d'une condamnation (art. 5 §2 de la loi du 22 mars 1999 sur l'ADN) (DIO22008).
- Contrôle restreint concernant l'application de la procédure SAC au sein d'une zone de police de la province de Flandre occidentale et certains services fournis par la zone de police à une (des) ville(s)/commune(s) de la zone de police (DIO22006).
- Contrôle restreint concernant l'utilisation de caméras pendant la concertation confidentielle entre le suspect et l'avocat dans une zone de police de la province de Liège (DIO22004).
- Contrôle restreint concernant la constatation d'excès de vitesse dans le cadre de l'application de la procédure 'SAC-5' et l'utilisation de portiques d'identification des poids lourds dans les zones de police de la Région flamande (DIO22003).
- Contrôle restreint relatif aux résultats du contrôle des fichiers de journalisation concernant les membres et les membres du personnel de l'Organe de contrôle de l'information policière (DIO22002).

- Contrôle spécial 2022 de la banque de données commune terrorisme et extrémisme (CO22T001)[71].

58. Voici à présent un aperçu chronologique des enquêtes de contrôle qui ont débouché sur **un rapport final ou un rapport d'enquête** en 2022, dans le cadre desquelles des mesures correctrices contraignantes ont d'ailleurs généralement été prises[72]:

- Contrôle restreint relatif à l'utilisation de *Clearview AI* par la police intégrée (rapport DIO21006 du 4 février 2022).
- Contrôle thématique relatif à l'utilisation, par la police intégrée, de caméras mobiles montées sur des drones (rapport DIO20009-1 du 15 mars 2022).
- Contrôle thématique concernant l'enregistrement et/ou l'écoute, par la police, de la concertation confidentielle entre le suspect et l'avocat (rapport DIO21002 du 29 mars 2022).
- Contrôle technique effectué auprès d'une zone de police de la province de Flandre occidentale par l'Organe de contrôle de l'information policière dans le cadre de ses compétences de contrôle et de surveillance (rapport CON21006 du 4 juillet 2022).
- Contrôle restreint relatif au signalement en BNG de mesures relatives au prélèvement ADN à la suite d'une condamnation (art. 5 §2 de la loi du 22 mars 1999 sur l'ADN (rapport DIO22008 du 12 septembre 2022[73]).
- Contrôle restreint auprès de la zone de police Bruxelles-Ouest concernant la saisie dans la BNG des infractions à la législation visant à limiter la propagation du coronavirus commises par des membres du personnel (rapport CON22005 du 26 septembre 2022[74]).
- Contrôle restreint concernant la constatation d'excès de vitesse dans le cadre de l'application de la procédure 'SAC-5' et l'utilisation de portiques

[71] En collaboration avec le Comité permanent de contrôle des services de renseignement et de sécurité.
[72] L'Organe de contrôle aspire dans ce contexte à une transparence maximale en établissant des versions publiques des rapports dans lesquelles il omet les techniques et tactiques policières non destinées au public, mais ce n'est pas toujours possible ni souhaitable. Certains rapports ne sont carrément pas rendus publics, soit pour des motifs d'opportunité, soit par souci de protéger les données à caractère personnel.
[73] Ce rapport n'a pas été rendu public mais a uniquement été transmis au Collège des procureurs généraux, au commissaire général, au directeur général de la Direction générale de la police judiciaire de la police fédérale et à la Commission permanente de la police locale.
[74] Ce rapport n'a pas été rendu public mais a uniquement été transmis au chef de corps de la zone de police Bruxelles-Ouest (Molenbeek-Saint-Jean/Koekelberg/Jette/Ganshoren/Berchem-Sainte-Agathe).

d'identification des poids lourds dans les zones de police de la Région flamande (rapport DIO22003 du 28 novembre 2022).

- Contrôle thématique de la BNG Administratif – Groupements et phénomènes devant faire l'objet d'un suivi – Recommandations de l'Organe de contrôle de l'information policière (rapport CON21005 du 6 décembre 2022)[75].

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

59. Pour l'année 2022, le COC et le Comité permanent R ont décidé d'axer le contrôle conjoint d'une part sur le suivi de certaines recommandations formulées dans les rapports des années précédentes. Ces recommandations ont principalement trait à l'accès direct aux banques de données communes (BDC) prévu pour l'Autorité nationale de sécurité (ANS), à la (réalisation de la) mission du DPO des BDC, au contrôle des fichiers de journalisation et à la transmission des listes concernant les entités des BDC à des instances tierces.

D'autre part, ce contrôle s'est penché plus en détail sur l'utilisation des banques de données communes par les services de renseignement.

3.3. Le contrôle des statistiques de la BNG en tant que fondement pour la rétention de données

60. En vertu de l'article 126/3 §1er, 8e alinéa de la loi du 13 juin 2005 relative aux communications électroniques, le COC a été en 2022 chargé **pour la première fois** d'une nouvelle mission, à savoir la validation (ou non) des statistiques relatives au nombre de faits punissables et au délai de conservation pour chaque arrondissement judiciaire et chaque zone de police dans le cadre de la rétention des données de communications (données de trafic et données de localisation).

Le 4 avril 2023 est paru au Moniteur belge l'arrêté ministériel du 30 mars 2023 portant exécution de l'article 126/3, §1er, de la loi du 13 juin 2005 relative aux communications

[75] Ce rapport n'a pas été rendu public mais a uniquement été transmis au ministre de l'Intérieur, au commissaire général, au directeur général de la Direction générale de la police administrative et au directeur de la Direction des opérations de police administrative de la police fédérale (seules des recommandations ont en l'occurrence été formulées étant donné que la Direction s'était conformée durant l'enquête aux constatations et aux critiques du COC).

électroniques en vue de l'adoption de la liste des arrondissements judiciaires et des zones de police soumises à l'obligation de conservation ainsi que la durée de conservation. Avant que cet arrêté n'ait pu être adopté, l'Organe de contrôle était déjà investi de l'obligation légale de **valider** ou non les statistiques de ces faits punissables (à savoir les infractions figurant sur la 'liste des écoutes') provenant de la Banque de données nationale générale (BNG).

Par décision du 10 novembre 2022, le COC a procédé à cette validation à l'issue d'une analyse approfondie et complexe des statistiques fournies par la police fédérale.

61. Des 416.480 faits punissables initialement notifiés par la police, le COC en a finalement retenu après analyse 350.144 comme constituant un motif de rétention des données. L'Organe de contrôle souhaite dans ce contexte offrir une transparence maximale quant à la méthodologie utilisée, tant par la police fédérale d'une part que par le COC d'autre part au niveau du processus de validation suivi. À ce titre, cette décision de validation a été publiée dans son intégralité sur le site Internet du COC.

Cette mission est nouvelle et implique un fort coefficient de travail, comme en témoigne le fait que le COC a dû y consacrer pendant 2 semaines plus de 60 % de sa capacité totale.

4. LES ACTIVITÉS POLITIQUES

4.1. Forums de concertation nationaux

62. Le COC prend part à un certain nombre de forums de concertation nationaux ou réunions. 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.

63. En sa qualité d'autorité de contrôle indépendante, le COC répugne cependant à siéger au sein des groupes de travail et réunions de toutes sortes auxquels il est invité (notamment par les ministres compétents). La frontière entre la fonction consultative et informative d'une part et le maintien de la propre indépendance d'autre part est parfois très mince.

4.2. Forums de concertation internationaux

64. 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[76]). 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, voire excessive. Le COC s'efforce néanmoins d'investir du temps dans ces assemblées car elles traitent de nombreux thèmes internationaux cruciaux, qui peuvent parfois revêtir de l'importance au niveau

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

national, comme le recours à la technologie de reconnaissance faciale dans les États membres de l'UE.

En 2022, le COC a à nouveau pris part à des dizaines de 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, participation à la rédaction des points de vue du CEPD, etc. …).

4.3. Communication externe et participation à des événements

4.3.1. Contacts avec la presse

65. En 2022, le COC a continué à entretenir ses contacts avec la presse. Le président a.i. exerce également la fonction de porte-parole de la presse tant du côté francophone que du côté néerlandophone, en marge de ses tâches opérationnelles et de gestion. La désignation d'un porte-parole de la presse est aussi la mise en œuvre du devoir d'information prévu à l'article 240, 1° de la LPD[77], qui vise à ce que le COC se tienne au maximum à la disposition de la presse. La presse, écrite ou audiovisuelle, n'hésite désormais plus à s'adresser à l'Organe de contrôle.

Tant la presse francophone que la presse néerlandophone ont fait paraître en 2022 des articles et des contributions faisant mention du COC ou pour lesquels le porte-parole de la presse avait été contacté[78].

4.3.2. Participation à des journées d'étude et formations

66. Le COC fait régulièrement l'objet de sollicitations en vue de prendre part à toutes sortes de formations, journées d'étude ou colloques organisés par des tiers. De telles participations sont l'occasion de diffuser les points de vue du COC de manière à ce que les instances contrôlées agissent de plus en plus de manière conforme. La mission

[77] Cet article 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 …* ».
[78] Presse francophone : Le Soir, les journaux du groupe Sud-Presse. Presse néerlandophone : Het Laatste Nieuws, Gazet van Antwerpen, HUMO, Tweakers.net, De Tijd, De Standaard, Knack.

de sensibilisation[79]du COC exige un déploiement aussi intensif que possible sur le terrain.

Pour illustrer ce propos par quelques exemples, les membres (du personnel) du COC ont notamment apporté en 2022 leur concours aux formations, journées d'étude et colloques suivants:

(1) ANPA (Académie Nationale de Police), formation des aspirants commissaires de police (N-F);
(2) Formation des aspirants inspecteurs de l'école de police ERIP (Bruxelles) (N/F);
(3) Podcast 'Dasprivé'[80] (N);
(4) Participation en tant qu'intervenant extérieur à la VUB, formation de master en criminologie, profil de master *Policing & Surveillance*, Prof. De Kimpe et Prof. Melgaço (N);
(5) Participation en tant qu'orateur au forum 'Privacycafé' organisé par le *Ministry of Privacy* (N);
(6) Participation en tant qu'orateur à l'atelier de deux jours de la VUB consacré à l'utilisation policière des technologies de surveillance, *VUB Chair in Surveillance Studies*;
(7) Formation auprès de l'assemblée de corps du parquet fédéral (N-F);
(8) Formation auprès du *Data Protection Institute* (certification DPO) (N);
(9) Colloque des autorités de contrôle COC, Comité P et AIG (F);
(10) …

Les membres et les membres du personnel du COC participent par ailleurs à des formations pertinentes, mais dont le nombre reste limité. La matière que traite le COC est complexe, est constituée de composantes nationales et internationales, comporte de nombreuses 'zones grises' et évolue rapidement, de sorte que la formation continue est indispensable.

[79] Le COC est en effet également investi de l'obligation légale 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* » (art. 240, 2° de la LPD).
[80] Voir www.dasprivé.be.

4.3.3. Site Internet

67. Le site Internet a encore été consulté régulièrement en 2022.

Voici les nombres de visiteurs recensés tout au long de l'année **2022**, correspondant à une moyenne de 579 visiteurs par mois, légèrement en baisse par rapport à 2021 (616 visiteurs par mois en moyenne) mais représentant toujours près du double de la moyenne de 2020 (356 visiteurs par mois). Entre 2021 et 2022, le nombre de visiteurs est resté comparable et semble donc se stabiliser.

Nombre de visiteurs du site Internet du COC	**2021**	**2022**
Janvier	603	534
Février	541	460
Mars	1087	663
Avril	751	652
Mai	832	691
Juin	746	536
Juillet	401	416
Août	341	407
Septembre	481	480
Octobre	526	616
Novembre	534	688
Décembre	550	799
Total	**7.393**	**6942**

Le site est accessible à l'adresse www.controleorgaan.be ou www.organedecontrole.be, le rôle de webmaster est endossé par l'unique assistante de direction du COC et le site est alimenté par les membres du DIRCOM.

4.3.4. Consultations du COC par des étudiants et d'autres externes

68. Le COC est toujours régulièrement consulté par des chercheurs ou des étudiants d'universités[81]et d'écoles supérieures et par d'autres parties externes. En 2022

[81] Concrètement pour les universités, notamment l'UCL, la KULeuven, l'UGent et la VUB.

également, des interviews dans le cadre de travaux de fin d'études de bacheliers ou de masters ou encore de *papers* ont ainsi été accordées à des étudiants ou chercheurs d'universités et d'écoles supérieures.

Non sans un certain regret, le COC n'est pas en mesure, par manque de capacité, de répondre aux nombreuses demandes de stages émanant d'universités/écoles supérieures et d'étudiants individuels.

5. PARTENARIATS ET COMPÉTENCES PARTAGÉES

69. Le législateur fédéral a prévu dans la LCA et la LPD plusieurs 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 (dans une mesure très restreinte) le Comité permanent P.

L'article 54/1 de la LCA prévoit que les autorités fédérales de protection des données doivent collaborer étroitement, entre autres en ce qui concerne le traitement des plaintes, les avis et les recommandations qui affectent les compétences de plusieurs autorités de contrôle. Le protocole de coopération conclu à cette fin en 2020[82]a déjà fait ses preuves et ne pose jusqu'ici pas de problèmes notables.

70. Pour illustrer la bonne interaction et la collaboration efficace entre le COC et l'APD, on peut notamment citer la décision sur le fond prise le 30 mars 2022 par la Chambre Contentieuse de l'APD (n° 45/2022) dans un dossier où le SPF Justice avait la qualité de défendeur. Ce dossier avait trait au non-respect des délais de conservation dans la banque de données SIDIS de l'administration pénitentiaire, qui avait été constaté par le COC dans le cadre du traitement de dossiers d'accès indirect. Le COC a transmis à ce sujet une déclaration motivée à l'APD, qui a donné au terme d'une enquête menée par son service d'inspection l'ordre de respecter les règles en matière de protection des données, qu'il a assorti d'un délai de mise en œuvre allant jusqu'en novembre 2022.

La collaboration avec le Comité P donne satisfaction également, et les plaintes sont transmises pour traitement en fonction de la compétence.

[82] Voir https://www.organedecontrole.be/files/Protocol_Federale_DPA_DEF_FR_24112020.pdf.

6. CONCLUSION ET PERSPECTIVES D'AVENIR

71. En **<u>2022 et dans le moment présent</u>**, le COC :

- est parvenu depuis sa relance du 5 septembre 2018, et en dépit de son envergure restreinte, à se faire en très peu de temps une place dans le paysage de la protection des données et (du contrôle) de la police. Le constat que le volet de la protection des données constitue environ 75 % des activités reste d'application en 2022 également ;

- jouit d'une grande confiance de la part à la fois des citoyens/personnes concernées et des responsables du traitement, comme le prouvent le nombre et le type de dossiers auxquels il a été fait allusion au fil du présent rapport d'activité. 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. Le COC est la plupart du temps aussi suivi par les responsables politiques lorsqu'il agit d'initiative. Outre la circulaire COL 9/2022 citée plus haut (voir le point 46), on peut par exemple aussi évoquer la circulaire du 18 mars 2022 relative au contrôle des personnes candidates à l'hébergement des personnes fuyant le conflit armé en Ukraine du ministre de la Justice, du ministre de l'Intérieur et du secrétaire d'État à l'Asile et la Migration[83], dans laquelle la vision du COC quant à l'impossibilité de procéder à des contrôles systématiques et non différenciés des personnes candidates à l'hébergement de réfugiés ukrainiens a été suivie;

- n'hésite pas à exercer de manière proportionnelle ses compétences correctrices – et donc ses pouvoirs de contrainte – et tente de pallier ainsi le vide classique qui affecte le droit à la protection de la vie privée et des données, à savoir l'absence d'un véritable mécanisme de maintien de la norme. De manière proportionnelle, parce que le COC ne veut pas rendre le travail de la police impossible à travers un exercice trop peu nuancé de ses compétences correctrices. À cet égard, il s'agit souvent d'un exercice d'équilibre délicat;

- ne se préoccupe pas seulement de la protection des données; il porte aussi énormément d'attention à tous les autres aspects opérationnels de la gestion de

[83] *M.B.* 8 avril 2022, en particulier les pages 3 et 4.

l'information policière et des informations des autres services qu'il contrôle, s'agissant là de matières relevant également de sa compétence.

72. Pour ce qui est de l'**avenir** :

- l'Organe de contrôle attend l'indispensable réparation de la loi relative à la protection des données, d'ailleurs déjà annoncée (depuis longtemps) par les autorités compétentes, dans le sillage de l'évaluation réalisée en octobre 2021 ;

- l'Organe de contrôle se heurte peu à peu aux limites de sa capacité financière et de sa capacité en termes de personnel, ce qui affecte en premier lieu les enquêtes proactives sur le terrain. Le COC a donc besoin de renforts en termes de nombre d'ETP et d'expertise, notamment au vu des nouvelles missions qui lui sont sans cesse confiées (rétention des données, réglementation européenne et/ou nationale à venir dans le domaine de l'intelligence artificielle, *big data policing*, *predictive policing*, techniques de surveillance avancées, etc.) ;

- le COC ne peut que rappeler les points d'amélioration ou adaptations qu'il sollicitait déjà dans ses rapports précédents, à savoir:

* rendre le COC compétent également pour les traitements de données non opérationnels de l'AIG[84], de manière à ce que celle-ci ne soit soumise qu'à une seule autorité de contrôle;

* conférer au COC la compétence d'agir à l'encontre de fonctionnaires de police individuels;

* définir clairement la compétence du COC à l'égard des écoles de police et des organes liés à la GPI;

* offrir au COC la possibilité – après consultation du magistrat compétent – de prendre également des mesures correctrices lorsqu'il y a une enquête pénale en cours;

* repenser fondamentalement le système de l'accès indirect et l'aligner sur le principe de l'accès direct qui est appliqué dans le reste de l'UE, avec possibilité

[84] Article 71 §1er, troisième alinéa de la LPD.

de demander un avis ou d'introduire un recours auprès du COC, et soumettre également dans ce cadre à un examen approfondi la problématique des éventuels moyens de droit à faire valoir contre la communication finale à la personne concernée;

* attribuer à l'Organe de contrôle la compétence formelle, dont est également investi le président du Comité permanent P[85], d'informer une instance disciplinaire de potentiels manquements disciplinaires et d'également l'obliger à examiner les faits et à vérifier si ceux-ci justifient d'initier une procédure disciplinaire, et à informer l'Organe de contrôle de la suite donnée à son information. Le COC constate en effet que certains chefs de corps ou instances disciplinaires continuent à minimiser la consultation illicite des banques de données policières et n'estiment même pas nécessaire d'initier une procédure disciplinaire alors qu'il est bel et bien question de manquements disciplinaires[86], voire d'infractions pénales[87].

* introduire l'astreinte administrative de manière à disposer d'une forme efficace de moyen de pression à l'égard des chefs de corps (ou des autorités de police) étant donné que l'amende administrative semble avoir été définitivement exclue (et que cette décision a été jugée conforme par la Cour constitutionnelle[88]), bien qu'elle existe dans la plupart des pays de l'UE à l'égard de la police[89].

73. Le COC 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. Le COC privilégiera toujours dans la mesure du possible une approche axée sur la médiation et la solution. La commission d'enquête parlementaire 'Attentats'[90], qui a

---

[85] Article 26, 4° de la loi du 13 mai 1999 portant le statut disciplinaire des membres du personnel des services de police.
[86] Articles 46 et 54-56 du Code de déontologie et article 3 de la loi du 13 mai 1999 portant le statut disciplinaire des membres du personnel des services de police.
[87] Article 151 et/ou article 550bis du Code pénal et/ou article 222, 1° et/ou 2° de la loi sur la protection des données et/ou article 5 et/ou article 8 de la loi organisant un Registre national des personnes physiques.
[88] Cour constitutionnelle, 14 janvier 2021, n° 3/2021, www.const-court.be/fr.
[89] Voir « First report on application and functioning of the Data Protection Law Enforcement Directive (EU) 2016/680 (LED), Commission from the Commission to the European Parliament and the Council », Bruxelles, 25.07.2022 (COM) 2022, 364 final, p. 12 : « *In addition, the majority of member states' laws give data protection supervisory authorities the power to impose administrative fines.* » (à savoir 18 États membres tant à l'égard des autorités qu'à l'égard des personnes physiques et 3 autres uniquement à l'égard des personnes physiques, soit au total 21 des 27 États membres).
[90] 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, DOC 54, n° 1752/008, p. 252.

fait appel pour ses travaux aux services du COC, a notamment émis la recommandation suivante en matière de législation et de réglementation : « *Le COC doit par ailleurs pouvoir exercer son contrôle sur l'ensemble de la sécurité de la gestion de l'information, et pas uniquement sur certains aspects partiels de cette matière.* », soulignant ainsi l'importance des activités du COC. En 2023 également, l'Organe de contrôle continuera à s'acquitter assidûment de cette mission, mais il espère néanmoins que le Parlement ne continuera pas éternellement à différer le renouvellement des mandats des membres du DIRCOM qui sont arrivés à échéance au 1er septembre 2021.

* * * * * * * * *

Rapport d'activité 2022, approuvé par l'Organe de contrôle le 6 juin 2023.

Ronny SAELENS	Koen GORISSEN	Frank SCHUERMANS
Membre-conseiller a.i.	*Membre-conseiller*	*Président a.i.*

ANNEXE : L'ORGANE DE CONTRÔLE EN CHIFFRES[91]

TYPE DE DOSSIER	2019	2020	2021	2022
Dossiers AI[92]	392	283	546	555
Avis protection des données	82	85	82	87
Avis réglementation	22	15	33	39
Plaintes	30	40	28	29
Avis sur l'utilisation de caméras	32	29	29	32
AIPD	27	10	33	29
Fuites de données	17	17	21	25
Contrôle global & Contrôle technique[93]	2	5	1	1
Contrôle thématique & Contrôle restreint[94]	3	5	8	7
Contrôle spécial BELPIU[95]	1	1	1	1
Contrôle spécial BD Terrorisme[96]	1	1	1	0
Contrôle international[97]	1	0	1	0
Validation rétention des données	0	0	0	1
TOTAL	**610**	**491**	**784**	**806**

[91] 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. Et en tout état de cause, 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.
[92] Dossiers d'accès indirect.
[93] Rapports d'enquêtes de contrôle publiés en 2022.
[94] Ibidem.
[95] Ibidem.
[96] Ibidem.
[97] Ibidem.

Décisions prises dans les enquêtes de contrôle	**2020**	**2021**	**2022**
Requêtes	1	36	7
Recommandations	80	33	7
Mesures correctrices	26	32	9
TOTAL	**107**	**101**	**23**

Mesures correctrices prises dans les enquêtes de contrôle	**2020**	**2021**	**2022**
Avertissement	3	2	1
Réprimande	1	0	1
Ordre de mettre le traitement en conformité avec les règles en matière de protection des données	21	26	6
Interdiction du traitement	1	1	8
Limitation définitive du traitement	-	1	0
Limitation temporaire du traitement	-	1	0
TOTAL	**26**	**31**	**16**