RAPPORT D'ACTIVITÉ DE L'ANNÉE DE FONCTIONNEMENT 2025



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 Président a.i.

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. Les missions

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 UIP

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

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

2.9. 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 de la banque de données commune T.E.R.

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 divers événements

4.3.1. Contacts avec la presse

4.3.2. Participation à des journées d'étude et formations externes

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: LE COC EN CHIFFRES

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

BDC T.E.R.: Banques de Données Communes Terrorisme - Extrémisme - Radicalisme

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

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

EDPB: *European Data Protection Board*/Comité européen de la protection des données

EDPS: *European Data Protection Supervisor*/Contrôleur européen de la protection des données (CEPD)

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 (loi relative à la protection des données)

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

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: Unité d'Information des Passagers

ZP: Zone de Police

A. Préambule du Président

1. Le présent rapport d'activité présente un aperçu des activités de l'Organe de contrôle de l'information policière ou COC[1] en 2025. C'est la **septième** année de fonctionnement 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 courte période résolument positionné dans le paysage du contrôle notamment des services de police.

2. Aucune modification n'est intervenue en 2025 au niveau du comité de direction (DIRCOM). Cela signifie que le DIRCOM a été composé durant toute l'année de fonctionnement de 2 membres de la direction au lieu des 3 prévus, et ce en attendant que la Chambre des Représentants décide de procéder à la désignation et à la nomination de trois nouveaux membres du DIRCOM pour la période de 6 ans prévue par la loi (voir plus loin le point 1.1.3.).

Les mandats des membres de la direction sont en effet expirés depuis le **1er septembre 2021** sans que le parlement fédéral n'ait initié dans l'intervalle la procédure en vue de leur renouvellement. Nous prions une nouvelle fois la Chambre des Représentants de remédier à cette situation en 2026.

3. Nous profitons de l'occasion pour remercier tous les collaborateurs du COC d'avoir donné le meilleur d'eux-mêmes en 2025 et d'avoir atteint avec cette équipe restreinte les résultats esquissés dans le présent rapport annuel, et ce en dépit des circonstances de plus en plus complexes et de la charge de travail croissante. Il y a tout lieu d'être fier de l'*output* (la production) et de l'*outcome* (les résultats) du COC, qui soutiendraient sans peine la comparaison (*benchmark*) à la lumière de ce personnel

[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.

limité. Cependant, cet *output* n'est évidemment pas infini et le COC se heurte à ses limites, s'il ne les a pas déjà dépassées.

La qualité prime en effet, ou devrait primer, sur la quantité.

Bruxelles, 19.05.2026
Frank SCHUERMANS
Président *a.i.*

B. Cadre légal

4. Initialement constitué en tant qu'organe de contrôle classique, l'Organe de contrôle de l'information policière se trouvait entre 1998 et 2014 sous l'autorité des ministres de tutelle de la police. En 2014, il a été transféré au parlement fédéral pour ensuite exercer, à partir du 05.09.2018, la mission additionnelle d'autorité de protection des données spécialisée à l'égard (notamment) de la GPI.

Le cadre légal se compose d'une part des normes internationales – la Charte des droits fondamentaux de l'Union européenne, 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) et la LFP (loi sur la fonction de police). À cela s'ajoutent des lois sectorielles ainsi que nombre de normes inférieures.

Nous soulignons que le COC n'est **pas uniquement** une autorité de protection des données, mais aussi une instance de contrôle 'régulière' qui prête attention à des éléments comme l'efficience et l'efficacité. Il convient toutefois de reconnaître que cet aspect de ses attributions est de plus en plus relégué à l'arrière-plan du fait de l'accroissement de la charge de travail (voir plus loin).

C. Vision et mission

5. Le COC aspire à contribuer à un fonctionnement policier et une gestion de l'information policière qui soient à la fois performants 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 l'UIP[4] et de l'AGD&A[5].

En tenant compte des limites et possibilités définies par la loi, il adopte une vision prioritairement axée sur l'appui et le soutien en commençant par 'assister' et sensibiliser les services contrôlés. À moins qu'il ne constate des irrégularités manifestes, il n'envisage en principe qu'en dernier recours une intervention contraignante à travers la prise de 'mesures correctrices'. La jurisprudence, notamment de la Cour de Justice de l'Union européenne, considère cependant qu'une autorité de protection des données est tenue de prendre immédiatement des mesures correctrices (et donc contraignantes) lorsqu'elle constate des violations de la législation et de la réglementation, laissant ainsi de moins en moins de marge pour une 'approche pédagogique préventive' (voir plus loin).

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

1. INTRODUCTION

1.1. Compétences et missions

1.1.1. Les missions

6. Les missions du COC englobent:

[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.

(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 (LFP);

(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 (voir le point 42);

(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 alinéas 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

[6] *Human Ressources Management.*

relatives aux communications électroniques impliquant la personne disparue.

7. 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 constituent tout de même un volet crucial de l'activité. Somme toute, les deux dimensions se mêlent en permanence dans toutes les activités du COC.

1.1.2. Compétences

8. Les compétences du COC sont en partie comparables aux missions classiques d'un organe de surveillance ou de contrôle.

9. Une série de réparations légistiques s'imposent néanmoins depuis plusieurs années du fait que le COC est (aussi) une autorité de protection des données. Ces propositions ont été transmises dès mai **2021** par le COC au gouvernement de l'époque, dans le cadre de l'évaluation de la loi relative à la protection des données prévue à l'article 286[7]. Cette loi de réparation reste indispensable pour permettre au COC d'optimaliser son fonctionnement, et donc aussi la surveillance de la GPI et des autres instances contrôlées. L'accord gouvernemental 2025-2029 (chapitre *«Sécurité»*, section *«Recherche et partage d'informations»*) ne fait pas non plus mention d'une loi de réparation en la matière, à moins que le passage suivant ne doive être interprété en ce sens: *«À la suite de la directive européenne 2016/680, la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel a déjà prévu la transposition de cette directive pour l'application spécifique qu'est le traitement de données à caractère personnel par les autorités compétentes pour la prévention, la recherche, la détection et la poursuite d'infractions pénales ou l'exécution de peines. La description des traitements eux-mêmes est*

[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.

aujourd'hui réglée par la loi du 5 août 1992 sur la fonction de police et le code de procédure pénale. Dans une prochaine étape, un cadre juridique sera créé par une loi spécifique sur les données de police afin de fusionner ces matières. Cette loi réglementera les droits et obligations de la police et des citoyens en ce qui concerne le traitement des données policières. Nous éviterons ainsi à l'avenir des situations où toutes les informations sont disponibles mais où l'on ne sait pas clairement qui est responsable ou compétent pour traiter et utiliser les informations disponibles. Nous examinons le fonctionnement de l'organe de contrôle des informations policières (COC) et, sur la base de cet examen, nous déterminons s'il est souhaitable de prévoir des fonds supplémentaires pour le personnel.».[8]

Le COC ne verrait aucune objection – bien au contraire – à ce qu'il soit procédé à une évaluation et à une adaptation de ses compétences et de sa capacité, et comprend donc ce passage de l'accord gouvernemental en ce sens. Le COC a constaté que la ministre compétente pour la digitalisation a en octobre 2025 attiré l'attention du parlement sur ce passage de l'accord gouvernemental et a suggéré de confier cette mission à la Cour des comptes.

1.1.3. Organisation et composition

10. Le COC se compose selon son cadre d'un comité de direction (DIRCOM) composé de 3 membres, dont 2 magistrats et 1 expert. À cela s'ajoute un «service d'enquête» (DOSE[9]) 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(e) de direction. Le COC peut en outre recruter contractuellement[10] 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 12 ETP. Cela dit, ce n'est jamais le cas. Dans les faits, le COC dispose en moyenne de 8 à 10 personnes pour traiter les dossiers opérationnels.

L'ensemble des tâches PLIF[11] repose également sur les épaules du président et de l'unique assistant(e) de direction, moyennant il est vrai un soutien de la part de Persopoint pour l'administration des salaires (et un support très partiel dans le domaine des ressources humaines).

---

[8] Accord de coalition fédérale 2025-2029, p. 136, https://www.belgium.be/sites/default/files/resources/publication/files/Accord_gouvernemental-Bart_De_Wever_fr.pdf.
[9] **D**ienst **O**nderzoeken/**S**ervice d'**E**nquête.
[10] 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.
[11] Personnel, Logistique, Informatique et Finances.

Comme nous le disions, le COC ne compte plus que 2 membres de la direction depuis juillet 2023, tous deux désignés dans la fonction supérieure: un membre-conseiller dans la fonction supérieure de président *a.i.* et un commissaire-enquêteur (expert et pas fonctionnaire de police) du DOSE dans la fonction supérieure de membre-conseiller *a.i.*

1.1.4. Quelques chiffres clés relatifs à l'organisation interne

11. Le COC est une institution de petite envergure compte tenu de ses missions et des institutions et organes qu'il doit contrôler. Durant l'année de fonctionnement 2025 également, le cadre n'a jamais été complet[12]. De plus, la technicité et la complexité du travail au sein du COC sont telles qu'un nouveau collaborateur a besoin d'au moins 1 an pour maîtriser un tant soit peu la matière et la fonction à exercer.

Le DIRCOM a tenu **41 réunions plénières formelles** en 2025, en plus des consultations informelles pour ainsi dire quotidiennes. À cela s'ajoute régulièrement une réunion plénière avec **tous** les membres du personnel, au cours de laquelle peuvent être abordés aussi bien des sujets opérationnels ou stratégiques, que des thèmes dits PLIF. Le DOSE et le service de soutien se réunissent également une fois par semaine pour discuter principalement de dossiers strictement opérationnels.

12. Le COC disposait en 2025 d'un **budget de dépenses approuvé (après adaptation) de 2.173.399 EUR**, pour lequel il a perçu une **dotation de 1.404 KEUR**. Les **dépenses réelles** globales ont atteint **1.625 KEUR** en 2025. Les charges salariales (théoriques) s'élevaient à 1.766.596 EUR.

On relève pour la deuxième année consécutive une réduction substantielle de la dotation du COC: 1.860 KEUR en 2023, 1.600 KEUR en 2024 et 1.404 KEUR en 2025. Du fait qu'il n'a pas été pourvu à certains postes vacants (comme c'est le cas depuis quelques années pour une fonction de membre du DIRCOM) et grâce à sa politique d'austérité, le COC parvient à accumuler chaque année des réserves que la Chambre utilise pour couvrir les dépenses.

[12] Principalement à cause d'un membre du DIRCOM manquant et de divers congés pris par les membres du personnel.

Quoi qu'il en soit, une partie substantielle des charges de fonctionnement ne sont toujours pas couvertes par la dotation, de sorte que celles-ci continuent à devoir être financées en puisant dans les réserves accumulées dans le passé, comme c'est le cas chaque année. Le COC est donc en quelque sorte 'sanctionné' pour le fait qu'il limite rigoureusement ses dépenses (pas d'experts externes, pas de consultants, pas d'avis de cabinets d'avocats, etc.) et qu'il n'a pas atteint – ou plutôt, n'est pas parvenu à atteindre – son cadre complet. Vu les effets de volume persistants (**à savoir une augmentation de 73% en comparaison de 2019**[13]**, venant de 'seulement' 40% en 2024**) et les missions additionnelles qui ont été confiées au COC depuis 2018 et qui lui seront encore confiées en 2026 (dans le cadre de l'entrée en vigueur du Règlement 2024/1689 relatif à l'intelligence artificielle, aussi appelé 'loi sur l'IA', et de la charge de travail de plus en plus importante découlant des obligations d'audit des systèmes informatiques à grande échelle européens (*«large scale information systems»*, comme nous le verrons plus loin au point 64), le cadre restreint actuel du COC et les profils disponibles – ou plutôt les profils manquants – posent clairement problème.

Vu que le COC répète ce message depuis plusieurs années sans qu'il n'y soit jamais donné suite, le COC est dans la réalité contraint d'opérer des choix difficiles qui consistent principalement à limiter au strict minimum ses enquêtes proactives (et dans une moindre mesure ses avis). Cette tendance se poursuit sans discontinuer, également en 2026.

[13] En 2025, le COC a traité un nombre record de 1090 dossiers, venant de 867 en 2024; à titre de comparaison, il était en 2019 – c'est-à-dire à l'époque de la fixation du cadre du COC – question de 616 dossiers.

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, de rectification ou de suppression de ses données à caractère personnel dans les banques de données policières – mieux connues sous l'appellation 'dossiers article 42 de la LPD'[14] ou 'dossiers AI'[15] – constituent depuis 2018 la majeure partie, en termes de volume, des activités quotidiennes du COC. Il en est demeuré ainsi en 2025, à nouveau au point d'affecter de manière significative, et encore plus que l'année précédente, les missions de contrôle proactives du COC. Chaque demande individuelle requiert en effet un investissement (en temps) substantiel.

14. 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 entre 100 et 150 dossiers par an. En 2025, **796 demandes** ont été introduites auprès du COC, s'agissant du **nombre le plus élevé** recensé depuis le lancement du COC en tant qu'autorité de protection des données en 2018 et d'une **augmentation de 41% par rapport à 2024** (de 565 à 796 demandes). Sur ce total, 167 demandes émanaient de ressortissants de pays tiers tandis que 629 ont été introduites par des Belges ou (très rarement) par des ressortissants d'autres États membres de l'UE.

Par rapport au lancement du COC en tant qu'autorité de protection des données en 2018, le nombre de demandes d'accès indirect a donc augmenté de 139% en moins de 7 ans. Nous pouvons à cet égard rappeler que le cadre du COC avait en 2018 été fixé sur la base d'un maximum de 200 demandes, soit environ 300% de moins que le nombre recensé en 2025. Les effets de volume que nous avions prédits dans notre rapport d'activité de 2024 se sont donc largement réalisés en 2025 et se poursuivront sans nul doute à l'avenir.

---

[14] 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).

[15] «AI» signifiant «**A**ccès **I**ndirect».

<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
2023	549
2024	565
2025	**796**

15. Des **796** dossiers AI susmentionnés, **732 avaient déjà été traités** lors de l'établissement des statistiques à la mi-avril 2026. **Autrement dit, cela signifie que 92% des demandes introduites en 2025 avaient à la mi-avril 2026 été clôturées avec une décision finale.**

<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
2023	45,77	37
2024	51,04	41
2025	**59,39**	**42**

Le délai de traitement moyen[16] était de **59 jours** en 2025 (médiane: 42 jours), ce qui reste globalement un excellent résultat. Il n'en est pas moins indéniable que les délais de traitement s'allongent, ce qui signifie que l'amélioration réalisée dans les années 2022-2023 grâce à un fonctionnement plus efficace du COC a désormais atteint ses limites. Il n'y a qu'une seule explication à ce constat, à savoir l'augmentation constante du nombre de demandes – qui s'est encore

[16] 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.

considérablement accélérée en 2025 – pour un nombre de membres/membres du personnel resté inchangé depuis 2018.

Si l'allongement des délais de traitement reste globalement limité, c'est surtout parce que le président attribue les demandes non plus exclusivement aux juristes du secrétariat, mais aussi aux membres du Service d'Enquête. Ces derniers se consacrent pleinement à ces dossiers, ce qui limite les possibilités de les affecter à des enquêtes de contrôle proactives (voir plus loin). Il s'agit là d'une évolution aussi regrettable qu'inéluctable.

16. Si nous faisons abstraction des dossiers de ressortissants de pays tiers[17,18], qui peuvent souvent être rapidement transmis à l'Office des Étrangers[19], nous obtenons pour l'année 2025 un **délai de traitement moyen de 69 jours** et une médiane de 49 jours pour les dossiers standard[20]. Même au niveau de ces dossiers 'nationaux' ou européens, nous relevons donc une augmentation du délai de traitement par rapport à 2024 (lorsque le délai de traitement moyen était de 61 jours et la médiane de 46 jours).

17. En 2025, les autres autorités de contrôle ont transmis 9 demandes au COC, 3 l'ayant été par le Comité P et 6 par l'APD. La collaboration avec les collègues a prouvé son efficacité au fil des années, de sorte que le citoyen ne subit aucun préjudice du fait que la Belgique a opté pour un système composé de plusieurs autorités de contrôle spécialisées. Il semble au contraire se frayer aisément un chemin jusqu'à l'autorité de contrôle compétente, en dépit des voix qui se sont parfois élevées pour affirmer le contraire.

18. Vu la lourde charge de travail, l'augmentation substantielle du nombre de demandes, les limitations techniques des banques de données de la GPI (notamment quant aux fichiers de journalisation exploitables), le fait que le COC dépend aussi de la rapidité et de la rigueur avec lesquelles la GPI fournit au COC les évaluations qu'il lui demande et les questions souvent complexes qui se posent, notamment en raison

[17] Autrement dit, des non-ressortissants de l'UE.
[18] Puisqu'il s'agit de demandes en application des règlements 2018/1860 et 2018/1861, autrement dit d'un signalement d'une décision de retour ou d'un refus d'entrée ou de séjour dans l'espace Schengen (*«entry ban»* ou interdiction d'entrée).
[19] Ce qui réduit (et donc écourte) artificiellement le délai de traitement moyen de l'ensemble des demandes.
[20] Nous entendons essentiellement par là des dossiers de Belges ou de personnes d'autres nationalités d'États membres de l'UE.

de la structure morcelée de la police belge, on ne peut que **constater une nouvelle fois que l'Organe de contrôle continue à offrir au citoyen un service rapide, efficace et qualitatif avec un investissement public minimal** (en termes de budget et de personnel).

19. De ces 796 dossiers traités, 473 avaient trait à la Banque de données nationale générale (BNG), autrement dit 59,42%, ce qui s'inscrit dans la lignée des années précédentes.

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

(1) maintien du (des) enregistrement(s): 179, soit **22,5%**
(2) archivage/effacement du (des) enregistrement(s): 152, soit **19%**
(3) rectification du (des) enregistrement(s): 151, soit **19%**
(4) (plus) aucune coopération de la part de la personne concernée[21]: 179, soit **22,5%**
(5) il n'y avait pas d'enregistrement dans la BNG: 117, soit **14,7%**
(6) la demande était purement une demande d'informations: 42, soit **5,3%**
(7) la demande n'était pas recevable: 16, soit **2%**
(8) le délai de conservation était dépassé: 54, soit **6,8%**

Le nombre total d'orientations est supérieur au nombre total de demandes ayant trait à la BNG du fait qu'un dossier peut parfois conduire à plusieurs orientations/décisions finales.

[21] 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.

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

Résultat	2021	2021 en %	2022	2022 en %	2023	2023 en %	2024	2024 en %	**2025**	**2025 en %**
Maintien de l'enregistrement	65	11,9	97	18,65	105	20	99	18	**179**	**22,5**
Rectification	92	18,58	67	13	75	14	78	14,2	**151**	**19**
Archivage/effacement	155	31,3	109	21	119	22	137	25	**152**	**19**
Total	312		273		299		314		**482**	
% Rectification Archivage/Effacement		**50**		**34**		**36**		**39,2**		**38**

Si nous prenons uniquement les dossiers dans lesquels le COC a émis une **évaluation <u>concrète</u>**, **nous <u>constatons qu'environ 38% des dossiers BNG traités en 2025 (303 dossiers sur 796) se sont soldés par une rectification et/ou un archivage/effacement complet(s) ou partiel(s)</u> des enregistrements effectués par la police dans la BNG**.

Cela signifie qu'il n'y a <u>pas</u> d'amélioration notable depuis 2022 dans le pourcentage qui continue à osciller autour de 35 à 40%, c'est-à-dire que dans plus d'un tiers des cas, les demandes introduites mènent à une rectification, un effacement ou un archivage.

L'effet positif de l'archivage *one shot* de 2022 pour dépassement des délais de conservation s'est donc complètement dissipé. Par ailleurs, il n'existe à ce jour toujours pas d'archivage automatique en cas de dépassement du délai d'archivage.

20. Ce pourcentage élevé est décevant après plus de 7 ans de pratique. Ce constat devrait encore davantage inciter les dirigeants de la GPI et ses autorités de tutelle à la réflexion et surtout à l'**<u>action</u>**, s'agissant là d'un appel que le COC a déjà lancé dans tous ses rapports d'activité publiés jusqu'ici. **La qualité (l'exactitude et la précision) des banques de données policières demeure un problème majeur et un défi de taille aux retombées potentiellement très préjudiciables pour**

le citoyen, même si le constat qui est fait ici se limite en l'espèce à la BNG, laquelle est indéniablement la banque de données la mieux tenue dès lors qu'elle est soumise à un processus de validation bien défini. Le citoyen peut en effet être directement ou indirectement préjudicié par des traitements de données incorrects, dépassés ou autrement impropres, et ce problème ne fait qu'empirer à mesure que les *screenings* de toutes sortes se multiplient, ce qui est de plus en plus le cas ces dernières années (par ex. le *screening* auquel sont soumis les candidats à une fonction dans un port).

21. Le COC a reçu 54 demandes d'accès indirect de la part de **candidats membres de la GPI (29)** ou de **fonctionnaires de police en poste (25)**, un nombre qui représente **6,8%** des demandes et même **8,6%** si nous excluons les demandes introduites par des ressortissants de pays tiers[22]. Ces nombres sont légèrement inférieurs à ceux recensés en 2024, mais n'en restent pas moins élevés. Autrement dit, les (candidats) fonctionnaires de police réalisent très bien l'importance d'enregistrements de qualité lorsqu'ils sont personnellement concernés.

22. En 2025, **42 demandes** ont également été introduites par des **candidats titulaires (38) ou des titulaires (4) des métiers classiques de la sécurité** (gardiens de la paix, militaires, agents pénitentiaires et agents de gardiennage privés)[23]. Par rapport aux années précédentes, il s'agit donc d'une **augmentation considérable** (2023: 21 et 2024: 20) **de 110%**. 12 demandes ont par ailleurs été introduites dans le cadre d'autres procédures de *screening*. Cette augmentation est à mettre en relation avec la multiplication des *screenings*, enquêtes d'antécédents et de moralité de toutes sortes, non seulement dans le cadre du recrutement mais aussi, plus généralement, du fait de l'augmentation du nombre de vérifications de sécurité pour l'accès à certains lieux, événements ou emplois. Ces *screenings* confrontent les candidats à leurs antécédents policiers et sont régulièrement suivis de l'introduction, auprès du COC, d'une demande d'accès/de rectification/d'effacement.

Le *screening* préalable réalisé dans le secteur de la sécurité privée constitue à cet égard une procédure particulièrement problématique étant donné que la personne

[22] En 2025, le COC a reçu 167 demandes de ressortissants de pays tiers (autrement dit, des non-ressortissants de l'UE).
[23] Pour autant que le COC ait pu le déduire du dossier, sachant que les personnes concernées ne sont évidemment pas tenues de communiquer cette information.

concernée est par essence et dans les faits informée par un employeur potentiel (qui a lui-même été avisé par le SPF Intérieur que si une autorisation est demandée pour cette personne, une enquête de sécurité sera initiée en raison de son profil problématique[24]) qu'elle n'a aucune chance d'être embauchée en raison de la notification susmentionnée du SPF Intérieur. Même si formellement, le SPF Intérieur n'a pas encore décrété que l'autorisation ne pourrait pas être accordée, les entreprises de gardiennage considèrent la seule annonce d'une enquête de sécurité à venir comme un motif suffisant pour refuser le candidat en question. Souvent, les candidats s'imaginent alors que le COC pourra résoudre leur problème, *quod non*.

En 2025, le COC a également traité en application de l'article 14 de la LPD[25] 2 dossiers qui lui ont été transmis par l'Office des Étrangers.

[24] Voir l'article 64 de la loi du 2 octobre 2017 réglementant la sécurité privée et particulière.

[25] Cette procédure limite les droits de la personne concernée lorsqu'une autorité visée au §1er de cet article (comme en l'occurrence l'OE), auprès de laquelle une demande d'accès a été introduite, est en possession de données policières. Dans ce cas de figure, l'OE doit demander à la GPI si – et le cas échéant dans quelle mesure – la personne concernée peut être autorisée à accéder à ces données provenant des services de police que l'OE a en sa possession. Si la police refuse ou ne répond pas à l'OE (ce qui arrive malheureusement aussi), l'OE s'adresse au COC en application du §6 de l'article 14. Ce paragraphe prévoit en effet dans un tel cas que *«lorsque le traitement porte sur des données initialement traitées par les services de police ou l'Inspection générale de la police fédérale et de la police locale, l'Autorité de protection de données saisie directement par la personne concernée ou par le responsable du traitement qui fait état de l'application du présent article, s'adresse à l'autorité de contrôle visée à l'article 71* (en l'occurrence au COC, NDLR) *pour qu'elle réalise les vérifications nécessaires auprès des autorités, organes ou organismes compétents»*.

<u>Tableau 4:</u> Nombre de dossiers <u>clôturés</u> en 2025, ventilés en fonction du type de banque de données policière auquel la demande avait trait[26]

Type de banque de données	2019	2020	2021	2022	2023	2024	**2025**
BNG	171	211	315	308	312	330	**474**
Banque de données de base	-	6	14	18	10	21	**23**
Banque de données particulière	-	2	6	3	2	2	**2**
Banque de données technique	-	2	4	0	3	1	**30**
Caméra	-	-	-	-	--		**27[27]**
SIS	68	41	202	197	166	204	**204**[28]
BDC T&E[29]	0	1	1	1	1	0	**2**
Autre[30]	1	6	10	8	8	5	**8**
Europol	7	7	1	5	5	7	**4**
Interpol	3	13	12	5	8	8	**12**
Total	250[31]	289[32]	564[33]	545[34]	515[35]	578[36]	**786[37]**

[26] Un tiret (-) signifie que cette catégorie n'était pas encore reprise séparément dans les chiffres de 2019.
[27] Tous les types de demandes d'accès à des images de caméras sont visés ici, tant les caméras *ANPR* que les caméras de surveillance fixes (temporaires) et les *bodycams*. Si la demande a trait à une caméra *ANPR*, elle est également comptabilisée dans la catégorie «Banque de données technique».
[28] Dont 159 qui relevaient (également) de la compétence de l'OE parce que la demande avait trait ou pouvait avoir trait (il arrive en effet souvent que l'on ne sache pas exactement quel accès la personne concernée veut réellement demander) à l'application des règlements 2018/1860 et 2018/1861, autrement dit à un signalement d'une décision de retour ou à un refus d'entrée ou de séjour dans l'espace Schengen (*«entry ban»* ou interdiction d'entrée), et non à l'application du règlement 2018/1862 (c'est-à-dire à un signalement à des fins de police et/ou de justice).
[29] Banque de données commune Terrorisme et Extrémisme.
[30] 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.
[31] 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.
[32] 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.
[33] 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.
[34] 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.
[35] Ce total de 515 est inférieur au nombre de dossiers clôturés (524) du fait qu'une requête peut avoir trait à plusieurs banques de données policières, mais en 2023, 80 requêtes se sont révélées sans rapport avec des enregistrements effectués par la police.
[36] Ce total de 578 est supérieur au nombre de dossiers clôturés (549) du fait qu'une requête peut avoir trait à plusieurs banques de données policières.
[37] Ce total de 786 est supérieur au nombre de dossiers clôturés (732) du fait qu'une requête peut avoir trait à plusieurs banques de données policières.

23. Un dossier d'accès indirect mobilise toujours beaucoup de temps de travail et inclut plusieurs étapes: analyse de la demande, consultation et analyse des traitements (multiples) dans les diverses banques de données policières, envoi aux entités concernées de la GPI d'une demande d'évaluation[38] de la pertinence (permanente) ou de la licéité[39] des enregistrements, concertation avec la GPI (et/ou éventuellement avec le parquet), correction/effacement éventuel(le) ou archivage des données à la demande du COC, contrôle *a posteriori* par le COC des rectifications promises ou annoncées par la GPI[40], communication avec le plaignant/déclarant ou son avocat, etc.

23.1. Étant donné que la structure actuelle de la police induit un morcellement de la responsabilité des enregistrements entre les différentes entités de police concernées (allant dans la pratique de deux à plus de dix entités), il est fréquent qu'une coordination s'impose. À l'évidence, il n'appartient **pas** à l'Organe de contrôle, en sa qualité d'autorité de contrôle, de mettre en place une telle coordination (opérationnelle) au sein de la police **intégrée**. C'est au contraire à la GPI qu'il incombe de fournir au COC une évaluation policière intégrée d'une personne concernée qui exerce ses droits. Il arrive parfois au COC de devoir le rappeler.

Pour cette raison, le COC poursuit sur la voie empruntée depuis 2021 en travaillant, au cas par cas en fonction de la complexité du dossier et de la constellation des faits, avec un seul 'coordinateur de la protection des données' désigné par le COC ou avec une seule entité de police coordinatrice censé(e) fournir cette évaluation policière intégrée. Par essence, cela implique d'ordinaire:

- la désignation du CG/ISPO[41] lorsqu'une coordination est requise entre plusieurs entités de la police fédérale et zones de police d'arrondissements judiciaires différents;

[38] Une demande peut en effet avoir trait à plusieurs enregistrements réalisés par différents services de police.
[39] 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.
[40] Ce contrôle s'avère indispensable dès lors que le COC est toujours régulièrement amené à constater qu'un effacement ou un archivage annoncé, par exemple, n'a pas été effectué. En règle générale, le COC procédera à cette vérification au bout d'un mois.
[41] Commissariat-général/Information Security & Privacy Office, un service qui se situe au niveau du commissariat-général de la police fédérale.

- la désignation d'une DCA (Direction de coordination et d'appui de l'arrondissement) – en collaboration avec la PJF (Police judiciaire fédérale) – de la police fédérale lorsqu'une coordination est requise entre plusieurs zones de police de cet arrondissement et/ou un nombre restreint d'entités fédérales (par ex. la Direction de la police de la route);
- la désignation d'une seule zone de police lorsque seules des zones de police d'un arrondissement donné sont concernées et que la zone de police en question totalise un nombre décisif d'enregistrements ou est en charge d'une importante enquête en cours.

23.2. En 2025, le COC a ainsi travaillé pour environ 156 des 796 demandes traitées, **soit 19,6%**, avec une 'entité coordinatrice centrale' censée assurer les contacts avec le COC (venant de 10% en 2023 et 11% en 2024). Nous constatons que ces désignations deviennent de plus en plus fréquentes, ce qui peut pour une part être mis en relation avec l'augmentation du nombre de dossiers et de leur complexité ainsi qu'avec le souhait du COC de garder les délais de traitement sous contrôle.

23.3. La réalité est cependant moins engageante, et la qualité des 'évaluations intégrées' fournies (grâce auxquelles le COC n'est donc plus obligé d'analyser les évaluations des différentes entités pour se faire une idée de la situation) est très variable. Le but n'est en effet pas que l'entité coordinatrice se cantonne à un rôle de 'boîte aux lettres' et se contente de transmettre au COC les évaluations des différentes entités, qui se comptent parfois par dizaines. Son rôle consiste avant tout à compiler toutes les évaluations afin d'en distiller cette fameuse évaluation intégrée. Que ce soit dans les faits ou sur le plan de la qualité, il reste un long chemin qu'il faudra nécessairement parcourir, notamment à la lumière de l'évolution inéluctable vers un système dans lequel le citoyen pourra exercer ses droits directement auprès de la police (voir plus loin les points 25 à 26.3 inclus).

24. C'est sur la base de ces dossiers que le COC a dû à nouveau constater en 2025, tout comme les années précédentes, que même la BNG contient encore trop d'inexactitudes ou d'erreurs, alors qu'il s'agit justement de la banque de données qui contient ou devrait contenir uniquement des données dites

validées[42]. Inutile de dire qu'il y a largement de quoi s'inquiéter de la qualité des autres banques de données policières.

25. En 2025 également, le COC s'est heurté à la problématique induite par les limites qui lui sont imposées dans sa possibilité d'informer le citoyen lors de la clôture de l'enquête. Le COC n'est toujours pas autorisé à communiquer quoi que ce soit du contenu ni à formuler de motivation dans un sens ou dans l'autre. Une personne concernée dispose néanmoins aussi d'un recours contre le responsable du traitement lui-même (le(s) ministre(s) de l'Intérieur et/ou de la Justice et/ou le chef de corps), même si ce moyen de droit n'est pour ainsi dire jamais utilisé dans la pratique. Comme nous l'indiquions dans les rapports d'activité de 2021, 2022, 2023 et 2024, la Cour de Justice de l'Union européenne à Luxembourg a rendu le 16.11.2023 un arrêt de principe 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, estimant que:

«1. L'article 17 de la directive (UE) 2016/680 …, lu en combinaison avec l'article 46, paragraphe 1, sous g), l'article 47, paragraphes 1 et 2, et l'article 53, paragraphe 1, de cette directive ainsi qu'avec l'article 8, paragraphe 3, et l'article 47 de la Charte des droits fondamentaux de l'Union européenne, doit être interprété en ce sens que, lorsque les droits d'une personne ont été exercés, en application dudit article 17, par l'intermédiaire de l'autorité de contrôle compétente et que cette autorité informe ladite personne du résultat des vérifications opérées, cette dernière doit disposer d'un recours juridictionnel effectif contre la décision de ladite autorité de clôturer le processus de vérification.

2. L'examen de la seconde question[43] n'a révélé aucun élément de nature à affecter la validité de l'article 17, paragraphe 3, de la directive 2016/680.».

Cet arrêt, lu en combinaison avec l'avis de l'avocate générale, conduit **à la conclusion que la Belgique devrait renoncer à son système d'accès indirect** et, à l'instar de tous les autres États membres de l'UE, **prévoir (également) dans la loi la possibilité pour le citoyen d'exercer ses droits directement auprès des services de police** responsables du traitement (ou des ministres compétents) et, à titre subsidiaire, indirectement auprès du COC. En résumé, la Cour estime que:

[42] Contrairement par exemple aux banques de données de base, le terme «validées» 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.

[43] Cette question de la Cour d'appel de Bruxelles était formulée comme suit: «*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 n'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?*».

1) l'exception aux droits de la personne concernée ne peut **pas** être la règle;

2) la personne concernée doit pouvoir exercer ses droits à titre **primaire** vis-à-vis du responsable du traitement (c'est-à-dire en l'occurrence les services de police belges ou les ministres);

3) l'accès indirect (c'est-à-dire par l'entremise de l'Organe de contrôle en sa qualité d'autorité de contrôle) est une **garantie (un droit) complémentaire** à laquelle (auquel) la personne concernée peut recourir;

4) les informations qui sont communiquées à la personne concernée ne peuvent **pas** être limitées de manière générale et systématique à la communication minimale qu'il *«a été procédé aux vérifications nécessaires»*;

5) le résultat du contrôle qui est communiqué par le COC à la personne concernée dans le cadre de l'accès indirect est une 'décision' contre laquelle la personne concernée peut former un recours juridictionnel.

26. Bien que l'arrêt de la Cour de Justice de l'Union européenne date de novembre 2023, aucune initiative n'a encore été prise depuis lors (jusqu'à la clôture du présent rapport d'activité à la mi-avril 2026) pour mettre la législation belge en conformité avec cet arrêt. Dans l'arrêt définitif qu'elle a rendu dans cette affaire le **24 juin 2025**, la Cour d'appel de Bruxelles confirme pourtant les principes énoncés plus haut en estimant, après avoir pris connaissance de l'arrêt de la Cour de Justice de l'Union européenne qui revêt pour elle un caractère contraignant (soulignement du COC) que:

*«**11**. Il ressort de l'arrêt préjudiciel de la Cour de Justice de l'U.E. que la directive 216/680 n'a **pas** fait l'objet d'une **transposition adéquate par le législateur belge** …*

***12**. Ces enseignements appellent une **nécessaire intervention du législateur** pour veiller à une transposition adéquate de l'article 17 de la directive 2016/680, lu en combinaison avec l'article 46, §1, sous g), l'article 47, §§ 1 et 2, et l'article 53, §1, de cette directive, ainsi qu'avec l'article 8, §3, et l'article 47 de la Charte, tels qu'interprétés par la Cour de Justice de l'U.E. dans les attendus reproduits ci-dessus de l'arrêt préjudiciel du 13 novembre 2023. Il appartient en effet au législateur de déterminer, dans l'exercice de sa compétence discrétionnaire, les moyens adéquats de transposition …*

***13**. Il ne peut être fait droit aux demandes des appelants … et ce, pour des motifs qui résultent des articles 211 et suivants de la loi précitée du 30 juillet 2018 et du principe de droit constitutionnel de la séparation des pouvoirs … Enfin, le principe de **la séparation des pouvoirs s'oppose à ce que la cour se substitue au pouvoir législatif** qui dispose de la compétence discrétionnaire du choix des moyens permettant de transposer adéquatement la directive 2016/680 dans le respect de l'arrêt préjudiciel. Il suit de ce qui précède que l'action originaire et les demandes formées par les appelants devant la cour après l'arrêt de la Cour de Justice de l'U.E. ne sont **pas recevables** et que l'ordonnance a quo est confirmée.».*

Les requérants ont décidé de ne pas se pourvoir en cassation, de sorte que ce verdict est définitif.

26.1. Tant le citoyen qui introduit une demande d'accès que le COC en sa qualité d'autorité de contrôle se trouvent donc dans une impasse inextricable dès lors qu'il est d'une part établi que la législation belge est contraire aux normes supérieures de l'Union européenne et viole donc depuis 2018 les droits de chaque ressortissant, mais qu'il est d'autre part impossible pour le juge d'y remédier aussi longtemps que le législateur ne sera pas intervenu. Indéniablement, la police exerce toujours des pressions pour échapper à l'accès direct et à sa propre responsabilité en renvoyant la 'patate chaude' au COC en sa qualité d'autorité de contrôle. Pour la police, il est évidemment très confortable de pouvoir tout simplement transmettre au COC chaque demande ou requête et de ne devoir elle-même entreprendre aucune démarche, si ce n'est après l'intervention du COC. À cet égard, il est d'ailleurs plus préoccupant encore de constater que les autorités de police et les autorités de tutelle continuent à jouer le jeu et ne montrent absolument aucune hâte à initier l'indispensable réforme qui permettra d'instaurer le système de l'accès direct auprès de la police.

Cette tendance du pouvoir exécutif à ignorer tout bonnement la jurisprudence européenne et nationale est manifestement devenue la 'nouvelle normale' et constitue en tout état de cause une évolution particulièrement regrettable dans différents domaines du droit et différentes matières, qui touche donc à présent aussi le droit de la protection des informations et données policières. Une nouvelle fois et au risque de se répéter, le COC insiste pour que les responsables politiques fassent au plus vite le nécessaire pour restaurer l'État de droit.

26.2. Dans un contexte international, enfin, il vaut la peine de mentionner les procédures dans lesquelles l'*European Data Protection Supervisor* (*EDPS*, le contrôleur européen d'agences européennes comme Europol et Eurojust) sollicite la coopération du COC lorsqu'une personne concernée introduit un recours auprès de l'*EDPS* contre une décision d'Europol concernant (généralement une restriction de) l'exercice de ses droits en matière de protection des données (droit d'accès, rectification, etc.).

26.3. Il convient d'attirer l'attention sur le fait qu'en vertu du Règlement Europol 2016/794, le système de l'accès direct s'applique aussi à l'égard d'EUROPOL (ainsi que de ses traitements de données et banques de données). Le COC et le citoyen se retrouvent ainsi dans une situation ambivalente dans laquelle, en présence d'une requête adressée par une même personne à la fois au COC et à EUROPOL – pour autant évidemment qu'EUROPOL dispose d'informations 'belges' –, le COC doit répondre par une décision finale vide de contenu en indiquant qu'il *«a été procédé aux vérifications nécessaires»*, alors qu'EUROPOL peut de son côté communiquer (et communique parfois) à la personne concernée la teneur de ces mêmes informations 'belges'. Un citoyen a donc en réalité tout intérêt – surtout s'il soupçonne l'existence de flux de données internationaux – à adresser simultanément sa demande au COC et à EUROPOL, puisqu'il a au moins auprès de ce dernier une chance d'obtenir des informations de contenu que le COC n'est pour sa part pas autorisé à communiquer ni à divulguer … Cette situation éveille à tout le moins chez le sujet de droit l'impression que l'Organe de contrôle 'tait' des informations qu'EUROPOL est par contre en mesure de lui fournir. Pour cette raison également, il est plus qu'urgent d'introduire en droit belge le système de l'accès direct afin de s'aligner sur le système d'EUROPOL.

2.2. Les demandes d'informations et d'avis

27. Le COC a continué en 2025 à fournir des informations et des avis aux professionnels – faisant la plupart du temps (dans 78% des cas) partie de la police, mais pas toujours – concernant des questions ayant trait principalement à la protection de la vie privée et à la protection des données, des problèmes d'application des règles du droit de police et de la gestion de l'information, des questions de compétence, etc. Il arrive régulièrement qu'il s'agisse de questions qui devraient plutôt être posées au Ministère public, dès lors qu'elles se rapportent à des compétences de recherche ou à

d'autres aspects du droit de la procédure pénale. La rotation relativement importante des délégués à la protection des données (DPO) fait aussi qu'il s'impose parfois d'expliquer aux nouveaux DPO le b. a.-ba du droit de la protection des informations et données policières.

27.1. Une question peut aussi 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 – 5 au total en 2025 – ont pour objectif de fournir à la GPI des lignes directrices et un cadre (juridique) sur certains thèmes, comme la réalisation de *screenings* par les services de police dans le cadre de 'journées d'information', 'journées de recrutement' ou autres 'jobdays' (force étant de constater qu'il est régulièrement procédé dans ce contexte à des *screenings* illégaux de toutes les personnes intéressées), l'impossibilité pour un membre du personnel CALOG de prendre part à une observation mise en place au titre de MPR, etc.

27.2. Le COC ne dispose pas d'une capacité suffisante pour non seulement transmettre les avis au(x) demandeur(s), mais pour aussi les mettre à la disposition de toute la GPI sous une forme adaptée (anonymisée), sachant que cela nécessite de les traduire[44], de les anonymiser, de procéder à leur chargement technique, etc.

28. Le demandeur était dans 35 cas un membre de la GPI. Parmi ces cas, il s'agissait 24 fois du DPO, 8 fois d'un autre membre de l'entité de police concernée et 3 fois du chef de corps. Parmi les autres demandes d'avis, 2 émanaient d'autorités de police, 2 d'une autorité autre qu'une autorité de police (l'INAMI[45] et la BCSS[46]), 2 d'une autre autorité de contrôle (le Comité P et l'AIG), 3 de citoyens, 1 d'un syndicat de la police et 1 d'un avocat.

Sept (7) demandes d'avis ont été formulées par des fonctionnaires de police en formation (aspirants commissaires, aspirant inspecteurs principaux, …) dans le cadre de diverses missions d'enseignement. Bien que l'assistance dans le cadre de missions d'enseignement ne figure pas parmi les missions légales et encore moins parmi les priorités du COC, l'Organe de contrôle s'efforcera toujours d'aider le demandeur, ou

[44] 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.
[45] L'Institut national d'assurance maladie-invalidité.
[46] La Banque Carrefour de la Sécurité Sociale.

du moins de le mettre sur la bonne voie (parfois même en organisant une réunion *Teams* parce que la question est trop complexe pour y répondre par e-mail ou par courrier)[47]. Le but n'est évidemment pas que le COC rédige le mémoire ou l'article du candidat à sa place, même s'il semble parfois, à analyser de plus près la demande formulée, que ce soit précisément ce que le demandeur espère obtenir. Inutile de dire que dans ce cas de figure, le demandeur est éconduit par le COC.

Le COC doit encore régulièrement rappeler qu'il lui est impossible d'être 'le juriste' et/ou 'le spécialiste de la protection de la vie privée' de (tous les membres de) la GPI. Le fait que les membres de la GPI continuent à contacter directement le COC et pas (d'abord) la propre organisation interne et/ou les autorités de police et/ou les ministres de tutelle (les responsables du cadre réglementaire, et de surcroît également les responsables du traitement) prouve l'absence cuisante – que nous évoquions déjà dans notre précédent rapport d'activité – d'un service juridique transversal à part entière à l'échelle de la GPI (soit au sein de la police fédérale, soit au sein du SPF Intérieur). En tout état de cause, il demeure indispensable que la GPI fasse d'abord intervenir ses canaux internes, et au moins son propre délégué à la protection des données (DPO), avant de contacter le COC. Il s'agit là d'un message que le COC s'efforce de faire passer depuis 2018, notamment sur son site Internet, mais malheureusement encore souvent sans succès.

29. Le volume relativement constant des demandes d'avis au fil des années prouve que le COC est considéré comme **le** centre d'expertise par excellence en la matière. La capacité et l'expertise nécessaires pour apporter une réponse de qualité à ces demandes restent cependant un défi de taille. **61 demandes d'avis** (autres que celles se rapportant à l'utilisation de caméras, cf. infra) ont été introduites en 2025[48]. Ce nombre est en baisse par rapport à 2024 (81) et renoue ainsi avec le niveau des années 2021 à 2023 incluse.

Le COC intervient aussi très souvent de manière **informelle** (avis téléphonique, réunions *Teams*, réponses directes par e-mail sans enregistrement dans le système de gestion des dossiers du COC, etc.). En 2025, **141 avis écrits ont à nouveau été**

[47] Voir également le même constat pour les demandes d'avis relatives aux traitements par caméra, au point 45.
[48] Dont 59 étaient clôturées début avril 2026.

rendus de cette manière (pour 73 en 2023 et 119 en 2024, soit **une hausse de 93%**), dont 26 à la demande de membres de la GPI, et au moins **36 réunions *Teams*** ont eu lieu. Le recours à cette dernière forme d'avis – interactive, verbale et à fort coefficient de travail – se stabilise ainsi au niveau de 2023 (après un record de 69 réunions *Teams* en 2024). Vu la technicité et la complexité de la matière, une réunion en direct permet en effet à l'Organe de contrôle de fournir des analyses, des réponses et des avis (immédiats) beaucoup plus approfondis et plus complets.

30. Pour 2025, le **délai de traitement moyen était de 33 jours** et s'aligne donc sur celui des années précédentes (respectivement 31, 35 et 39 jours en 2022, 2023 et 2024). Le COC s'efforce toujours de prendre comme principe un délai de réponse de 1 mois. En la matière, la médiane – qui était de 17 jours en 2025 (venant de 21,5 jours en 2023 et 20 jours en 2024) – constitue un meilleur indicateur encore.

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

Tableau 5: Demandes d'avis sur la législation et la réglementation entre 2018 et 2025

2018	2019	2020	2021	2022	2023	2024	**2025**
12[49]	22[50]	15	33	39	49	36	**26**

31. L'importante compétence d'avis sur les projets de réglementations (lois, décrets/ordonnances, 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 peut aussi concerner des projets des entités fédérées (décrets, ordonnances, arrêtés des gouvernements fédérés, …).

32. La problématique que nous avions déjà évoquée dans notre précédent rapport d'activité, à savoir le fait que les entités fédérées ne sollicitent pas l'avis du COC lorsque les règles et/ou la pratique de la gestion de l'information policière et du

[49] 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.
[50] *Ibidem.*

fonctionnement de la police sont directement ou indirectement impactées, est toujours d'actualité, surtout pour les projets de réglementations des autorités flamandes.

Cette situation engendre des effets problématiques, dont un conflit entre les (projets de) règles des entités fédérées et les règles fédérales qui régissent cette matière et qui doivent toujours prévaloir et/ou l'impact réel de ces (projets de) réglementations sur le fonctionnement et le financement des services de police. Souvent, ces derniers n'ont pas été consultés durant le processus d'élaboration et n'étaient absolument pas demandeurs de ces réglementations, sans compter qu'ils ne sont pas non plus financés par les entités fédérées. L'organisation et les attributions de la GPI ainsi que le statut des membres de son personnel sont en effet, en vertu de l'article 184 de la Constitution, réglés par la loi fédérale (formelle).

33. En 2025, le COC a reçu **26 demandes d'avis** et a effectivement rendu **13 avis**. Pour les 13 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 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.

33.1. Sur les 13 avis émis en 2025, **1 était négatif**. Le COC n'émet un avis négatif que dans les cas où la nature des remarques et objections fait que le texte soumis n'est pas acceptable ou ne saurait être corrigé sans des modifications fondamentales.

33.2. Dix-sept (17) demandes d'avis ont été (également[51]) transmises par l'APD, dont 1 seulement provenait des entités fédérées, ce qui démontre – si besoin est – la nécessité pour les entités fédérées de transmettre également leurs (projets de) réglementations pour avis au COC. Douze (12) demandes d'avis ont été reçues directement de l'autorité sollicitant l'avis.

La diminution observée par rapport aux années précédentes est principalement à attribuer à une combinaison de plusieurs facteurs: (1) le fait que le gouvernement a

[51] Certaines demandes d'avis sont en effet transmises à la fois directement par le demandeur et indirectement par l'intermédiaire de l'APD.

été en affaires courantes jusqu'en février 2025, (2) la période de démarrage du nouveau gouvernement, (3) un gouvernement moins actif que les années précédentes sur le plan de la création de nouvelles réglementations, et (4) la diminution significative du nombre de demandes émanant des entités fédérées.

34. Les avis sont disponibles pour consultation sur le site Internet du COC (www.organedecontrole.be), de manière à ce que non seulement le grand public, mais aussi toutes les parties prenantes puissent en prendre connaissance. Pour les avis importants et les avis négatifs, le COC prévoit également dans la mesure du possible une communication sur LinkedIn. Principalement par manque de capacité, le COC n'est pas présent sur d'autres réseaux sociaux. Le COC n'a en effet **pas** de collaborateur en charge de la communication.

35. Ces avis font l'objet d'une discussion et d'une approbation au sein du DIRCOM et doivent être rendus dans un délai de 60 jours, ou de 15 jours en cas d'urgence motivée. En 2025, le **délai de traitement moyen** était de **29 jours** (médiane: 22 jours), un chiffre qui doit cependant être nuancé dès lors que cette moyenne a été abaissée par le nombre de dossiers dans lesquels le COC ne rend pas d'avis et qui peuvent donc généralement être clôturés plus rapidement.

Si nous considérons uniquement les dossiers dans lesquels un avis a effectivement été rendu, nous obtenons un **délai de traitement moyen de 51 jours**, ce qui prouve – si besoin est – que le délai légal de 60 jours n'a pas été calculé avec trop de largesse. Pour une part, ce délai s'explique dans le cas du COC également par le temps nécessaire à la réalisation en sous-traitance des traductions et à leur contrôle (généralement quelques semaines).

2.4. Les plaintes

36. Les dossiers de plaintes ont trait pour une part à des traitements (prétendument) illicites de la part de membres de la GPI. Ces plaintes sont introduites par des citoyens ou par des collègues fonctionnaires de police 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[52], ou a effectué d'autres traitements illicites. Les plaintes peuvent par ailleurs avoir trait à la thématique plus vaste de la licéité des traitements de données, qu'il s'agisse de traitements relevant du RGPD ou de la *LED*.

36.1. Les plaintes de victimes (prétendues) de **fraudes d'identité** se multiplient; si le COC en avait reçu 7 en 2024, **il en a dénombré pas moins de 16 en 2025**. Les victimes en question ne comprennent pas (1) que la police soit apparemment impuissante face aux agissements du fraudeur, mais surtout (2) qu'elle ne parvienne pas à mettre un terme aux problèmes qu'elles rencontrent (comme le fait qu'elles soient systématiquement soumises à des vérifications approfondies en cas de contrôle de police ou lorsqu'elles veulent franchir la frontière, qu'elles soient 'emmenées à l'écart' au vu et au su de leur famille, de leurs amis et de leurs éventuelles relations d'affaires pour être soumises à un contrôle et à une fouille, au risque de manquer l'avion, une réunion importante, etc.).

36.2. Comme nous l'indiquions dans notre rapport d'activité de 2024, le COC a été assigné en justice par une victime de fraude d'identité qui lui reprochait de ne pas avoir, en sa qualité d'autorité de contrôle, consenti dans le cadre du traitement de sa plainte et de la décision finale des efforts suffisants pour résoudre son problème et mettre un terme aux problèmes qu'il rencontrait lors de voyages internationaux, et/ou pour obliger la police à faire le nécessaire. Le plaignant a introduit le 12 juillet 2024 un recours contre la décision motivée rendue le 3 juin 2024 par le COC. La question a finalement été tranchée par la Cour d'appel de Bruxelles dans un arrêt du 24 mars 2025[53], qui a débouté le plaignant de toutes ses demandes à l'égard du COC. Sur invitation du COC, la Cour a également rendu à cette occasion une décision de principe essentielle en estimant que le traitement par la police d'un 'alias' est licite, légalement obligatoire et inévitable, même si cela engendre (régulièrement) des désagréments pour la victime.

[52] 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.
[53] Bruxelles (1re chambre francophone), dossier W.H contre l'Organe de contrôle de l'information policière, numéro de rôle 2024/RG/1264, *non publié*. Cet arrêt est définitif.

La problématique de la fraude d'identité et du traitement de ces dossiers par la police n'en demeure pas moins délicate, s'agissant d'une matière dans laquelle l'intervention de la police laisse dans la pratique encore largement matière à amélioration. Le COC finalisera en 2026 le rapport du contrôle thématique qu'il a réalisé à ce sujet. Le traitement de ce type de dossiers représente un travail énorme, en particulier en présence de plusieurs alias et d'interventions de plusieurs entités de police.

36.3. Le traitement de dossiers de plaintes prend du temps, nécessite des investigations poussées et ne se prête pas (ou plus) à un traitement plutôt informel et/ou souple. Ce constat est dû aux exigences formelles imposées à la fois pour la décision et pour la constitution d'un dossier administratif. Le COC est en effet soumis pour sa décision finale à un devoir de motivation formelle et matérielle, ce qui l'oblige à accorder une attention particulière au respect des principes généraux de bonne administration. Dans son arrêt du 6 novembre 2023 (arrêt n° C.23.0092.N), la Cour de cassation a confirmé que le COC est une autorité administrative soumise aux principes généraux de bonne administration. La jurisprudence de la Cour de Justice de l'Union européenne ne laisse elle non plus planer aucun doute sur les missions de l'autorité de contrôle: *«L'autorité de contrôle doit procéder au traitement d'une telle réclamation avec toute la diligence requise.»*[54].

Cela implique inévitablement que les délais de traitement se sont effectivement à nouveau allongés en 2025 (voir plus loin le point 38).

Six (6) plaintes ont été transmises par une autre autorité de contrôle, dont 4 par le Comité P, 1 par l'APD et 1 par la Vlaamse Toezichtcommissie (VTC), la commission flamande en charge du contrôle de l'application du RGPD.

[54] CJUE 26 septembre 2024, C-768/21, considérant 32 avec référence à l'arrêt SCHUFA Holding, C-26/22 et C-64/22, considérant 56, ainsi qu'à la jurisprudence citée.

<u>Tableau 6:</u> 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
2023	16	18	34
2024	12	22	34
2025	**19**	**41**	**60**

Le nombre total de dossiers de plaintes **<u>a pour ainsi dire doublé</u>** par rapport aux années précédentes. Le tableau ci-après présente la suite donnée à ces dossiers de plaintes par le COC, à la mi-avril 2026:

<u>Tableau 7:</u> Suite donnée par le COC aux dossiers de plaintes[55]

Suite donnée	2020	2021	2022	2023	2024	**2025**
Sans suite: COC pas compétent	5	4	6	1	1	**5**
Sans suite: plainte irrecevable[56]	3	3	4	3	3	**4**
Sans suite: pas d'objections	11	1	1	1	1	**0**
Sans suite: plainte manifestement non fondée	4	0	2	1	1	**3**
Sans suite: pas de coopération du plaignant	10	8	7	5	12	**14**
Sans suite: autre service déjà en charge du traitement	3	1	3	3	0	**1**
Sans suite: traitement non opportun[57]	4	1	2	2	2	**3**
Traitement conforme	3	4	7	4	11	**9**
Rectification d'office[58]	0	0	0	0	0	**2**

[55] À la date de clôture du présent rapport d'activité à la mi-avril 2026.
[56] Par exemple parce qu'il s'est finalement avéré que la plainte n'était pas dirigée contre un fonctionnaire de police.
[57] Par exemple en raison d'une enquête disciplinaire ou pénale en cours dans laquelle le COC ne souhaite pas s'immiscer.
[58] Cela signifie que le COC, en marge des demandes spécifiques d'un plaignant ou d'un demandeur, fait également procéder d'office à certaines rectifications.

Ordre de traitement conforme	0	2	0	1	0	**0**
Sous-traitant réprimandé	0	1	0	0	0	**0**
Avertissement au responsable du traitement	2	0	0	0	1	**0**
Ordre de rectification	1	0	0	0	0	**1**
Ordre d'effacement	1	0	0	0	0	**1**
Ordre de limitation du traitement définitive	0	0	0	1	0	**0**
Transmission à la hiérarchie policière	7	0	4	2	1	**4**
Transmission au ministère public	3	0	1	0	1	**0**
Procès-verbal dressé	4	1	2	0	0	**0**
Mesure interne prise par la GPI	0	1	1	0	0	**0**
Ouverture d'une enquête disciplinaire	5	1	2	0	0	**0**
Total	66	28	42	24	34	**47**

37. La grande **majorité** des plaintes sont soit **non fondées**, soit le plaignant n'offre **(plus) aucune coopération**.

Vu le fort coefficient de travail des plaintes relatives à des consultations illicites réalisées par des fonctionnaires de police, le COC se limite 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 traitement par le COC lui-même – transmis au chef de corps/directeur.

38. Le **délai de traitement moyen** des dossiers de plaintes était de **102 jours** en 2025 (médiane: 68 jours). L'augmentation observée en 2024 (95,4 jours) se poursuit donc, alors que les délais de traitement avaient encore tendance à diminuer entre 2021 et 2023 (74 jours en 2021, 73 jours en 2022 et 61,85 jours en 2023).

Vu l'évolution de la jurisprudence quant aux attentes (légales) à l'égard d'une autorité de protection des données, les exigences imposées pour le traitement de chaque plainte, l'exigence de conformité aux principes généraux de bonne administration, dont les droits de la défense (*fair play*) et le fait que chaque décision peut être

attaquée en justice, le traitement de ces dossiers prend immanquablement de plus en plus de temps et monopolise de plus en plus de capacité (tant pour l'enquête que pour le traitement juridique formel).

Sachant cela, un délai de traitement moyen d'un peu plus de 3 mois reste dans l'ensemble un excellent résultat.

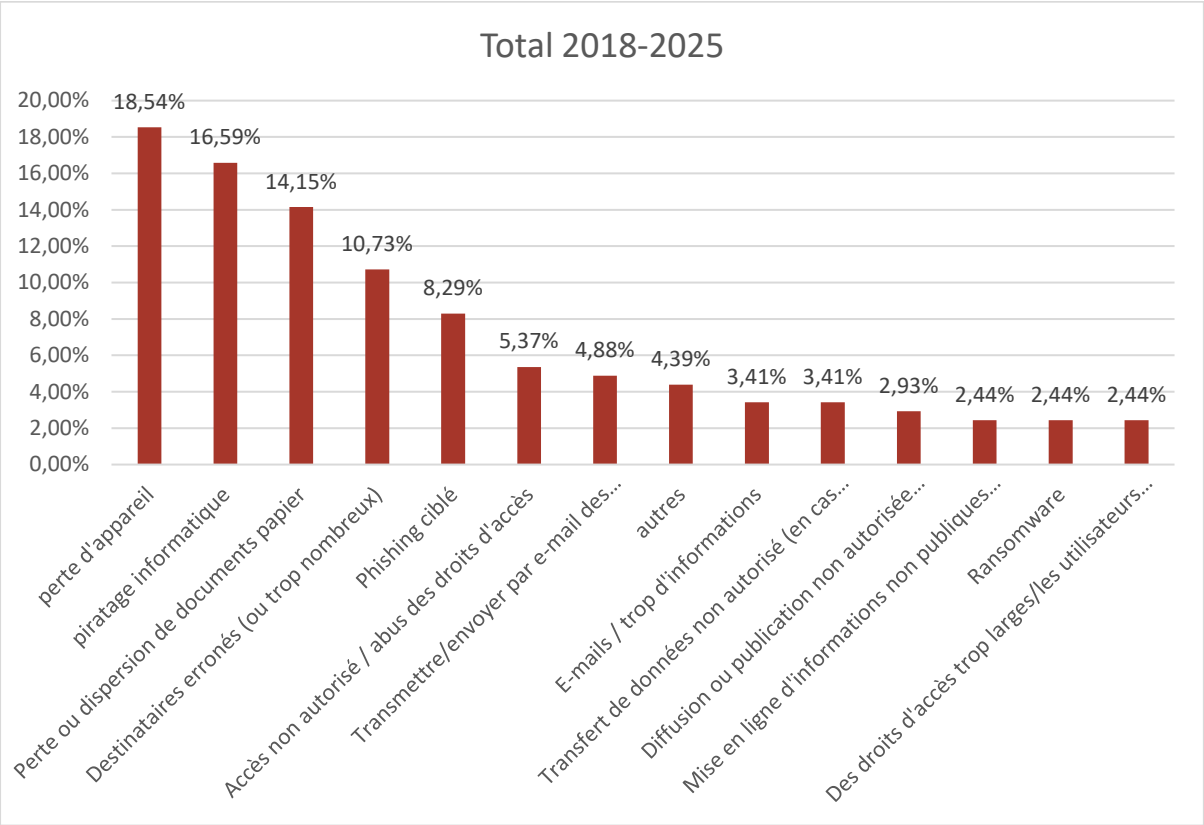
2.5. Les brèches de sécurité (databreach)

39.1. En 2025, **42 brèches de sécurité** ont été notifiées au COC par la GPI. Ce nombre dépasse légèrement celui rapporté pour 2023 (40), qui était le plus élevé depuis le lancement de l'Organe de contrôle en tant qu'autorité de protection des données en 2018. 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 (1) ETP informaticien**. Le COC limite donc en principe son examen à la question de savoir si la brèche a été correctement traitée, si toutes les mesures requises avaient été prises au préalable pour en empêcher la survenance et si toutes les mesures requises ont été prises par la suite pour (tenter d')empêcher que de telles brèches se reproduisent encore et pour en limiter le plus possible les effets préjudiciables.

39.2. Concrètement, il s'agit de cas de *hacking*, de perte ou de vol d'un appareil ou de documents sur papier, de *phishing* ciblé, de divulgation en ligne d'informations non publiques, d'accès trop étendus ou non autorisés, de mots de passe compromis, d'abus de droits d'accès, etc. (voir plus loin le tableau 8)

<u>Tableau 8:</u> Catégories de brèches de sécurité notifiées depuis le lancement du COC en tant qu'autorité de protection des données spécialisée en 2018



39.3. Onze (11) brèches de sécurité ont été notifiées par la police fédérale et 31 par la police locale. Sur le plan du contenu, il s'agissait à 18 reprises d'une matière relevant du RGPD (autrement dit, l'infraction avait trait à des données à caractère personnel non opérationnelles) et à 36 reprises d'une matière relevant de la *LED* (autrement dit, l'infraction avait trait à des données à caractère personnel opérationnelles)[59]. Très souvent, il n'est plus possible de déterminer s'il y a bien eu une brèche de sécurité, ni le cas échéant quelles données en faisaient l'objet (et se sont donc perdues, ont fait l'objet d'une violation de la confidentialité, etc.).

<u>Tableau 9:</u> Nombre de brèches de sécurité notifiées par an

2019	2020	2021	2022	2023	2024	**2025**
17	17	20	25	40	38	**42**

[59] Une même notification peut relever à la fois du RGPD et de la *LED*.

2.6. Les enquêtes internationales

40. Le COC est également sollicité pour prendre part à des enquêtes internationales. Vu sa capacité limitée, le COC est réticent à prendre part à des enquêtes internationales et se montre très sélectif à cet égard.

40.1. En ce qui concerne les évaluations SCHEVAL (Schengen)[60], un commissaire-enquêteur du COC a pris part en 2025 à l'évaluation Schengen de la Bulgarie en tant que membre de l'équipe d'enquête. Celle-ci s'est déroulée sur place du 9 au 14 novembre 2025, après quoi un travail considérable doit encore être accompli pour l'établissement du rapport. Le membre du personnel concerné faisait partie de l'équipe d'évaluation *«Data Protection»*, qui opérait aux côtés des équipes *«Internal Security»*, *«Visa Policy»*, *«Return»* et *«Border Management»*).

Pour des raisons de capacité, le COC tente de limiter sa participation en prenant part non pas chaque année, mais seulement tous les 2 ans à une évaluation SCHEVAL et de faire ainsi preuve de la solidarité attendue. Dans l'intervalle, un pôle d'experts a été constitué à l'échelle de l'UE, et quatre membres du personnel du COC en font entretemps partie. D'un autre côté, le COC acquiert dans le cadre de ces évaluations une expérience très précieuse qui peut se révéler particulièrement utile par la suite. Dans le cadre de l'évaluation Schengen dont la Belgique fera l'objet à la mi-2026, le membre du personnel qui a pris part à l'évaluation SCHEVAL de la Bulgarie sera ainsi également chargé de défendre ce dossier pour le COC en ce qui concerne le volet relatif à la protection des données.

2.7. Protection des données dans des secteurs et matières spécifiques

2.7.1. Contrôle spécial: les contrôles UIP

41. 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 n'a

[60] Règlement (UE) 2022/922 du Conseil du 9 juin 2022 relatif à la création et au fonctionnement d'un mécanisme d'évaluation et de contrôle destiné à vérifier l'application de l'acquis de Schengen, et abrogeant le règlement (UE) n° 1053/2013.

pas été procédé en **2025** à une enquête auprès de l'Unité belge d'Information des Passagers (UIP ou 'BELPIU'). Ce constat est surtout à mettre en relation avec la nécessité, pour le COC, d'établir des priorités.

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

42. Le COC a été investi en 2019 d'une **nouvelle compétence** à l'égard du service Recherche de l'AGD&A[61] dans le cadre des réquisitions adressées à la BELPIU dans des matières fiscales. L'article 281 §4 de la loi générale sur les douanes et accises du 18 juillet 1977 prévoyait initialement un contrôle et une vérification *a posteriori* de ces réquisitions en fonction des principes de subsidiarité et de proportionnalité. En 2024, la loi du 16 mai 2024 modifiant la loi du 25 décembre 2016 relative au traitement des données des passagers (parue au Moniteur belge le 05.07.2024) a converti la compétence de contrôle *a posteriori* du COC en une **compétence d'autorisation préalable**[62].

Concrètement, cela signifie que le COC décide dans ces dossiers si la demande du conseiller général est ou non recevable et fondée et peut ou non être transmise par l'AGD&A à la BELPIU (l'Unité d'Information des Passagers). En 2025, le COC n'a toutefois reçu **aucune demande d'autorisation préalable** de la part de l'AGD&A. Le COC présume que l'AGD&A a en 2025 fait uniquement appel au Ministère public pour obtenir ces renseignements. Reste à voir si cette tendance se confirmera en 2026.

---

[61] L'Administration générale des Douanes et Accises.

[62] *«§ 4. Dans les conditions fixées à l'article 27 de la loi du 25 décembre 2016 relative au traitement des données des passagers, un fonctionnaire ayant le titre de conseiller général, désigné par l'Administrateur général des Douanes et Accises, peut soumettre 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, une demande d'accès aux données des passagers.* ***L'Organe de contrôle de l'information policière examine le bien-fondé de la demande en veillant à assurer un juste équilibre entre les intérêts en cause et décide si la demande peut être transmise à l'Unité d'Information des Passagers.***
En cas d'urgence dûment justifiée, le fonctionnaire visé à l'alinéa 1er peut requérir directement du fonctionnaire dirigeant de l'UIP la communication des données des passagers nécessaires. ***Il communique sa demande écrite et motivée ainsi que les données recueillies sans délai et au plus tard dans les 24 heures à l'Organe de contrôle de l'information policière. Ce dernier interdit à l'Administrateur général des Douanes et Accises de traiter les données recueillies si les conditions légales n'ont pas été respectées et ordonne l'effacement immédiat des données.****».*

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

43. Pour des raisons de priorisation, le COC n'a **pas** mené en 2025 d'enquêtes spécifiques au sujet de la gestion de l'information de l'AIG. Le COC partage sa compétence de contrôle à l'égard de l'AIG 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).

2.8. Utilisation de caméras par les services de police

2.8.1. Généralités

44. Le COC est investi d'une mission de contrôle à l'égard de toute forme d'utilisation de caméras, tant visible que non visible (cachée). Vu l'augmentation constante et même spectaculaire du nombre de caméras – **on dénombrait fin 2025 aux alentours de 17.000 caméras de surveillance fixes (temporaires) et caméras *ANPR*, sans compter les (milliers de) *bodycams* et les caméras montées sur des *drones*** –, le COC ne saurait bien évidemment en aucun cas procéder dans tout le pays à un contrôle proactif de l'utilisation des caméras. Ce contrôle doit être exercé avant tout à l'initiative des corps de police eux-mêmes, et ensuite de leurs autorités de police administrative et judiciaire. Quelques rares exceptions mises à part, le COC constate toutefois que ces autorités laissent généralement aux chefs de corps toute liberté de déployer des caméras comme bon leur semble. Les autorités administratives sont même les véritables instigatrices de ce déploiement, affirmant que 'le citoyen en est demandeur' … Même dans son rôle réactif, on peut s'attendre à ce que le COC ne soit de toute façon pas en mesure de faire face au nombre croissant de questions, de plaintes et de demandes d'accès dans le cadre de l'utilisation de caméras.

C'est en tout cas la tendance que l'on a vu sensiblement s'amorcer en 2025.

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

45. Les questions et demandes concernant l'utilisation de caméras sont (principalement) soumises par la GPI au COC. **26 demandes d'avis** ont été introduites à ce sujet en 2025. Ces demandes d'avis émanaient pour la plupart des corps de police (17), le plus souvent du DPO (13) et parfois du chef de corps (1), d'autres fonctionnaires de police (5) ou de fonctionnaires de police en formation auprès de l'ANPA (1). L'assistance dans le cadre de missions d'enseignement ne figure pas parmi les missions de l'Organe de contrôle, mais le COC constate souvent que l'aspirant n'a aucune autre institution à laquelle s'adresser et s'efforce donc de le mettre sur la bonne voie (voir plus haut le point 28).

Les membres du personnel de la GPI continuent à consulter directement le COC, sans recourir d'abord aux canaux internes (du DPO ou du service juridique), et parfois même à l'insu du DPO et a fortiori du chef de corps. Même 7 ans après son lancement en tant qu'autorité de protection des données, le COC est encore amené à prier les fonctionnaires de police de respecter la procédure de consultation standardisée, qui est expliquée sur le site Internet du COC et qui exige de s'acquitter d'abord en interne des démarches requises.

Certaines demandes d'avis émanaient également d'autres instances ou personnes, à savoir d'une autorité de police (1), d'une autorité autre qu'une autorité de police (1) ou de citoyens (5).

Entre le 25 mai 2018 (date de l'entrée en vigueur des nouvelles dispositions relatives à l'utilisation de caméras) et la fin 2025, le COC a traité **203 demandes d'avis** concernant cette thématique.

Deux avis d'initiative ont également été émis[63], à savoir:

- l'avis BD250018 du 30/09/2025 relatif à l'utilisation d'une *dashcam* à bord d'un véhicule de police;

[63] La rédaction de ces deux avis a été entreprise en 2025, bien que l'avis BD250022 n'ait été officiellement émis qu'en 2026.

- l'avis BD250022 du 26/02/2026 relatif au pilotage d'un *drone* de police par des membres de la police intégrée.

<u>Tableau 10:</u> Nombre de demandes d'avis ou d'informations concernant l'utilisation de caméras

Année	**Nombre**
2019	32
2020	29
2021	29
2022	32
2023	21
2024	34
2025	**26**
TOTAL	203

46. À cela s'ajoutent les analyses d'impact relatives à la protection des données ou **AIPD**[64] qui ont trait à des traitements par caméra et qui sont soumises au COC par les entités de police pour consultation préalable.

47.1. En 2025, **9 AIPD** ont été soumises pour analyse au COC dans le cadre de l'utilisation de caméras par la police, un nombre qui induit une légère augmentation par rapport à 2024 mais qui reste tout de même nettement inférieur à celui des années 2021 à 2023. Il arrive parfois qu'une analyse soit précédée d'une concertation entre le COC et le service de police afin de pouvoir mieux la préparer.

Le délai de traitement moyen d'une analyse *prima facie* était en 2025 de **68 jours** (pour 40 jours en 2024; médiane: 43 jours), ce qui constitue une augmentation. Cela peut à notre avis s'expliquer par le fait que si l'on peut d'une part affirmer d'une manière générale que le niveau de connaissances de la GPI dans le domaine de l'utilisation de caméras s'est significativement amélioré – notamment après 7 années d'assistance de la part du COC –, certains traitements (projetés) deviennent d'un autre côté plus complexes (avec davantage d'acteurs externes, davantage de flux de

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

données mixtes), ce qui complique également l'analyse (juridique). La réglementation de l'utilisation de caméras demeure en effet relativement complexe, en particulier lorsque l'on est en présence de plusieurs finalités, autorités et services et que différentes législations s'appliquent donc en même temps, comme la loi caméras de 2007 et la loi sur la fonction de police.

Tableau 11: Nombre d'AIPD soumises pour avis au COC concernant l'utilisation de caméras

Année	Nombre
2019	27
2020	10
2021	33
2022	28
2023	19
2024	7
2025	**9**

47.2. Une AIPD peut évidemment aussi avoir trait à d'autres traitements de données, et cela a été le cas en 2025 pour 3 déclarations. Deux d'entre elles, soumises par la police judiciaire fédérale, avaient trait à des outils d'analyse complexes du type *big data*, tandis que la troisième portait sur la nouvelle application 'Cross Arrest'. Celle-ci est une application informatique nationale (tel est du moins l'objectif final) destinée à l'enregistrement et au suivi des arrestations administratives et judiciaires conformément à l'article 33*bis* de la LFP et à l'arrêté d'exécution à paraître qui encadre cette application (dont la publication est prévue en 2026).

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 des autres autorités de contrôle. Vu leur impact sur le fonctionnement opérationnel

des services, l'exercice de ces compétences s'entoure de la circonspection de mise, mais toujours dans les contours définis par la jurisprudence de la Cour de Justice de l'Union européenne. Si d'une part, le COC ne peut ignorer les irrégularités constatées, il se refuse d'autre part à perturber de manière disproportionnée le fonctionnement opérationnel de la GPI. Cet exercice d'équilibre est à la fois difficile et délicat.

48.1. De plus, la marge dont une autorité de protection des données dispose pour appliquer ce que l'on pourrait appeler une 'politique de tolérance' est réduite du fait des verdicts rendus par la Cour de Justice de l'Union européenne, qui estime que l'autorité de contrôle est investie de l'obligation légale de *«garantir un niveau cohérent et élevé de protection des données à caractère personnel par une application rigoureuse des règles»* (soulignement du COC)[65] et que lorsqu'une telle autorité constate, à l'issue de son enquête, une violation des dispositions du règlement (NDLR: il s'agissait d'une application du RGPD), elle est *«**tenue*** (soulignement du COC) *de réagir de manière appropriée afin de remédier à l'insuffisance constatée, toute mesure devant, (…), notamment être appropriée, nécessaire et proportionnée en vue de garantir le respect dudit règlement, compte tenu des circonstances de l'espèce»*[66]. L'autorité de contrôle dispose donc en effet, de l'avis de la Cour, d'une certaine marge d'appréciation quant à la manière dont il **doit** être remédié à l'insuffisance constatée, mais *«cette marge d'appréciation est cependant limitée par la nécessité de garantir un niveau cohérent et élevé de protection des données à caractère personnel par une application rigoureuse des règles»* (soulignement du COC)[67].

Une mesure correctrice du COC n'est pas une 'sanction' et n'a pas pour but de 'punir'; son unique objectif est de faire en sorte que le responsable du traitement remette les traitements de données à caractère personnel en conformité avec la législation et la réglementation en vigueur.

48.2. Cela signifie que la politique de tolérance relative qui est appliquée pour certaines irrégularités ou illicéités constatées se heurte à ses limites. Lorsque l'irrégularité est évidente, le COC **doit** prendre des mesures correctrices, le cas

[65] CJUE 26 septembre 2024, C-768/21, considérant 40.
[66] CJUE 26 septembre 2024, C-768/21, considérant 33. Il n'existe évidemment aucune raison d'évaluer différemment les traitements relevant de la *LED*.
[67] CJUE 26 septembre 2024, C-768/21, considérant 38.

échéant moyennant certaines modalités, comme l'octroi d'un délai pour remédier aux manquements constatés.

Bien que l'autorité de contrôle ne soit selon la Cour de Justice de l'Union européenne pas tenue dans tous les cas d'imposer une mesure correctrice, elle a néanmoins l'*«**obligation** (…) de réagir de manière appropriée afin de remédier à l'insuffisance constatée»* (soulignement du COC)[68]. Or, dans la pratique, le COC ne pourra *«remédier»* efficacement à l'insuffisance constatée qu'en mettant fin à un certain traitement de données à caractère personnel, ou du moins en le suspendant. Comme l'indique également la Cour, il convient en effet, en cas de violation du droit de l'Union, de rétablir la situation pour la rendre conforme au droit de l'Union, grâce à l'intervention de l'autorité de contrôle[69].

À cet égard, la Cour indique clairement qu'il *«**n'est pas exclu** que, à titre **exceptionnel** et compte tenu des **circonstances particulières** du cas concret, l'autorité de contrôle puisse s'abstenir d'adopter une mesure correctrice bien qu'une violation de données à caractère personnel ait été constatée»* (soulignement du COC)[70]. Cela peut notamment être le cas, selon la Cour, lorsque le responsable du traitement a dans l'intervalle *«pris les mesures appropriées et nécessaires pour que ladite violation prenne fin et ne se reproduise pas»*[71]. **Lorsqu'un responsable du traitement n'en a pas l'intention, le COC n'a plus d'autre choix que de mettre fin aux illicéités constatées en imposant une mesure correctrice.**

Il est donc clair que le principe consiste pour l'autorité de contrôle à imposer une mesure correctrice lorsqu'elle constate une illicéité. Le COC n'a en la matière qu'une marge de manœuvre très réduite.

L'expérience nous apprend que les entités de la GPI se conforment dans la grande majorité des cas aux remarques du COC ou à sa vision, de sorte qu'une mesure correctrice effective et formelle n'est généralement pas nécessaire pour rendre la situation à nouveau conforme au droit. Autrement

[68] CJUE 26 septembre 2024, C-768/21, considérant 41.
[69] CJUE 26 septembre 2024, C-768/21, considérant 45.
[70] CJUE 26 septembre 2024, C-768/21, considérant 43.
[71] CJUE 26 septembre 2024, C-768/21, considérant 43.

dit, le COC ne doit la plupart du temps pas prendre de mesure correctrice du fait que le corps se rallie à la vision du COC et/ou anticipe l'annonce par le COC qu'en l'absence de régularisation de la situation, il prendra telle ou telle mesure correctrice formelle. En d'autres termes, le COC s'efforce donc de provoquer l'«intention» de remédier à l'insuffisance constatée qui est évoquée par la Cour de Justice de l'Union européenne, en obligeant au moins l'entité de police à adopter une position explicite témoignant ou non de cette intention.

2.9.1. Les mesures correctrices prises

49. Les mesures correctrices se déclinent sur toute une gamme pouvant aller d'un avertissement, à un rappel à l'ordre officiel indiquant qu'un traitement est illicite, à la suspension d'un certain flux de données, jusqu'à une interdiction temporaire ou définitive d'un traitement.

En 2025 également, le COC a à nouveau formulé des **suggestions**, des **requêtes**, des **recommandations** et des **mesures correctrices**. Les **suggestions** sont soumises sous la forme de pistes de réflexion afin d'améliorer un ou plusieurs aspects de la gestion de l'information policière, mais sont pour le reste laissées à l'appréciation de l'entité responsable du traitement de la GPI ou des ministres responsables du traitement. L'éventuelle implémentation des suggestions ne fait l'objet d'aucune forme de suivi. Les **requêtes** ont pour but d'optimaliser le fonctionnement (par exemple des bonnes pratiques), tandis que les **recommandations** revêtent un caractère un peu plus contraignant (sans pour autant être contraignantes du point de vue juridique et formel) et s'assortissent généralement d'un délai de mise en œuvre fixé par le COC.

Tableau 12: ***Décisions prises dans les enquêtes de contrôle***

Décisions prises dans les enquêtes de contrôle	2020	2021	2022	2023	2024	**2025**
Suggestions	/	/	/	**/**	6	**9**
Requêtes	1	36	7	5	5	**10**
Recommandations	80	33	7	6	13	**14**
Mesures correctrices	26	31	16	2	3	**1**
Total	107	100	30	13	27	**34**

50. Le nombre de décisions prises dans des enquêtes de contrôle a renoué en 2025 avec le niveau de 2022, mais reste sous pression en raison principalement:

- d'une augmentation substantielle du volume des activités réactives;
- de la capacité monopolisée par le suivi des requêtes, recommandations et mesures correctrices formulées dans le passé;
- du cadre limité du COC fixé en 2018 et resté inchangé depuis lors;
- de la conformité informelle de la part des entités contrôlées, qui fait que le COC n'a pas à prendre des mesures correctrices formelles.

Un examen des mesures correctrices prises en 2025 révèle la répartition suivante:

Tableau 13: ***Types de mesures correctrices prises dans les enquêtes de contrôle***

Mesures correctrices prises dans les enquêtes de contrôle[72]	2020	2021	2022	2023	2024	**2025**
Avertissement	3	2	1	0	1	**0**
Réprimande	1	0	1	0	0	**0**
Ordre de mettre le traitement en conformité avec les règles en matière de protection des données	21	26	6	0	1	**1**
Interdiction du traitement	1	1	8	2	1	**0**
Limitation définitive du traitement	-	1	0	0	0	**0**
Limitation temporaire du traitement	-	1	0	0	0	**0**
Total	26	31	16	2	3	**1**

N'ayant pris qu'une seule mesure correctrice formelle, le COC fait donc un usage particulièrement proportionné et mesuré des ordres contraignants à l'égard de la GPI.

[72] Il convient de répéter 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 2025, le COC était (encore) impliqué, chaque fois en qualité de défendeur, dans 8 procédures judiciaires qui ont été entamées en 2020 (1), 2021 (2), 2023 (1) et 2024 (4). Trois (3) de ces procédures ont cependant été clôturées par un jugement définitif. Alors que 4 nouvelles procédures avaient encore été initiées en 2024, soit par des citoyens (2), soit par des organisations de la société civile (1[73]), soit par des zones de police (2[74]), **aucune nouvelle procédure n'a été intentée contre le COC en 2025**.

Depuis 2018, la justice n'a donné tort que dans un seul cas au COC et seule une mesure correctrice encore active a été annulée par la Cour d'appel de Bruxelles, ce qui prouve une fois de plus que le COC exerce sa compétence correctrice/contraignante de manière réfléchie, juridiquement étayée et modérée.

52. Toutefois, ces procédures induisent un fort coefficient de travail pour le COC même si celui-ci recourt dans ce contexte aux services d'un cabinet d'avocats. **Tous les textes (comme les conclusions et les interventions écrites) sont en effet révisés et approuvés avant d'être déposés au greffe.**

[73] À savoir la *Ligue de Droits Humains*.
[74] Il s'agit de la zone de police RUPEL (composée des communes de Boom, Hemiksem, Niel, Rumst et Schelle) et de la zone de police ZENNEVALLEI (composée des communes de Beersel, Hal et Leeuw-Saint-Pierre).

Les principales procédures en cours sont les suivantes:

52.1. L'affaire D.D. (B.A.)/*Ligue des Droits Humains* contre le COC, introduite le 2 septembre 2020. Dans cette affaire, la Cour d'appel de Bruxelles a, dans le cadre du recours contre l'ordonnance du 17.05.2021 du président du Tribunal de première instance francophone, soumis dans son arrêt du 9 mai 2022 deux questions préjudicielles à la Cour de Justice de l'Union européenne concernant la problématique du système belge de l'exercice indirect, par le citoyen, de ses droits en matière de protection des données (voir plus haut les points 25 à 26.1 inclus).

Le 16.11.2023, la Cour de Justice a répondu à ces questions dans son arrêt C-333/22 qui dispose que toute personne concernée doit pouvoir former un recours juridictionnel contre la communication minimale du COC – imposée par l'article 42 de la LPD – qu'il *«a été procédé aux vérifications nécessaires»*, communication qui, de l'avis de la Cour, constitue une 'décision finale' du COC.

La Cour d'appel de Bruxelles a finalement rendu le 24/06/2025 un arrêt définitif dans lequel elle indique d'une part que la *LED* n'a pas été correctement transposée en droit belge dès lors que cette transposition prévoit exclusivement un système d'accès indirect et restreint considérablement les droits du citoyen en matière de protection des données, mais reconnaît d'autre part ne pas être en mesure de donner satisfaction au citoyen étant donné que seul le législateur est à même de modifier la loi (voir plus haut le point 26). Aucun pourvoi en cassation n'ayant été introduit, ce verdict est définitif et l'affaire est donc clôturée. Le COC est cependant au regret de constater, un peu moins d'un an plus tard, que ni les ministres compétents et responsables du traitement, ni la GPI elle-même n'ont entrepris depuis lors les démarches nécessaires pour donner suite à cet arrêt et mettre la législation et la pratique belges en conformité.

52.2. En 2023, la Cour de cassation a, par son arrêt du 6 novembre 2023 (arrêt n° C.23.0092.N) prononcé dans le cadre d'un pourvoi en cassation du COC, annulé l'arrêt du 12.12.2022 de la Cour d'appel d'Anvers dans l'affaire de la zone de police 'Regio Turnhout' contre le COC. Il s'agissait d'un recours introduit par ladite zone de police contre certaines mesures correctrices que le COC avait imposées à l'issue d'un contrôle

technique. Vu les modifications légales intervenues entretemps, le COC avait déjà levé 2 des 3 mesures correctrices en question. La Cour d'appel de Bruxelles a finalement rendu le 24/11/2025 un arrêté définitif qui annulait les 3 mesures correctrices, y compris celles qui avaient déjà été levées, essentiellement parce que le COC aurait enfreint les principes de bonne administration, en l'occurrence l'obligation de motivation.

Un aspect important pour le COC réside néanmoins dans le fait que la Cour a sur le principe suivi sa vision quant à la seule mesure correctrice restante, à savoir l'illicéité du flux proactif de données policières de la zone de police à destination des Pays-Bas; la mesure a toutefois été annulée parce que la Cour a estimé qu'elle n'était pas motivée de manière suffisamment différenciée en fonction du type d'informations faisant l'objet de la communication transfrontalière. En dépit de ce raisonnement pour le moins singulier – puisque la Cour a d'une part adhéré au principe que tout flux à destination des Pays-Bas est illicite mais a tout de même annulé par ailleurs la mesure imposée en raison d'une motivation insuffisante –, le COC a décidé pour des raisons d'économie de procédure (et budgétaires) de ne pas se pourvoir en cassation dans cette procédure qui ne revêtait plus aucune pertinence du point de vue du contenu et qui traînait depuis 2021 … À elle seule, cette procédure a coûté au COC aux alentours de 68.000 EUR en frais de justice et honoraires. Cette affaire est donc elle aussi définitivement clôturée.

52.3. En 2024, dans le cadre d'une plainte introduite par un citoyen et par la *Ligue des Droits Humains*, une procédure a été intentée contre la décision prise par le COC le 2 avril 2024. Dans cette décision, l'Organe de contrôle avait conclu à l'existence d'un fondement juridique suffisant pour la réalisation du 'triptyque', dont spécifiquement le relevé des empreintes digitales et la prise de photos. Attendu que l'objet de la plainte consiste dans les faits en une contestation au sujet du droit en vigueur, le COC a cité l'État belge en intervention forcée. Il n'appartient en effet pas tant au COC, mais bien à l'État belge de se fendre sur ce point. Cette affaire est toujours en cours devant la Cour d'appel de Bruxelles, en attente d'une fixation d'audience pour être traitée.

52.4. Dans une affaire de fraude d'identité, enfin (voir plus haut le point 36.2), la Cour d'appel de Bruxelles a débouté le plaignant de toutes ses demandes à l'égard du COC dans un arrêt du 24 mars 2025[75]. Là aussi, aucun pourvoi en cassation n'a été introduit et l'affaire est définitivement clôturée.

53. Quoi qu'il en soi, les procédures susmentionnées **obligent le COC à procéder de manière beaucoup plus formelle et formaliste et lui laissent moins de liberté pour faire preuve de pragmatisme et de flexibilité**, dès lors que tous ses agissements sont ou peuvent être confrontés aux principes généraux de bonne administration.

[75] Bruxelles (1re chambre francophone), dossier W.H contre l'Organe de contrôle de l'information policière, numéro de rôle 2024/RG/1264, *non publié*. Cet arrêt est définitif.

3. LES ACTIVITÉS RELEVANT PRINCIPALEMENT DU CONTRÔLE

3.1. Les enquêtes de contrôle menées auprès de la GPI

3.1.1. Généralités

54. Cette mission relève de l'activité principale du COC depuis sa création en 1998. L'accent est 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 nécessitent également un suivi en 2025. Les enquêtes de contrôle sont généralement initiées d'office mais peuvent aussi découler d'une demande des instances administratives ou judiciaires.

55. 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 recherche documentaire (*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 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 de base et banques de données particulières;
- contrôle et utilisation des fichiers de journalisation;
- BNG et option 35[76];
- triptyque[77];
- politique de profils;
- utilisation de caméras;
- fonctionnement *ANPR*;
- …

56. 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;

(2) BNG et autres banques de données policières (ponctualité, exactitude, qualité et actualité des saisies, respect des délais de conservation, conformité de la communication d'informations policières à des tiers, …);

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

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

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

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

etc.

[76] On entend par « option 35 » le transfert normal des données de l'*ISLP* vers la Banque Nationale Générale (BNG).
[77] 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.

Les rapports du COC sont généralement disponibles pour consultation dans une version publique[78] sur le site www.organedecontrole.be, dans la rubrique Publications. Certains rapports ne sont pas rendus publics, mais uniquement diffusés en interne au sein de la GPI et de ses autorités.

3.1.2. Aperçu des principales enquêtes de contrôle

57. Certaines enquêtes de contrôle peuvent durer relativement longtemps du fait que le COC consacre du temps à leur suivi (et à la fourniture d'une assistance à l'entité contrôlée). L'objectif est de clôturer le suivi dans l'année (y compris la vérification qu'il a été donné suite aux mesures correctrices ou le contrôle de la suite éventuelle donnée aux requêtes ou recommandations formulées), mais il s'avère que ce n'est pas toujours possible.

58. Voici un aperçu des enquêtes de contrôle effectivement **initiées**[79] en 2025:

- Contrôle restreint concernant le screening des élèves de 7e année en sécurité intégrale (CON25001).
- Contrôle international relatif à l'évaluation Schengen périodique (SCHEVAL) de la Bulgarie (DIO25001).
- Contrôle thématique relatif au recours, par la zone de police Bruxelles-Capitale/Ixelles, à une caméra montée sur un *drone* appartenant à et opérée par une entité privée (DIO25002).

Par rapport aux années précédentes, le COC a donc initié nettement moins de contrôles proactifs.

58.1. Par ailleurs, certaines enquêtes ne sont pas poursuivies au-delà de la phase exploratoire. En d'autres termes, il arrive que le COC décide d'initier sur un certain thème une recherche exploratoire afin de déterminer s'il serait opportun de procéder à un contrôle à part entière sur ce thème. Cela peut par exemple être le cas dans le sillage de communiqués de presse qui pourraient de prime abord indiquer l'existence

[78] 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.
[79] Le nom concret et individualisé de la zone de police a ici été remplacé par le nom de la province dans laquelle elle est située.

de traitements de données illicites. Dans certains cas, le COC décide à l'issue de cette première collecte d'informations de ne pas poursuivre l'enquête. Cette décision peut se fonder sur des raisons diverses: le manque de capacité, le fait qu'il ressort des informations recueillies que les traitements ont bien été effectués conformément à la loi, le constat qu'il s'agit d'une problématique devant en priorité être traitée en interne au sein de la GPI et de ses autorités de tutelle (et non par l'autorité de contrôle), le fait que l'information diffusée au grand public se révèle ne pas correspondre aux faits, etc.

59. Voici à présent un aperçu des enquêtes de contrôle qui ont débouché sur **un rapport final** en 2025:

- Rapport de contrôle du 20 février 2025 concernant l'utilisation d'une caméra mobile montée sur un *drone* dans le cadre de l'appui interzonal pour le contrôle du respect d'une interdiction de dépasser les cyclistes (DIO24010).
- Rapport de contrôle du 4 mars 2025 concernant le screening de partenaires externes au sein du Complexe 'Polis Center' de la police fédérale (DIO24007).
- Rapport du 24 mars 2025 du contrôle technique effectué auprès de diverses entités de la police intégrée concernant la validation centrale des données policières dans la Banque de données nationale générale (CON23002).
- Rapport de contrôle (*prima facie*) du 7 juillet 2025 relatif à un outil/une banque de données OSINT[80] à utiliser par la police judiciaire fédérale (DIO24013).
- Rapport du 21 octobre 2025 du contrôle thématique relatif au recours, par la zone de police Bruxelles-Capitale/Ixelles, à une caméra montée sur un *drone* appartenant à et opérée par une entité privée (DIO25002).
- Rapport de contrôle du 21 octobre 2025 relatif à la panne survenue au sein du centre de données de la police fédérale le 1er décembre 2023 (CON23004).

Enfin, il a également été procédé en 2025 à un contrôle auprès d'une zone de police de la province d'Anvers (DIO240011) au sujet de l'utilisation d'un *drone* par une entité privée dans le cadre d'un projet *«drone in a box»*. Cette enquête ne s'est cependant pas soldée par un rapport de contrôle formel étant donné que la zone de police

[80] Pour des raisons opérationnelles et afin de protéger les tactiques et techniques utilisées, nous ne mentionnons dans le présent rapport d'activité aucun autre élément qui permettrait une identification.

concernée a confirmé après la visite sur place et pendant l'enquête avoir mis un terme à la collaboration avec l'entreprise privée (qui incluait la mise à disposition d'un *drone* et d'un pilote civil). Eu égard notamment à l'attitude constructive de la zone de police et à cette décision de mettre un terme à la collaboration, le COC a décidé le 13.03.2025 de ne pas établir de rapport de contrôle formel (éventuellement avec mesure correctrice).

3.2. Le contrôle de la banque de données commune T.E.R.[81]

60. Il n'a **pas** été initié en 2025 de nouvelle enquête concernant le fonctionnement de la banque de données commune T.E.R.

Comme le COC l'a annoncé en janvier 2024 à la Chambre des Représentants lors du débat au sujet du rapport de contrôle 2022, il ne lui est pas – ou plus – possible de procéder chaque année ni même à intervalles plus espacés à un contrôle proactif de la BDC T.E.R. En 2026, notamment en raison de la composition (toujours) provisoire de son DIRCOM, le COC ne procédera pas non plus à un contrôle proactif de la BDC T.E.R., laquelle s'est vu attribuer un nouveau cadre légal par la loi T.E.R. du 29 mars 2024[82].

Il y a là de quoi relativiser la vision de la Cour constitutionnelle (et du Conseil des ministres) telle qu'elle a été énoncée récemment dans l'arrêt 30/2026 du 12 mars 2026, qui fait régulièrement référence au contrôle du COC en tant que garantie de la licéité, de la légitimité et de la proportionnalité des traitements[83]. En vérité, le COC ne dispose ces dernières années pas de la capacité nécessaire pour exercer un véritable contrôle, et encore moins un contrôle *«permanent»* (voir l'arrêt 30/2026).

---

[81] Cette banque de données commune (terrorisme) visée dans la loi sur la fonction de police (sous-section 7bis de la section 12 du chapitre IV) sera toutefois rebaptisée 'banque de données commune «Terrorisme, Extrémisme, processus de Radicalisation» («T.E.R.»)' à dater du 01.01.2025 en vertu de la loi du 29 mars 2024 portant création de la banque de données commune «Terrorisme, Extrémisme, processus de Radicalisation» («T.E.R.») et modifiant la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, la loi du 30 juillet 2018 portant création de cellules de sécurité intégrale locales en matière de radicalisme, d'extrémisme et de terrorisme et la loi du 5 août 1992 sur la fonction de police, *M.B.* 16.04.20204, 42879.

[82] *Ibidem*.

[83] Considérants B.2.3., B.19.2, B.29, B.47.5, B.56.3, mais surtout le considérant B.55.6: *«Compte tenu des autres garanties contre les abus contenues dans la loi attaquée,* ***et en particulier du contrôle permanent exercé par l'Organe de contrôle de l'information policière*** *et par le Comité permanent R, l'article 4 de la loi attaquée n'entraîne pas une limitation disproportionnée du droit au respect de la vie privée, du droit à la protection des données à caractère personnel et du droit à un recours effectif.»*.

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

61. En vertu de l'article 126/3 §1er, 8e alinéa de la loi du 13 juin 2005 relative aux communications électroniques, le COC est chargé 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 dans le cadre de la rétention des données de communications (données de trafic et données de localisation).

Les décisions de validation du COC sont disponibles pour consultation sur le site Internet de l'Organe de contrôle, dans la rubrique Publications/Rapports.

Cette mission induit un fort coefficient de travail, mais l'expérience acquise lors des exercices précédents permet au COC de s'en acquitter désormais nettement plus aisément.

Cette opération doit être réitérée chaque année.

En 2025, le COC n'a pris **aucune** décision dans le cadre de la rétention des données[84].

[84] Les statistiques des années 2022-2023-2024 et le dossier introduit à ce sujet n'ont été transmis au COC qu'à la fin 2025 et ont conduit à une décision de validation qui a été prise le 16 janvier 2026 (cf. www.organedecontrole.be).

4. LES ACTIVITÉS POLITIQUES

4.1. Forums de concertation nationaux

62. En 2025 également, le COC a pris part à un certain nombre de forums de concertation et/ou réunions, tant formels qu'informels, avec par exemple des ministres en charge de la police et leurs cabinets, les services de police, les administrations concernées, les autres autorités administratives ou judiciaires, etc. concernant des initiatives ou thèmes législatifs ou opérationnels projetés; il peut aussi s'agir 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 est cependant réticent à siéger au sein des groupes de travail (soi-disant 'informels') et réunions de toutes sortes auxquels il est invité (tant par le pouvoir exécutif que par le pouvoir judiciaire). La frontière entre la fonction consultative et informative d'une part et le maintien de la propre indépendance d'autre part est très mince. Le COC est régulièrement amené soit à décliner l'invitation, soit à clarifier les contours de ses interventions.

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 du *Supervision Coordination Group*, qui est subdivisé en sous-groupes de plus en plus nombreux. Le COC s'y consacre aux sous-groupes de travail 'EUROPOL' et 'SIS' (le système d'information Schengen), mais les nouveaux sous-groupes de création plus récente comme 'EES[85]' et (dans une moindre mesure) 'EURODAC[86] et 'ETHIAS'[87], qui découlent tous (de la multiplication) des systèmes informatiques à grande échelle européens (*«large scale information systems»*), requièrent également de plus en plus

[85] *Entry Exit System* (https://commission.europa.eu/news-and-media/news/more-secure-efficient-and-convenient-way-travelling-non-eu-nationals-2026-04-10_fr).
[86] *EURODAC* est la base de données biométriques centralisée de l'Union européenne, conçue pour aider à la gestion des demandes d'asile et soutenir les efforts visant à détecter, investiguer et prévenir le terrorisme et les formes graves de criminalité, www.eulisa.europa.eu/activities/large-scale-it-systems/eurodac?etrans=fr.
[87] European Travel Information and Autorisation System, https://travel-europe.europa.eu/fr/etias.

d'efforts. Le COC se voit en effet confier dans chacun de ces systèmes un nombre croissant de compétences et de missions, à nouveau sans que sa capacité ne soit adaptée d'une quelconque manière.

Par ailleurs, le COC représente la Belgique au sein 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[88]). Le COC s'efforce d'investir du temps dans ces assemblées car elles traitent en effet de thèmes cruciaux (par exemple le recours à l'intelligence artificielle dans les États membres de l'UE, l'interaction entre le RGPD/la *LED* et la loi sur l'IA de l'Union européenne, etc.), mais n'est pas en mesure d'assurer un suivi de tous les thèmes pertinents.

En 2025, le COC a à nouveau pris part à des dizaines de réunions, précédées de la préparation requise et accompagnées ultérieurement du suivi requis (approbation de comptes rendus, contributions aux positions communes, échange d'arguments, etc.).

4.3. Communication externe et participation à divers événements

4.3.1. Contacts avec la presse

65. En 2025, le Président *a.i* a continué à exercer la fonction de porte-parole de la presse tant du côté francophone que du côté néerlandophone, en marge de ses tâches opérationnelles, de gestion et de direction. La désignation d'un porte-parole de la presse est la mise en œuvre du devoir d'information prévu à l'article 240, 1° de la LPD[89], qui vise à ce que le COC se tienne au maximum à la disposition de la presse.

Tant la presse francophone que la presse néerlandophone ont fait paraître en 2025 également des articles et des contributions faisant mention du COC ou pour lesquels le porte-parole de la presse avait été contacté.

[88] L'European Data Protection Supervisor, l'EU-DPA, https://edps.europa.eu.
[89] 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 …»*.

4.3.2. Participation à des journées d'étude et formations externes

66. Le COC fait régulièrement l'objet de sollicitations en vue de prendre part en tant qu'orateur/formateur à toutes sortes de formations, journées d'étude ou colloques organisés par la police ou 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 – et de leur propre initiative – de manière conforme, et soient en mesure de le faire. La mission de sensibilisation[90] du COC exige qu'il se rende le plus possible sur le terrain et honore ces invitations, d'autant qu'il s'agit également d'une opportunité de démystifier certains aspects et/ou d'éliminer des idées et préjugés tenaces.

Les exemples qui suivent illustrent ce propos.

66.1. Y ayant été invités, les membres (du personnel) du COC ont dispensé en 2025 les formations internes suivantes à la GPI[91]:

(1) ANPA (Académie Nationale de Police), formation des aspirants commissaires de police (N/F).
(2) Formation des aspirants inspecteurs de l'école de police ARPB (de la 72e à la 75e PROM, Bruxelles) (N/F).
(3) Formation à l'intention des futurs commissaires principaux de police en vue de l'obtention du brevet de direction (N/F).
(4) Formation spécifique 'Gold Commander' de l'ANPA (N/F).
(5) Formation dispensée auprès du Service Gestion fonctionnelle de la zone de police Bruxelles-Nord (N/F).
(6) Formation dispensée à un nouveau membre du personnel du CG/ISPO (F).
(7) Réunion avec les membres du SICAD et le gestionnaire fonctionnel de l'arrondissement Hal-Vilvorde (N).

---

[90] 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).
[91] Ces invitations émanent tant de la police fédérale (PJF/DCA) que de la police locale de l'arrondissement, la plupart du temps des chefs de corps et/ou des délégués à la protection des données (DPO) et/ou des gestionnaires fonctionnels, des services de contrôle interne et d'autres dirigeants.

(8) Séminaire de la concertation provinciale des chefs de corps de la province d'Anvers consacré à la protection de la vie privée et des données ainsi qu'au fonctionnement du COC (N).

(9) Réunion avec les DPO de la province de Flandre occidentale consacrée à la protection de la vie privée et des données (N).

(10) Réunion avec les DPO de la Région de Bruxelles-Capitale consacrée à la protection de la vie privée et des données (N/F).

(11) Participation à la journée d'inspiration de la zone de police Aalst consacrée à l'intelligence artificielle et intitulée 'AI gebruik door de GPI. Aandachtspunten en bezorgdheden van de toezichthouder.' (Utilisation de l'IA par la GPI. Points d'attention et préoccupations de l'autorité de contrôle.) (N).

(12) Participation au projet FEEDIS USER REVIEW de la police fédérale (N).

66.2. Les membres (du personnel) du COC ont à nouveau dispensé en 2025 des formations organisées par d'autres institutions (d'enseignement), notamment:

(1) au *Data Protection Institute* (DPI), Certification DPO Police[92];

(2) des séminaires organisés par la maison d'édition Politeia.

66.3. Par ailleurs, le COC publie également sur le SharePoint interne de la police les avis et/ou rapports pertinents pour toute la GPI qui ne se prêtent pas à une diffusion externe au grand public. À la fin 2025, 20 publications étaient disponibles (dans les deux langues nationales). En 2025, le COC a émis des rapports, rendu des avis ou pris position sur les thèmes suivants:

- Rapport du 24.03.2025 du contrôle technique effectué auprès de diverses entités de la police intégrée concernant la validation centrale des données policières dans la Banque de données nationale générale (CON23002).

[92] Voir www.dp-institute-eu; il s'agit malheureusement toujours (plus de 7 ans après l'entrée en vigueur du nouveau cadre de la protection des données), du fait de l'absence persistante d'une formation interne au sein de la GPI, de la seule formation de haut niveau menant à une certaine forme d'attestation ou de certification de la fonction de DPO. Les membres et les membres du personnel du COC fournissent dans le cadre de cette formation une contribution essentielle induisant un fort coefficient de travail. L'objectif est toujours de réduire ces efforts, voire d'y renoncer complètement, une fois que le ministre de l'Intérieur aura reconnu une formation interne à la fonction de DPO satisfaisant aux normes de qualité requises. Une évaluation de la formation des DPO de police dispensée les 23 et 24 avril 2025 dans les locaux de la ZP Bruxelles-Capitale a révélé un NPS (*Net Promotor Score*) particulièrement élevé de 9,1 (sur 10, l'objectif fixé par le DPI étant de 5,5), qui constitue donc un excellent résultat.

- Avis d'initiative du 02.09.2025 relatif à un projet d'AIPD de référence pour l'accès en temps réel, par la GPI, aux images des caméras de la SNCB (DI250007).

- Avis d'initiative du 16.09.2025 relatif au déploiement d'un système permettant aux citoyens de déclarer certains faits en recourant à un appel vidéo (DD250036).

- Avis d'initiative du 06.10.2025 relatif au fondement juridique de la consultation internationale de numéros d'immatriculation et à l'application dite 'GAS-5' – établissement d'un procès-verbal/de compléments par la commune/le fonctionnaire sanctionnateur (BD250017).

66.4. Le COC a pris part en tant qu'orateur aux événements suivants:

- Réunion-débat de l'APIEA-BVVE (l'association professionnelle des inspecteurs et experts d'assurances) et de l'ECSA (European Corporate Security Association) sur le thème 'De toekomst van de private opsporing, de very first steps naar publiek-private samenwerking' (L'avenir de la recherche privée, les tout premiers pas vers un partenariat public-privé.), 30.01.2025.

- Journée nationale de formation de l'INCC[93] consacrée à la recherche d'ADN en matière pénale et à la protection des données (N).

- Participation au projet européen *PACE* (Public Administration Cooperation Exchange), avec visite d'une délégation de la Roumanie et de la Lettonie, 'Belgian DPA's in the context of the SIS' (EN).

- Participation à la journée d'étude '*Drones* 2025' du CPS (Centre for Policing and Security) (N).

Les membres et les membres du personnel du COC participent par ailleurs dans la mesure du possible eux-mêmes à des formations pertinentes. La matière que traite le COC et sa mission de contrôle sont (juridiquement et techniquement)[94] complexes, sont constituées de composantes nationales et internationales, comportent de

[93] Institut National de Criminalistique et de Criminologie.
[94] D'un point de vue juridique, les dossiers et thèmes traités par le COC se caractérisent par un mélange de droit national et international de la protection de la vie privée et de la protection des données, de droit de police, de droit pénal et de procédure pénale, de droit administratif et constitutionnel et de droit (procédural) civil.

nombreuses 'zones grises' et évoluent rapidement, de sorte que la formation continue est indispensable.

La participation aux formations internes de la GPI sera toutefois encore davantage limitée à partir de 2026, à nouveau pour des raisons de capacité.

4.3.3. Site Internet

67. Le site Internet a encore été consulté régulièrement en 2025, et même nettement plus que les années précédentes. Le **cap des 20.000 visiteurs par an** a été franchi.

Voici les nombres de visiteurs recensés tout au long de l'année **2025**, correspondant à une **moyenne de 1686 visiteurs par mois**, ce qui représente une nouvelle augmentation – même impressionnante cette fois – par rapport aux années précédentes (en moyenne 300 visiteurs de plus par mois qu'en 2024). Voilà qui explique aussi d'emblée pourquoi le nombre de demandes d'accès indirect a connu en 2025 une telle augmentation. Il est donc clair que le COC jouit d'une notoriété croissante auprès des citoyens et des professionnels.

Nombre de visiteurs du site Internet du COC	2021	2022	2023	2024[95]	2025
Janvier	603	534	649	/ (595)	1428
Février	541	460	568	/ (261)	1421
Mars	1087	663	792	/ (847)	1463
Avril	751	652	597	/ (667)	1602
Mai	832	691	711	1017	1547
Juin	746	536	606	1517	1472
Juillet	401	416	471	1243	1216
Août	341	407	460	1143	1593
Septembre	481	480	614	1460	1673
Octobre	526	616	766	1584	2471
Novembre	534	688	378	1696	2865
Décembre	550	799	674[96]	1348	1478
Total	**7.393**	**6942**	**7.286**	**13378**	**20229**

Le site est accessible à l'adresse www.controleorgaan.be ou www.organedecontrole.be et le rôle de webmaster est endossé par l'assistante de direction.

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 et d'écoles supérieures et par d'autres parties externes. En 2025 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. Pour des raisons de capacité, le COC n'est par contre pas en mesure de répondre aux demandes de stages émanant d'universités/écoles supérieures et d'étudiants individuels.

[95] Pour des raisons techniques, les chiffres des mois de janvier à avril 2024 inclus ne sont pas disponibles. Nous avons donc pris pour ces mois une moyenne des années précédentes. Toutefois, il pourrait s'agir d'une sous-estimation vu la nette augmentation du nombre de visiteurs observée pour les autres mois de 2024 par rapport aux années précédentes.
[96] Pour des raisons techniques, le chiffre exact de décembre 2023 n'est pas disponible. Nous avons donc pris une moyenne des deux années précédentes, à savoir 674.

5. PARTENARIATS ET COMPÉTENCES PARTAGÉES

69. Le législateur fédéral a prévu dans la LCA et la LPD plusieurs autorités fédérales de protection des données: 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.

69.1. 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[97] a dans l'intervalle largement fait ses preuves.

Force est de constater, après 7 années de fonctionnement, que les points de vue des différentes autorités de contrôle ne sont pas contradictoires et que chacune des autorités de contrôle susmentionnées veille à s'en tenir à son propre domaine de compétence et à réorienter au besoin les demandes.

Le choix posé par la Belgique en 2018 d'opter pour la création d'autorités de protection des données spécialisées en marge de l'autorité de protection des données générale de droit commun prouve donc son efficacité.

69.2. Pour terminer, il convient d'ajouter que le COC donne également toujours suite aux demandes d'auditions émanant du parlement, même s'il n'a pas été sollicité dans ce contexte en 2025.

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

6. CONCLUSION ET PERSPECTIVES D'AVENIR

70. Pour ce qui concerne **le présent**, les constats suivants restent pertinents.

70.1. Bien qu'ayant une envergure restreinte parmi les autorités de contrôle, le COC est parvenu à **se faire résolument une place dans le paysage de la protection des données et du contrôle (de la police)**.

70.2. Le COC 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. Le COC a reçu en 2025 également de nombreuses réactions positives tant des services de police[98] que des citoyens[99] qui font appel au COC.

---

[98] Quelques exemples:

- Le CP de la ZP Noord (Kapellen/Stabroek): *«Merci de tout cœur pour votre réponse détaillée.»*.
- Le DPO de la ZP Montgomery: *«Je tiens à vous remercier à nouveau vivement pour cet entretien qui a richement alimenté ma réflexion. Comme convenu, je vous confirme le caractère purement exploratoire et informel de cet entretien ainsi que …»*.
- Le DPO de la ZP Vesdre: *«Par ce courriel, je souhaite simplement vous remercier pour votre professionnalisme durant ces 2 ans dans le cadre de mon CDD en tant que DPO. Je me suis sentie plus soutenue par vos avis et je trouve que c'est important que cette relation existe entre le DPO et l'Organe de contrôle.»*.
- Le DPO de la police fédérale/DGA/DAB: *«J'accuse bonne réception de votre avis et vous en remercie. Conscient de la complexité du casus qui vous a été soumis mais ne doutant pas non plus de la richesse intellectuelle générée par la réflexion, je vous prie de bien vouloir adresser mes remerciements à vos collaborateurs qui ont pris soin d'investiguer le sujet.»*.
- Le CP/DPO de la ZP Mariemont: *«Tout d'abord, à l'instar des remerciements adressés à votre collègue, merci pour les outils que vous nous fournissez afin de traiter au mieux la demande en conformité avec le cadre légal.»*, et plus loin: *«Je tenais d'abord à vous remercier vous, et les membres du COC, car vos demandes par e-mail contiennent de plus en plus de la doctrine qui nous permet de nous aider dans nos tâches de DPO. Pour vous avoir déjà rencontré en personne lors de différents colloques, vous savez que malheureusement nous ne sommes pas suffisamment informés/formés ou que nous manquons tout simplement de capacité. Cela est d'autant plus vrai pour des zones de police de petite et moyenne catégorie. C'est donc une véritable richesse de vous lire. Merci!»*.
- Le DPO de la ZP Waterloo: *«Je vous remercie pour votre message. Cette expérience ayant été particulièrement riche en enseignements, je me suis permis d'adapter notre formulaire d'analyse afin qu'il soit davantage en adéquation avec les attentes du COC.»*.
- Le DPO de la ZP VLAS: *«C'est avec des sentiments quelque peu mitigés et une pointe d'excitation que je vous adresse ces quelques mots. Cette journée a été pour moi la dernière passée au bureau puisque je me retirerai officiellement de la vie professionnelle le xxx. Les nombreux contacts et entretiens que j'ai eus avec vous ont été inspirants, particulièrement instructifs, toujours éclairants et surtout très enrichissants. À chaque fois, vous vous êtes montré un modèle d'expertise dans les domaines de la gestion de l'information policière et de la protection des données et de la vie privée. Bien que je sois impatient de découvrir ce que me réserve cette nouvelle étape de ma vie, je conserve d'excellents souvenirs de mon passage au sein de l'organisation policière. Je tenais donc avant de partir à vous adresser, ainsi qu'à tous vos collègues du COC, tous mes remerciements et mes vœux de réussite les plus sincères. Je tiens à ce que vous sachiez qu'à vous tous, vous faites vraiment la différence …»*.
- Un CP à la suite d'une plainte qu'il avait introduite: *«Je prends bonne note de la clôture du dossier et je tiens à vous remercier de l'entretien éclairant que nous avons eu ensemble. Indéniablement, notre organisation a encore du pain sur la planche. Comme je vous l'ai indiqué, j'entreprendrai les démarches requises auprès de l'AIG.»*.

[99] Quelques exemples:

- Un citoyen: *«Je viens de prendre connaissance de votre travail au sein du COC, d'abord par L'Echo et puis en lisant votre rapport d'activité. On y voit une rigueur et une capacité de contrecarrer les dérives du système qui vous font grand honneur. Dans le marasme institutionnel belge, vous me semblez encore un Européen 'à l'ancienne', de ceux qui ont construit l'Europe, au lieu de la détruire. Étant également fonctionnaire européen, et en voyant bien comme cela peut (dis)fonctionner dans les grandes institutions, je suis impressionné par votre courage, encore plus vu que vous êtes 'ad interim' … Également en tant qu'habitant de la Belgique, je vous remercie pour votre action, et je reste à votre disposition si vous avez besoin d'aide, à tout niveau possible.»*.

70.3. Les demandes d'avis et les expériences vécues par les formateurs du COC lors de formations internes de la GPI prouvent par ailleurs que le personnel de la GPI manque encore toujours cruellement de connaissances et d'expertise dans cette matière. Toutefois, il n'appartient pas au COC[100] de s'acquitter du rôle et des missions de formation des responsables du traitement. **L'enseignement dispensé par la police, en tout cas (également) dans cette matière, n'offre pas la qualité que l'on serait en droit d'espérer.**

70.4. En 2025 également, le COC a exercé ses compétences correctrices de manière très marginale et proportionnelle et lorsque la loi ne lui laisse pas d'autre choix. L'assistance et les conseils, dans les limites de ses possibilités, sont en tout temps la première option envisagée, même si cette approche s'avère de moins en moins évidente. En marge de la protection de données, le COC porte aussi énormément d'attention à d'autres besoins et aspects opérationnels.

71. Pour ce qui est de l'**avenir**, il convient de formuler et/ou de rappeler les constats et/ou recommandations qui suivent.

71.1. L'Organe de contrôle attend **depuis 2021** l'indispensable **réparation/amendement de la loi relative à la protection des données**, d'ailleurs déjà annoncé(e) par les autorités compétentes.

- Un citoyen: *«Je vous remercie pour votre professionnalisme.»*.
- Un citoyen à la suite d'une plainte qu'il avait introduite: *«J'accuse par la présente bonne réception du procès-verbal de décision de l'Organe de contrôle de l'information policière du xxx dans le cadre du dossier DKL25xxx. Je prends bonne note du fait que ma plainte a été jugée irrecevable dès lors que ma demande portait sur l'accès à des documents administratifs conformément à la loi du 11 avril 1994 relative à la publicité de l'administration et que cette matière ne relève pas de la compétence matérielle de l'Organe de contrôle. Je tenais à vous remercier pour la motivation claire et juridiquement étayée qui accompagnait cette décision. Sachant que ma demande avait trait à des notifications concrètes de nuisances auprès de la ZP xxx, il était très important pour moi de savoir que ces notifications avaient effectivement été enregistrées et traitées. Cela confirme objectivement qu'un traitement de données à caractère personnel a été effectué, même si ma demande initiale ne relevait pas de la compétence formelle de traitement des plaintes de l'Organe de contrôle. Votre décision me permet à présent d'axer prioritairement mon suivi de ce dossier sur l'administration de la ville de xxx. … J'utiliserai votre décision comme un élément additionnel dans le contexte plus vaste, qui tend à établir que la problématique de nuisances en question était déjà connue d'autres instances administratives, ou aurait en tout cas pu l'être. Je tiens à vous remercier explicitement pour le soin et la rigueur juridique dont vous avez fait preuve dans le traitement de ce dossier. Votre décision me fournit une référence précieuse pour poursuivre le suivi de cette question, et j'apprécie tout particulièrement la transparence avec laquelle l'Organe de contrôle a délimité et appliqué ses compétences.»*.
- Un citoyen à la suite d'un dossier d'accès indirect: *«Je vous remercie de tout cœur de votre message et du soin que vous avez apporté au traitement de ma demande du 16 juin dernier en vue de l'exercice indirect de mes droits auprès de l'Organe de contrôle de l'information policière. J'apprécie les efforts que vous et votre équipe avez déployés pour effectuer les vérifications nécessaires et m'en informer. Votre communication transparente me rassure quant au traitement correct de mes données à caractère personnel.»*.

[100] D'autant que ce n'est tout bonnement pas faisable.

71.2. L'Organe de contrôle se heurte toutefois de plus en plus aux **limites 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 (la gouvernance belge de la loi sur l'IA de l'Union européenne), nouvelle réglementation PNR, *big data policing*, *predictive policing*, techniques de surveillance avancées, systèmes informatiques à grande échelle européens, etc.). Un appel qui est malheureusement resté jusqu'ici sans réponse …

Si d'une part des moyens additionnels sont dégagés et des possibilités sont créées pour les services de police, on ne pense que rarement – pour ne pas dire jamais – aux moyens et aux possibilités des autorités de contrôle. Les projets de législations et de réglementations ainsi que la jurisprudence (par exemple de la Cour constitutionnelle, voir plus haut le point 60) insistent souvent sur la présence et l'importance du contrôle, que ce soit pour 'faire passer' politiquement l'une ou l'autre réglementation ou nouvelle compétence ou pour en évaluer la constitutionnalité, mais les décideurs politiques ne joignent jamais le geste à la parole en dotant ces autorités de contrôle des moyens et méthodes (additionnels) qui leur permettraient de mieux s'acquitter de leur mission. La conclusion qui s'impose est que l'équilibre entre d'une part l'application efficace des règles et d'autre part le contrôle démocratique se perd de plus en plus, et qu'une autorité de contrôle ne peut finalement réaliser que ce que ses moyens lui permettent de réaliser …

71.3. La tendance à se pourvoir de plus en plus en justice contre le COC ne s'est pas poursuivie en 2025, mais ce constat était principalement à attribuer à deux éléments: d'une part le fait que le COC n'a pour ainsi dire pas imposé de mesures correctrices parce qu'il a réalisé nettement moins de contrôles proactifs, et d'autre part le fait que les services de police se conforment préventivement aux points de vue adoptés par le COC.

71.4. En 2025 également, le COC ne peut que **rappeler les points d'amélioration** 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[101], 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;

* aligner enfin le système d'accès mis à la disposition du citoyen pour exercer ses droits de contrôle (consultation, rectification, suppression ou limitation des données à caractère personnel) sur le droit et la jurisprudence de l'UE;

* attribuer à l'Organe de contrôle la compétence formelle, dont est également investi le président du Comité permanent P[102], d'informer une instance disciplinaire de (potentiels) manquements disciplinaires et d'également l'obliger à informer l'Organe de contrôle de la suite donnée à son information;

* prévoir pour le COC l'astreinte administrative étant donné que l'amende administrative a été définitivement exclue à l'égard des institutions publiques (et que cette décision a été jugée conforme par la Cour constitutionnelle[103]), bien qu'elle existe dans la plupart des pays de l'UE à l'égard de la police[104].

72. La commission d'enquête parlementaire 'Attentats'[105] 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. Cette recommandation n'avait rien perdu de sa pertinence en 2025 et en acquerra de plus en plus dans les années à

[101] Article 71 §1er, troisième alinéa de la LPD.
[102] Article 26, 4° de la loi du 13 mai 1999 portant le statut disciplinaire des membres du personnel des services de police.
[103] Cour constitutionnelle, 14 janvier 2021, n° 3/2021, www.const-court.be/fr.
[104] 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).
[105] 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.

venir vu l'explosion des informations et des renseignements, des *big data* et de la surveillance de masse, sans oublier la digitalisation et l'intelligence artificielle.

73. Le contrôle de l'application des règles et des instances qui en sont chargées n'est pas un luxe superflu, loin de là. Ce contrôle est indéniablement de plus en plus menacé, mais il demeure une composante essentielle dans un État de droit démocratique basé sur le principe de la séparation et de l'équilibre des pouvoirs (et des intérêts).

* * * * * * * * *

Rapport d'activité 2025, approuvé par l'Organe de contrôle le 19 mai 2026.

Ronny SAELENS
Membre-conseiller *a.i.*
(Sé)

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

ANNEXE: LE COC EN CHIFFRES[106]

TYPE DE DOSSIER	2019	2020	2021	2022	2023	2024	**2025**
Dossiers AI[107]	392	283	546	555	549	565	796
Avis protection des données	82	85	82	87	59	81	61
Avis réglementation	22	15	33	39	49	36	26
Plaintes	30	40	28	29	34	34	60
Avis sur l'utilisation de caméras	32	29	29	32	21	34	26
Notifications *ANPR*[108]	2	8	3	16	33	50	58
AIPD	27	10	33	29	19	7	9
Brèches de sécurité	17	17	21	25	40	38	42
Contrôle global & Contrôle technique[109]	2	5	1	1	1	1	0
Contrôle thématique & Contrôle restreint[110]	3	5	8	7	6	4	2
Contrôle spécial BELPIU[111]	1	1	1	1	0	0	0
Contrôle spécial BD Terrorisme[112]	1	1	1	0	0	0	0
Contrôle international[113]	1	0	1	0	3	1	1
Validation rétention des données	0	0	0	1	1	2	0
Déclaration COC - GPI/MP[114]	4	3	2	14	10	14	9
TOTAL	**616**	**502**	**789**	**836**	**825**	**867**	**1090**

[106] 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. Ces chiffres n'incluent pas tous les dossiers, par ex. les réponses informelles et les réunions *Teams* (cf. le point 29), ni les procédures judiciaires en cours qui monopolisent beaucoup de la capacité du COC. Le tableau a été légèrement modifié par rapport aux rapports d'activité précédents puisque l'on y a ajouté 2 types de dossiers qui n'étaient pas comptabilisés auparavant, à savoir les notifications de l'utilisation du système *ANPR* et les dossiers ayant trait à des déclarations faites par le COC aux chefs de corps ou au ministère public.
[107] Dossiers d'accès indirect.
[108] Il s'agit des notifications adressées au COC par les entités de la GPI au sujet de l'utilisation non visible de caméras et de l'utilisation visible de caméras *ANPR* à des fins de police administrative, conformément à l'article 44/11/3*decies* §4, 5e alinéa de la LFP.
[109] Rapports d'enquêtes de contrôle publiés.
[110] *Ibidem.*
[111] *Ibidem.*
[112] *Ibidem.*
[113] *Ibidem.*
[114] Il s'agit de la déclaration d'indications d'infractions pénales et/ou d'infractions disciplinaires aux chefs de corps ou au ministère public dans le sillage du traitement de plaintes ou de dossiers d'accès indirect.

Décisions prises dans les enquêtes de contrôle	**2020**	**2021**	**2022**	**2023**	**2024**	**2025**
Suggestions	/	/	/	**/**	**6**	**9**
Requêtes	1	36	7	5	**5**	**10**
Recommandations	80	33	7	6	**13**	**14**
Mesures correctrices	26	31	16	2	**3**	**1**
Total	**107**	**100**	**30**	**13**	**27**	**34**

Mesures correctrices prises dans les enquêtes de contrôle	2020	2021	2022	2023	2024	**2025**
Avertissement	3	2	1	0	1	0
Réprimande	1	0	1	0	0	0
Ordre de mettre le traitement en conformité avec les règles en matière de protection des données	21	26	6	0	1	1
Interdiction du traitement	1	1	8	2	1	0
Limitation définitive du traitement	0	1	0	0	0	0
Limitation temporaire du traitement	0	1	0	0	0	0
TOTAL	**26**	**31**	**16**	**2**	**3**	**1**

