

## VERSION PUBLIQUE

**RAPPORT CONCERNANT LA VISITE EFFECTUÉE  
AUPRÈS D'UNE ZONE DE POLICE DE LA PROVINCE  
DE FLANDRE OCCIDENTALE PAR L'ORGANE DE  
CONTRÔLE DE L'INFORMATION POLICIÈRE DANS  
LE CADRE DE SES COMPÉTENCES DE CONTRÔLE ET  
DE SURVEILLANCE**

*Référence : [CON21006](#)*

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



## VERSION PUBLIQUE<sup>1</sup>

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

La loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel (LPD)<sup>2</sup> a réformé l'Organe de contrôle en une autorité de contrôle à part entière en plus des compétences de contrôle en matière de gestion de l'information policière prévues par la loi du 5 août 1992 sur la fonction de police (LFP). L'article 71 §1<sup>er</sup> et les Titres 2 et 7 de la LPD décrivent les missions et les compétences du COC. Il est dans ce contexte fait référence par ailleurs aux missions de contrôle visées aux articles 44/1 à 44/11/14 inclus de la LFP, relatifs à la gestion de l'information par les services de police. L'Organe de contrôle est ainsi investi d'une mission de surveillance et de contrôle, ce qui signifie qu'en marge de la protection de la vie privée et des données, le COC prête également attention à des éléments comme l'efficacité de l'intervention policière. En vertu de la réglementation susmentionnée, le COC dispose dès lors d'une compétence de surveillance générale à l'égard de tous les traitements de données (à caractère personnel) opérationnels et non opérationnels effectués par la GPI<sup>3</sup>.

L'Organe de contrôle est compétent pour les services de police<sup>4</sup>, pour l'inspection générale de la police fédérale et de la police locale (AIG)<sup>5</sup> et pour l'unité d'information des passagers (BELPIU)<sup>6</sup>. La compétence de surveillance de l'Organe de contrôle à l'égard de la police intégrée couvre à la fois les activités de traitement opérationnelles et non opérationnelles<sup>7</sup>.

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

Dans ce cadre, le COC procède aux constatations et peut formuler des questions, des requêtes et/ou des mesures correctrices (au caractère contraignant) en tant que « *ultimum remedium* » si le COC constate des infractions aux lois et règlements.

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

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

L'Organe de contrôle exerce également une surveillance sur toutes les formes d'utilisation, par la police, de caméras visibles conformément aux articles 25/1 à 25/8 inclus de la LFP. Dans le cadre de l'utilisation de caméras non visibles, l'Organe de contrôle fonctionne en quelque sorte comme une commission « MAP »<sup>8</sup>. Conformément à l'article 46/6 de

---

<sup>1</sup> La version publique d'un rapport de l'Organe de contrôle ne comporte pas ou pas nécessairement tous les éléments figurant dans le rapport de base adressé aux destinataires (autorités policières, administratives ou judiciaires). Certains éléments ou passages ont été omis ou anonymisés. Il peut y avoir diverses raisons à cela, qui peuvent être de nature légale ou être dictées par des motifs d'opportunité : la volonté de ne pas divulguer des techniques ou tactiques policières, le secret de l'enquête, le secret professionnel, le fait qu'un manquement a été résolu dans l'intervalle, etc.

<sup>2</sup> M.B. 5 septembre 2018. Cette loi contient des dispositions qui donnent exécution au Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), ci-après dénommé « RGPD », et à la Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil (ci-après dénommée « directive Police-Justice » ou LED (Law Enforcement Directive)).

<sup>3</sup> Le COC établit une distinction entre différentes formes de contrôles ou de surveillance. Le COC procède soit à :

- **un contrôle global** : il s'agit d'un contrôle qui s'assortit d'une ou plusieurs visites approfondies sur place et d'une portée très large ;
- **un contrôle thématique** : comme le nom l'indique, il s'agit d'une enquête menée sur un thème déterminé et qui peut inclure à la fois de la *desk research* et des visites sur place ;
- **un contrôle technique** : il s'agit d'un contrôle qui se concentre sur la licéité, l'exhaustivité et l'exactitude des enregistrements/traitements effectués dans les banques de données policières ;
- **un contrôle restreint** : ce contrôle porte sur un seul ou sur quelques aspects (partiels) d'un traitement de données policier ou non policier ;
- **un contrôle international** : il s'agit des éventuelles enquêtes internationales auxquelles le COC apporte son concours ;
- **un contrôle spécial** : il s'agit d'un contrôle portant sur des matières particulières, comme les contrôles annuels des banques de données communes terrorisme et extrémisme.

<sup>4</sup> Tels que définis à l'article 2, 2<sup>o</sup> de la loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux (art. 26, 7<sup>o</sup>, a de la LPD).

<sup>5</sup> Telle que définie à l'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 (art. 27, 7<sup>o</sup>, d de la LPD).

<sup>6</sup> Telle que visée au chapitre 7 de la loi du 25 décembre 2016 relative au traitement des données des passagers (art. 26, 7<sup>o</sup>, f de la LPD).

<sup>7</sup> Art. 4 §2, 4<sup>ème</sup> alinéa de la loi du 3 décembre 2017 portant création de l'Autorité de protection des données.

<sup>8</sup> MAP signifie « **M**éthodes **A**dministratives **P**articulières ».

la LFP, toute autorisation et prolongation d'utilisation non visible de caméras dans les cas visés à l'article 46/4 doit être notifiée à l'Organe de contrôle sauf lorsque l'utilisation des caméras est réalisée sous le contrôle d'un magistrat. L'Organe de contrôle doit alors examiner si les conditions pour la décision, la prolongation ou l'exécution de cette mesure sont remplies. L'Organe de contrôle prend en outre connaissance des plaintes et statue sur leur bien-fondé<sup>9</sup>.

Les membres et les membres du personnel de l'Organe de contrôle, dont notamment son 'Service d'Enquête (DOSE)<sup>10</sup>, disposent à cet égard de compétences d'investigation, après quoi l'Organe de contrôle – et plus spécifiquement son comité de direction (DIRCOM) – peut au besoin prendre des mesures correctrices<sup>11</sup>.

Un recours juridictionnel peut être introduit dans les trente jours contre certaines décisions de l'Organe de contrôle devant la Cour d'appel du domicile ou du siège du demandeur qui traite l'affaire selon les formes du référé conformément aux articles 1038, 1040 et 1041 du Code judiciaire<sup>12</sup>.

## 1. INTRODUCTION

Vu les compétences dont il est investi en sa qualité de service de contrôle externe et d'autorité de contrôle compétente à l'égard des traitements de données effectués par la police intégrée organisée à deux niveaux (GPI), l'Organe de contrôle de l'information policière ('l'Organe de contrôle' ou 'le COC') a décidé de donner suite à la demande qui lui a été adressée le 4 mai 2021 par le procureur du Roi de Flandre occidentale en vue de mener une enquête de contrôle au sein d'une zone de police de Flandre occidentale (ci-après 'la PZ WV').

Cette demande découlait d'une impression générale de dysfonctionnement de la zone de police ressentie par le Collège de police (instance administrative), qui a ensuite, en marge du gouverneur de la province, prié également le procureur du Roi de bien vouloir prendre les initiatives requises en la matière. Dans le même temps, le Collège de police a désigné un auditeur privé en vue de procéder à un contrôle plus général du fonctionnement de la zone de police. En marge de cet audit privé dont le rapport final a été délivré en octobre 2021, le procureur du Roi a demandé concrètement à ce qu'il soit fait appel à l'Organe de contrôle « *afin de contrôler le traitement des informations et des données à caractère personnel enregistrées dans les banques de données policières ou de mener toute autre enquête relevant des compétences de l'Organe de contrôle et axée sur le traitement de l'information policière* ».

Le présent rapport expose les conclusions de l'enquête de contrôle susmentionnée.

## 2. OBJET DE LA VISITE ET MÉTHODOLOGIE

Comme nous le disions, le COC a accédé à la demande du procureur du Roi de Flandre occidentale et a mené une enquête de contrôle au sein de la PZ WV. En ce qui concerne le COC, cette enquête de contrôle était en sa qualité de « contrôle technique »<sup>13</sup> résolument axée sur la gestion de l'information policière. Si une visite sur place s'avérait nécessaire, elle durerait en principe au maximum une demi-journée.

Le 23.08.2021, le chef de corps de la PZ WV a été avisé par courrier que le COC allait procéder à un contrôle technique au sein de sa zone de police.

À travers de telles visites techniques, le COC aspire à se faire une idée des processus de travail de la zone de police dans le cadre de la gestion de l'information policière. En l'occurrence, la visite technique du COC se limite en principe aux thèmes suivants :

- contrôle des journalisations – motifs de la consultation – BNG, Registre national, casier judiciaire ;
- banques de données particulières ;

<sup>9</sup> Art. 240, 4<sup>o</sup> de la LPD.

<sup>10</sup> Dienst Onderzoeken / Service d'Enquête.

<sup>11</sup> Art. 244 et 247 de la LPD.

<sup>12</sup> Art. 248 de la LPD.

<sup>13</sup> Le COC subdivise actuellement comme suit ses contrôles/enquêtes/visites :

- **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 se penche surtout sur l'efficacité opérationnelle et l'exactitude des enregistrements effectués dans les banques de données. Un contrôle technique peut aussi parfois avoir trait à un problème plutôt ponctuel ;
- **un contrôle thématique** est une enquête menée sur un thème déterminé et qui peut inclure à la fois de la *desk research* et des visites sur place ;
- **un contrôle restreint** porte sur un seul ou sur quelques aspects (partiels) d'un traitement de données policier ou non policier ;
- **un contrôle international** couvre les éventuelles enquêtes internationales auxquelles le COC apporte son concours ;
- **un contrôle spécial** portant sur des matières particulières, comme les contrôles annuels des banques de données communes terrorisme et extrémisme ou les enquêtes *BELPIU*.

- triptyque<sup>14</sup> – arrestations judiciaires ;
- BNG : option 35<sup>15</sup> – validation centrale : situation/points d'attention

La visite se déclinait en trois phases.

Dans une première phase, les informations et documents nécessaires ont été demandés à la PZ WV. En fonction du contenu des réponses et des documents transmis, des questions spécifiques ont été posées en vue d'un examen plus approfondi de ces aspects lors de la visite proprement dite.

Dans un courrier introductif adressé au chef de corps de la zone de police, les documents suivants ont été demandés :

- un document de politique interne relatif à la création et à l'utilisation des banques de données particulières ;
- une liste des banques de données particulières utilisées au sein de la zone de police ;
- une liste des collaborateurs de la zone de police avec leurs fonctions actuelles.

En attendant de recevoir les documents demandés, le COC a demandé les journalisations pour la BNG et le Registre national.

La deuxième phase avait trait à l'analyse des documents reçus et des journalisations demandées.

La troisième phase consistait en la visite sur place proprement dite auprès de la PZ WV, qui se composait de plusieurs parties :

- 1) une introduction du COC et des membres présents de la zone de police ;
- 2) une discussion de la situation actuelle des banques de données particulières ;
- 3) une discussion sommaire des notes du corps transmises et des réponses aux questions posées par le COC ;
- 4) une discussion de l'analyse des journalisations demandées par le COC et des motifs de consultation ;
- 5) une visite guidée générale du commissariat qui s'assortissait de la possibilité de poser des questions ponctuelles.

### 3. CADRE JURIDIQUE

#### 3.1. Banques de données particulières

L'article 44/11/3 de la LFP dispose que la création d'une banque de données particulière n'est possible que si les missions de police administrative et judiciaire exigent que les services de police structurent les données à caractère personnel et les informations visées à l'article 44/1 de la LFP de manière à pouvoir les retrouver directement (il s'agit donc d'une banque de données 'opérationnelle').

L'article 44/11/3 §1<sup>er</sup> de la LFP prévoit par ailleurs comme condition à la création d'une banque de données particulière qu'elle ne soit possible que si les conditions cumulatives suivantes sont remplies :

- dans des circonstances spécifiques ;
- dans le cadre de l'exercice des missions et finalités de police administrative et judiciaire ;
- pour des besoins particuliers.

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

- a) la nécessité de classifier des données à caractère personnel ou informations au sens de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité ;
- b) l'impossibilité technique ou fonctionnelle d'alimenter la BNG de tout ou partie des données à caractère personnel et informations traitées dans ces banques de données ;

---

<sup>14</sup> L'établissement du triptyque est l'opération qui consiste à relever les empreintes digitales et palmaires, à prendre des photos et à établir le signalement individuel en vue de l'identification d'une personne (voir aussi le point 13).

<sup>15</sup> L'option 35 désigne le transfert normal de données d'ISLP vers la Banque de données nationale générale (BNG).

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

Conformément aux articles 58 et 59 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel (LPD), les services de police devront solliciter au préalable l'avis du COC lorsque :

- lors de la réalisation de l'analyse d'impact relative à la protection des données (AIPD)<sup>16</sup>, si le traitement, en particulier par le recours aux nouvelles technologies, est susceptible d'engendrer un risque élevé pour les droits et les libertés des personnes physiques (article 58) ;
- l'AIPD indique que le traitement présenterait un risque élevé si le responsable du traitement ne prenait pas de mesures pour atténuer le risque ; ou si le type de traitement, en particulier en raison de l'utilisation de nouveaux mécanismes, technologies ou procédures, présente des risques élevés pour les libertés et les droits des personnes concernées (article 59 §1<sup>er</sup> 1<sup>o</sup> et 2<sup>o</sup>).

La GPI ne peut donc par exemple pas retenir les arguments suivants pour créer une banque de données particulière :

- la charge de travail requise par la collecte, l'alimentation et le transfert des données vers la BNG ;
- le manque de connaissance de l'utilisation de la BNG ou d'une banque de données de base ;
- le manque (prétendu) de convivialité de la BNG ou d'une banque de données de base.

### 3.2. Triptyque

L'établissement d'un triptyque est essentiel pour la poursuite de l'objectif visant à fournir les bonnes informations, au bon moment et au bon endroit en vue de permettre une réalisation plus efficace des missions de police judiciaire et administrative.

Le triptyque judiciaire a pour but de contribuer à l'identification de personnes et se compose de 3 volets :

- a : empreintes digitales et palmaires ;
- b : photos ;
- c : signalement individuel.

### 3.3. Journalisation de la BNG

La police est tenue de conserver des fichiers de journalisation<sup>17</sup>. Un fichier de journalisation est l'instrument par excellence permettant de contrôler la licéité ou non du traitement et de garantir l'intégrité et la protection des données<sup>18</sup>. À ce titre, les fichiers de journalisation sont importants également dans le cadre des procédures disciplinaires internes ou des enquêtes administratives. Les statistiques du conseil disciplinaire de la GPI démontrent qu'une consultation illicite constitue l'infraction disciplinaire la plus fréquente. Les fichiers de journalisation sont par conséquent essentiels pour le contrôle tant proactif que réactif, et ce tant au niveau interne qu'externe.

Cette importance est également démontrée par la Directive commune contraignante des Ministres de la Justice et de l'Intérieur relative aux règles d'accès des membres des services de police à la banque de données nationale générale, aux banques de données de base, particulières et techniques du 13 juillet 2021 (*M.B.* 13 juillet 2021), en particulier au chapitre V intitulé 'L'identification, l'authentification et la journalisation (logging)' (« *L'accès aux banques de données et le traitement de données qu'elles contiennent font l'objet d'une journalisation (logging) (...)* »).

## 4. CONCLUSIONS DE L'ENQUÊTE

Le COC a reçu de la zone de police les documents suivants :

- une liste des banques de données particulières que la zone de police utilise dans le cadre de son fonctionnement opérationnel ;
- une liste des collaborateurs de la zone de police avec leurs fonctions actuelles.

<sup>16</sup> En anglais *DPIA* pour *Data Protection Impact Assessment*.

<sup>17</sup> Art. 56 §1<sup>er</sup> de la LPD donnant exécution à l'article 25 de la directive Police-Justice ; art. 44/4 §2, 2<sup>e</sup> alinéa de la LFP.

<sup>18</sup> Art. 56 §2 de la LPD.

#### 4.1. Banques de données particulières

Le 24 septembre 2021, le COC a reçu un e-mail de la PZ WVl indiquant que le document de politique interne demandé concernant la création et l'utilisation des banques de données particulières n'a pas encore été élaboré et serait en cours de rédaction. Lors de la concertation menée lors de la visite du 17.02.2022 auprès de la zone de police, il est apparu que l'élaboration de la note du corps n'avait pas encore été initiée. La PZ WVl aurait l'intention de se concerter à ce sujet avec une autre zone de police de l'arrondissement de Flandre occidentale.

Le COC a néanmoins reçu le 24 septembre 2021 de la PZ WVl une liste des banques de données particulières opérationnelles en usage selon la zone de police. La zone de police fournissait dans ce document une explication sommaire des données traitées dans ces banques de données. Sur cette base, le COC a procédé à une analyse *prima facie* dont il ressort que plusieurs de ces banques de données ne répondent pas aux critères permettant de les retenir en tant que banques de données particulières.

Le COC ne peut se défaire de l'impression que la zone de police, en dépit des conditions univoques énumérées à l'article 44/11/3 §1<sup>er</sup> de la LFP, éprouve des difficultés à distinguer les banques de données particulières des autres banques de données opérationnelles et non opérationnelles.

Vu l'absence de la note demandée relative aux banques de données particulières, le COC a demandé à titre de complément les notes permanentes relatives à la gestion générale de l'information. À la lecture de ces notes, le COC constate qu'il y est question de banques de données qui ne figurent pas sur la liste transmise des banques de données particulières, mais qui répondent peut-être tout de même aux critères permettant de les retenir en tant que banques de données particulières.

Par courrier du 07.12.2021, la PZ WVl a été informée des banques de données figurant sur la liste transmise qui peuvent effectivement être considérées comme des banques de données particulières. Il était également demandé dans ce courrier de dresser pour le 07.01.2022 au plus tard une nouvelle liste des banques de données en usage au sein de la PZ WVl. Le COC constate que la PZ WVl n'a pas donné suite à cette demande dans le délai imparti.

Le COC constate par ailleurs que pour les banques de données pouvant être considérées comme des banques de données particulières, il n'a pas été prévu de règles de ventilation ni de délais de conservation, ni même de journalisations.

Vu l'absence d'une nouvelle liste des banques de données particulières en date du 07.01.2022, la PZ WVl a indiqué lors de la visite sur place du COC qu'elle avait demandé aux chefs de service de dresser une liste de toutes les banques de données, après quoi il serait procédé à une analyse fonctionnelle des banques de données. Lors de la visite, le COC a remarqué que la coopération des personnes avec qui il s'est entretenu à l'établissement de la liste des banques de données particulières utilisées au sein du corps était plutôt limitée. Le chef de corps et le délégué à la protection des données ont à cette occasion indiqué qu'ils vérifieraient surtout eux-mêmes quelles banques de données sont encore en usage.

#### 4.2. Notes du corps relatives à la gestion de l'information

Devant l'absence d'un document de politique interne concernant la création et l'utilisation des banques de données particulières, le COC a demandé à la PZ WVl toutes les notes du corps relatives à la gestion de l'information, à la gestion de l'utilisation de la BNG, à la sécurité de l'information, à la gestion des accès, etc.

Le COC a reçu de la PZ WVl un certain nombre de notes du corps, qui ont été soumises à une analyse *prima facie* dont le COC a conclu que certaines des notes transmises ne sont plus conformes à la législation en vigueur, aux directives et/ou au fonctionnement interne de la zone de police.

Après cette analyse *prima facie*, les notes du corps ont été soumises à une analyse plus approfondie qui a révélé quelques aspects manquant de clarté sur lesquels le COC souhaitait obtenir des précisions. Un questionnaire a été adressé à ce sujet à la PZ WVl.

Le COC a reçu des réponses mais a constaté que la PZ WVl n'avait pas répondu à certaines questions, ou pas de manière complète, ce qui laisse à penser qu'il existe en interne au sein de la PZ WVl un manque de clarté quant à la teneur des notes du corps. Le COC s'est par conséquent vu dans l'obligation de transmettre un second questionnaire pour faire la lumière sur ces aspects.

Lors de la visite, des questions plus poussées ont été posées au sujet des aspects qui manquaient de clarté. Les réponses formulées par la PZ WVl ont révélé que les notes du corps existantes avaient d'urgence besoin d'une révision et n'étaient pas ou pas entièrement respectées par les collaborateurs concernés.



Pour ce qui est de l'information/de la direction des collaborateurs sur la base des notes du corps, le COC constate que la PZ WVl pourrait faire mieux. Il relève de la prérogative et de la mission légale du chef de corps de veiller à ce que les collaborateurs reçoivent des directives correctes et claires et à ce que celles-ci soient diffusées, suivies et évaluées au sein de la zone de police (application du cycle *PDCA*<sup>19</sup>).

#### 4.3. Journalisation et motif de la consultation (applications BNG-RRN)

L'aspect suivant abordé par ce contrôle technique était la journalisation des consultations de la BNG et du Registre national effectuées par les membres du personnel de la PZ WVl. Ces journalisations permettent – ou du moins devraient permettre – de vérifier le motif de la consultation, ou son absence.

Avant de consulter ces deux banques de données, il est obligatoire de spécifier le motif de la consultation.

La police est pour ce faire tenue de conserver des fichiers de journalisation. Un fichier de journalisation est l'instrument par excellence permettant de contrôler la licéité ou non du traitement et de garantir l'intégrité et la protection des données et du traitement de données.

Le COC a constaté que le motif de la consultation n'était pour ainsi dire jamais spécifié et que lorsqu'il l'était, il n'était pas suffisamment clair. Dans la mesure du possible, il convient de toujours encoder une référence la plus concrète possible pour motiver une consultation.

Un premier fichier de journalisation que le COC a examiné contenait toutes les consultations effectuées par les collaborateurs de police de la PZ WVl durant la période du 01.01.2021 au 13.09.2021 inclus. Il s'agit de consultations tant de données de citoyens que de données propres de collègues de la zone. Ces journalisations ont été filtrées de manière à retenir dans cette liste les collaborateurs de police qui ont effectué des recherches sur des collègues, qui ont recherché leurs propres données et/ou qui ont été recherchés par des collègues dans le Registre national (RRN), la BNG-consultation (PLC), la BNG-contrôle (PCT), la BNG-police administrative (BPC) et la BNG-circulation (TEC).

Sur la base de l'analyse de cette journalisation, le COC a constaté que 68 % des collaborateurs de la PZ WVl avaient effectué une recherche sur leurs propres données ou celles de collègues internes à la PZ WVl et que 84 % d'entre eux avaient effectué une recherche sur leurs propres données ou fait l'objet d'une recherche effectuée par un collègue. Ces constatations n'ont pas été analysées par le COC jusqu'au niveau individuel de chaque membre du personnel, d'une part parce que cela ne relevait pas de ses missions et compétences primaires, et d'autre part en raison de la capacité limitée. De plus, le COC n'est pas compétent pour mener des enquêtes pénales préliminaires à la demande du parquet ou du juge d'instruction. Autrement dit, dès que l'Organe de contrôle rencontre des indications d'infractions ou de délits, les informations pertinentes sont transmises au ministère public. Dans l'analyse *prima facie* réalisée par le COC, on trouvera par conséquent tant des recherches licites que des recherches illicites<sup>20</sup>.

Un deuxième fichier de journalisation était la liste des motifs de consultation. Une analyse de ce fichier de 793.440 lignes/consultations révèle une moyenne de 8 clics par session de consultation. Le COC constate que seuls 43.431 motifs de consultation (1,8 %) ont été retrouvés pour ces consultations. Sur ces 43.431 motifs de consultation, 42.489 avaient été spécifiés parce que c'était obligatoire pour des raisons techniques (informatiques), à savoir pour l'application RRN-photo. Pour la BNG et les consultations du RRN, le motif de consultation n'a été spécifié que pour 942 recherches, soit dans 0,1187 % des cas. Ici aussi, il est obligatoire de spécifier un motif de consultation mais il est techniquement possible d'effectuer une recherche sans le faire. Parmi ces 942 motifs, le COC n'a pu distinguer que 19 fois (0,0024 % des cas) un motif clairement identifiable comme un numéro de procès-verbal, un numéro d'apostille ou autre.

Le COC constate donc :

- que le motif de la consultation n'était pour ainsi dire jamais spécifié et que lorsqu'il l'était, il n'était pas suffisamment clair (par ex. « travailler », « cti », « IV », etc.). Dans la mesure du possible, il convient de toujours encoder une référence la plus concrète possible pour motiver une consultation : numéro de référence du CAD<sup>21</sup> pour le dispatching, numéro d'identification de l'équipe d'intervention à l'origine de la demande, etc. Les services d'intervention, les services de quartier, la police judiciaire et autres peuvent pour leur part utiliser par exemple le numéro de dossier, le numéro de procès-verbal ou le numéro de RIR<sup>22</sup>. Si l'on clique pour

<sup>19</sup> *Plan, Do, Check, Act*.

<sup>20</sup> Une recherche licite est une recherche dans le cadre de laquelle le collaborateur de police a un intérêt opérationnel à consulter une banque de données. Cet intérêt opérationnel n'est pas présent lors d'une recherche illicite.

<sup>21</sup> Numéro de référence attribué par le système *Computer-Aided Dispatching*.

<sup>22</sup> RIR désignant un rapport d'information.

accéder à d'autres informations durant une même session de consultation (intervention, quartier ou police judiciaire) ou intervention sur le terrain (dispatching dans le cadre d'une même intervention pour une même équipe déployée sur le terrain), il n'est évidemment pas nécessaire de saisir à nouveau un motif.

- qu'au sein des services à l'origine du plus grand nombre de consultations, comme le dispatching, l'application BNG-contrôle est étonnamment peu utilisée. Lorsque cette application n'est pas utilisée, il existe un gros risque de passer à côté d'une grande quantité d'informations ayant un impact direct sur le terrain, par ex. des signalements de personnes.

Le COC estime pouvoir conclure de l'analyse qui précède que les collaborateurs de la PZ WVl ne sont souvent pas conscients qu'il est légalement obligatoire de spécifier un motif de consultation avant d'effectuer une recherche ou une consultation. L'obligation de spécifier un motif de consultation est stipulée aux articles 56 §1<sup>er</sup>, §2 et §3 de la LPD et 44/11/3 §4 de la LFP. Le Comité de coordination de la GPI a publié à ce sujet une note permanente en 2021, qui portait la référence CG-2021/4833. La sensibilisation à l'obligation de spécifier un motif de consultation et, à titre subsidiaire, le suivi du respect de cette obligation relèvent des prérogatives du chef de corps en sa qualité de responsable du traitement.

Lors de la visite, la zone de police a indiqué que depuis l'entrée en service du délégué à la protection des données au sein de la zone (juin 2021), une journalisation avait été à une seule reprise demandée pour certains collègues sélectionnés arbitrairement. La zone de police a à cette occasion constaté elle-même que le motif de la consultation ne faisait pas la lumière sur le 'pourquoi' d'une consultation. Le chef de corps et le délégué à la protection des données ont alors convenu de demander plus fréquemment des journalisations et de mener à ce sujet une sensibilisation et un travail actifs.

En réponse à la demande du procureur du Roi, le COC a recherché quels collaborateurs de la zone faisaient l'objet d'un enregistrement dans *ISLP*. Sur la base des résultats obtenus, un certain nombre de dossiers ont été extraits d'*ISLP*. La journalisation de ces dossiers a permis au COC de constater qu'un certain nombre de collaborateurs de police avaient effectué des consultations et posé des actes dans les dossiers en question sans en être le verbalisateur. Certains collaborateurs de police avaient même, alors qu'ils étaient eux-mêmes des suspects dans le cadre d'un dossier donné, consulté et imprimé des procès-verbaux, etc.

Le résultat de ce volet de l'enquête a été transmis à toutes fins utiles et pour poursuite d'enquête au procureur du Roi de Flandre occidentale.

#### 4.4. Triptyque

Dans le sillage de la lecture d'une note interne, le COC a procédé dans *ISLP* à un contrôle par échantillonnage très restreint de faits pour lesquels on pourrait s'attendre à ce qu'un triptyque soit établi pour les suspects. Sur cette base, il a été examiné si les personnes étaient enregistrées de manière à permettre le contrôle de l'exactitude des enregistrements à partir du flux d'*ISLP*<sup>23</sup> vers la BNG<sup>24</sup>.

Ce contrôle par échantillonnage restreint a révélé que la PZ WVl ne recourt pas suffisamment à l'établissement du triptyque. Alors que la note permanente de la PZ WVl ne laisse planer aucun doute sur l'obligation d'établir un triptyque pour chaque arrestation judiciaire, il s'est avéré dans sept cas sur les neuf que le triptyque n'avait pas été établi ou n'était pas complet. Dans un seul cas, le triptyque était complet et le numéro AFIS<sup>25</sup> a pu être retrouvé dans la banque de données de base *ISLP*. Ce contrôle par échantillonnage semble indiquer que l'établissement du triptyque est loin de satisfaire aux exigences, et qu'il convient de prendre des mesures pour remédier à ce manquement. Une bonne gestion de l'information policière est en effet entièrement tributaire de l'accomplissement correct d'une série d'actes de base, dont le triptyque.

La PZ WVl a alors à son tour effectué une recherche détaillée pour les années 2020 et 2021, dont il est ressorti que le triptyque avait très rarement été validé. Le COC ne peut donc ici que constater, comme nous le disions, que la mission légale de l'établissement du triptyque n'est pas réalisée conformément à la directive MFO-3, ou l'est de manière largement insuffisante. Ce manquement met en péril le transfert de données vers la Banque de données nationale générale (BNG), et par extension l'efficacité et l'efficacités des traitements de données par et pour toute la police intégrée.

#### 4.5. Validation centrale

---

<sup>23</sup> Une banque de données de base telle que définie à l'article 44/11/2 de la LFP.

<sup>24</sup> La Banque de données nationale générale telle que définie à l'article 44/7 de la LFP.

<sup>25</sup> Numéro identique dans *ISLP* qui fait référence aux empreintes digitales relevées.



Un dernier aspect qui a été examiné avait trait à la réalisation de ce que l'on appelle une validation centrale<sup>26</sup> au sein de la zone de police.

Le COC peut en conclure qu'il est régulièrement procédé à la validation centrale au sein de la PZ WVL et que les données des banques de données de base sont transférées à la BNG correctement et dans le délai imparti.

## 5. CONCLUSION – REQUÊTES, RECOMMANDATIONS ET MESURES CORRECTRICES

En réponse à la demande initiale du COC en vue de fournir un document de politique interne concernant la création et l'utilisation des banques de données particulières, la PZ WVL a répondu que cette note du corps n'avait pas encore été élaborée mais serait en cours de rédaction et devrait encore être finalisée et validée. Lors de la visite sur place, il est apparu que la PZ WVL aurait l'intention de se concerter à ce sujet avec une zone de police voisine pour élaborer la note du corps. Le COC considère qu'il s'agit là d'un bon point de départ ; en revanche, il est urgent d'effectuer également les démarches nécessaires à l'égard de la sécurité de l'information et de la protection des données.

La sécurité de l'information requiert des efforts permanents dans le cadre desquels une approche structurelle et un suivi périodique sont indiqués. Le cadre régissant la sécurité de l'information doit par conséquent être déployé plus avant et implémenté, étant entendu qu'un certain nombre de travaux à réaliser dans le domaine de la sécurité de l'information requièrent un suivi, comme la mise en œuvre de la note du corps, la sensibilisation dans le cadre des recherches et du motif de consultation, l'établissement du triptyque, etc. Une gestion adéquate de l'implémentation de la sécurité de l'information en général au sein de la PZ WVL, par le truchement de la cellule de sécurité de l'information (CSI), est à cet égard primordiale. Le délégué à la protection des données est l'une des figures clés de cette CSI.

En ce qui concerne l'utilisation de banques de données opérationnelles et non opérationnelles comme la BNG, l'ISLP et le Registre national, le COC ne peut que constater que les obligations légales régissant la consultation de ces banques de données ne sont soit pas connues, soit délibérément ignorées. Le fait que les collaborateurs de police effectuent des recherches sur les données de collègues et/ou sur leurs propres données témoigne d'une importante et alarmante crise de valeurs au sein de la zone de police, qui pourrait à son tour engendrer une méfiance réciproque croissante et des dysfonctionnements au sein de la zone de police. La PZ WVL doit par conséquent miser résolument sur la sensibilisation, le contrôle et la répression (pour une part avec l'aide des instances judiciaires et administratives) de ces pratiques afin de les ramener à un niveau correspondant à celui de recherches licites.

Dans le cadre de la qualité des traitements de données effectués par la police, tous les actes revêtent de l'importance et ici aussi, le COC est au regret de constater qu'un acte de base comme la réalisation du triptyque pose problème au sein de la zone de police. La PZ WVL a elle-même pu constater la présence d'un grand nombre de triptyques incomplets et non validés. Là encore, c'est au chef de corps qu'il appartient d'élaborer la politique qui permettra la réalisation correcte des actes de base et d'en assurer le suivi.

L'Organe de contrôle est d'avis que bien que plusieurs domaines, également parmi ceux relevant de la portée du présent contrôle, laissent encore largement matière à amélioration et nécessitent des actions, les dirigeants de la zone de police ne manquent pas de bonne volonté lorsqu'il s'agit de plancher sur ces aspects et d'élaborer et de mettre en œuvre une politique adéquate en matière de sécurité de l'information. Le COC a également décelé chez les collaborateurs qui ont pris part à la visite une volonté manifeste de s'acquitter correctement de leurs tâches et de remédier aux manquements mis au jour par le COC.

### **L'Organe de contrôle**

#### **prie la PZ WVL**

#### Requête

---

<sup>26</sup> Les données structurées enregistrées sont, à l'issue de leur préparation dans l'application locale (ISLP, enregistrement local, Feedis, ...), transmises au niveau central où elles font l'objet d'un contrôle automatique.

de transmettre un nouveau point de la situation concernant les banques de données particulières dans un délai de maximum 3 mois à compter de la réception du présent rapport ;

## **émet les recommandations suivantes :**

### Recommandation 1

Le COC recommande à la PZ WVL de s'atteler à présent vraiment à l'élaboration d'un **document de politique interne relatif aux banques de données particulières** qui pourra être considéré comme un premier pas pertinent dans le processus visant à mettre en place au sein de la zone de police une politique univoque dans le cadre de l'implémentation des banques de données particulières ;

### Recommandation 2

Les données ne peuvent être traitées que lorsqu'elles sont encore adéquates, pertinentes et non excessives. Le COC recommande de prévoir **pour les banques de données particulières une évaluation régulière** et la détermination de **délais de conservation** ;

### Recommandation 3

Dans le cadre d'une **politique rigoureuse du contrôle de l'accès aux banques de données particulières**, le COC insiste pour qu'il soit **recouru à l'AMF<sup>27</sup>** si cette possibilité technique peut être prévue. Ce système permet en effet de réduire les risques inhérents à l'utilisation de mots de passe ;

### Recommandation 4

Le COC recommande de prévoir pour la consultation des **banques de données particulières** un **champ à compléter** qui devra permettre de spécifier le **motif de la consultation**. L'utilisation de cases à cocher ne suffira pas à obtenir une donnée identifiable, ni à satisfaire aux dispositions légales des articles 56 §1<sup>er</sup>, §2 et §3 de la LPD et 44/11/3 §4 de la LFP ;

### Recommandation 5

Le COC recommande d'élaborer une **politique de sécurité de l'information** et un **plan de sécurité de l'information**, et/ou au besoin d'actualiser et remplacer les notes du corps relatives au fonctionnement opérationnel, aux traitements de données, à la gestion de l'information, etc. ;

### Recommandation 6

Le COC recommande également de créer une **cellule de sécurité de l'information (CSI) interne** composée des parties prenantes impliquées dans la sécurité de l'information, la protection et l'échange de données (délégué à la protection des données, chef de corps, service TIC, CIL, etc.). Le COC recommande que cette CSI se réunisse régulièrement afin de mettre en place, de réaliser, d'évaluer et au besoin d'adapter les évaluations et le suivi nécessaires de la politique régissant cette matière ;

### Recommandation 7

Le COC recommande d'attirer régulièrement **l'attention des membres du personnel sur les notes du corps** existantes et de veiller à ce que les directives qu'elles contiennent soient respectées ;

### Recommandation 8

Conformément à la directive ministérielle MFO-3 et aux fiches qui y sont jointes, il convient de toujours établir le **triptyque complet ou partiel** prévu par la directive. Vu les manquements importants constatés au niveau de l'établissement des triptyques au sein de la zone de police, le COC insiste pour que ces directives soient communiquées, expliquées et régulièrement répétées (à travers des campagnes de sensibilisation). Il est important également de prévoir en permanence, sur une base structurelle et périodique, la fourniture d'informations au sujet de l'établissement du triptyque, et ce par le biais de différents canaux d'information (e-mails/intranet/séances d'information/formations/...), et de procéder régulièrement à des contrôles par échantillonnage ;

## **ordonne les mesures correctrices suivantes à la PZ WVL,**

Vu les articles 221 §1<sup>er</sup> et 247, 4<sup>o</sup>, 5<sup>o</sup> et 6<sup>o</sup> de la LPD,

### Mesure correctrice 1

---

<sup>27</sup> AMF signifiant authentification multi-facteurs.

Réaliser une **analyse fonctionnelle des banques de données particulières**. Les banques de données particulières qui ne sont plus conformes aux dispositions légales doivent être supprimées et leurs données effacées. Aussi longtemps que cette analyse n'a pas été réalisée et vu que les banques de données particulières font à présent l'objet d'une utilisation opérationnelle, il existe un risque réel de traitement illicite de données à caractère personnel. Cette analyse sera transmise au COC dans un délai de 6 mois à compter de la réception de la présente mesure correctrice ;

#### Mesure correctrice 2

**Déclarer les banques de données particulières** de préférence dans le **RegPol**, et à titre subsidiaire au moins dans un propre registre des traitements, et faire parvenir à l'Organe de contrôle la confirmation et l'aperçu de ces déclarations dans un délai de 6 mois à compter de la prise de connaissance de la présente mesure correctrice ;

#### Mesure correctrice 3

Consulter régulièrement les **journalisations de la BNG** et procéder à des **contrôles proactifs, par échantillonnage** (au moins 1x/an), dans le but de vérifier le respect de l'obligation d'introduire le **motif de la consultation** et de détecter les **éventuelles consultations illégitimes**, et ce une première fois dans les six mois à compter de la prise de connaissance de la présente mesure correctrice, et faire part au COC des résultats de ces contrôles ;

#### Mesure correctrice 4

Élaborer **un règlement/une politique** prévoyant un **mécanisme de contrôle** périodique et effectif du monitoring d'**éventuelles consultations (il)licites de la BNG, des banques de données de base et des banques de données particulières**.

Les fichiers de journalisation des traitements doivent être conservés pendant au minimum dix ans. Le responsable du traitement peut, si nécessaire, prolonger ce délai de maximum vingt ans par une décision motivée et après évaluation. Le COC demande de prévoir les fichiers de journalisation nécessaires et de les tenir à la disposition des organes de contrôle compétents. L'Organe de contrôle ordonne à la PZ WV de procéder à un contrôle annuel obligatoire des journalisations et de tenir les résultats à la disposition du COC.

Dit pour droit que la date d'entrée en vigueur des mesures correctrices 1 à 4 incluse et la date de prise de connaissance desdites mesures doivent être comprises comme étant la date de la transmission du présent rapport **définitif** de l'Organe de contrôle augmentée de deux jours.

L'Organe de contrôle informe la zone de police de la possibilité dont elle dispose d'introduire un recours dans les 30 jours de la décision auprès de la Cour d'appel du domicile ou du siège du demandeur (article 248 §1<sup>er</sup>, alinéa premier, et §2 de la LPD).

Ainsi décidé par l'Organe de contrôle de l'information policière le 4 juillet 2022.

Koen Gorissen  
Membre-conseiller  
[signé]

Frank Schuermans  
Membre-conseiller  
[signé]

Philippe Arnould  
Président  
[signé]