CONTRÔLE TECHNIQUE

RAPPORT DU CONTRÔLE ET DE LA VISITE DE LA ZP DANS LA PROVINCE DU HAINAUT PAR L'ORGANE DE CONTRÔLE DE L'INFORMATION POLICIÈRE DANS LE CADRE DE SES COMPÉTENCES EN MATIÈRE DE CONTRÔLE ET DE SURVEILLANCE

VERSION PUBLIQUE

Référence : CON20002

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

Table des matières

1 Introduction 3
1.1 Les pouvoirs de l'Organe de contrôle de l'information policière (COC) 3
2 ORGANISATION ET METHODOLOGIE DU CONTRÔLE 4
2.1 La première phase 5
2.2 La deuxième phase 5
3 CADRE JURIDIQUE 6
3.1 Les banques de données particulières (GBO) 6
3.2 L'accès et les traitements illégitimes aux banques de données 7
3.3 Le flux de l'information et l'alimentation de la BNG 8
3.4 Le triptyque 9
4 RESULTATS DU CONTRÔLE 9
4.1 Situation du DPO au sein de la ZP Hainaut 10
4.2 Les banques de données particulières 10
4.3 Logging 12
4.4 Fonctionnement et alimentation de la BNG 13
4.5 Triptyque 14
5 CONCLUSIONS – RECOMMANDATIONS, DEMANDES ET MESURES CORRECTRICES 15

VERSION PUBLIQUE[1]

1 Introduction

1. Compte tenu de ses compétences en tant que service de contrôle externe et autorité de contrôle compétente en matière de traitement des données par la police intégrée organisée à deux niveaux (GPI), l'Organe de contrôle de l'information policière ('Organe de contrôle' ou 'COC') a décidé de procéder à un 'contrôle technique'[2] de la zone de police dans la province du Hainaut (ZP Hainaut). Le présent rapport est lié aux conclusions du contrôle.

1.1 Les pouvoirs de l'Organe de contrôle de l'information policière (COC)

2. Dans le cadre de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel (LPD)[3], le COC a été réformé et est devenu une autorité de contrôle à part entière. L'article 71 §1 et le titre 7 LPD définissent les tâches et compétences du COC. Il s'agit notamment des missions de contrôle contenues dans les articles 44/1 à 44/11/14 de la Loi sur la Fonction de Police (LFP) en ce qui concerne la gestion de l'information des services de police. Parmi ses missions, le COC a été chargé d'une mission de surveillance[4] et de contrôle[5]. Cela signifie qu'en plus de la protection de la vie privée et des données, le COC se préoccupe également d'éléments tels que l'efficience et l'efficacité de l'action policière.

Le COC est compétent notamment pour les services de police[6], pour l'Inspection générale de la police fédérale et locale (AIG)[7] et pour l'unité d'Information des Passagers (UIP)[8].
La compétence du COC en ce qui concerne les services de police couvre à la fois les activités de traitement opérationnelles (Titre 2 LPD) et non opérationnelles (RGPD)[9].

---

[1] 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.

[2] Le COC fait la distinction entre plusieurs formes de contrôle ou de supervision :
- **Contrôle global** : il s'agit d'une enquête de surveillance qui s'accompagne d'une ou plusieurs visite(s) approfondie(s) sur le terrain ou de visites où la portée de la surveillance est très large.

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

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

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

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

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

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

[4] Les missions de surveillance sont axées sur le respect par les forces de police des règles en matière de protection des données et du respect de la vie privée.

[5] Lors des missions de contrôle, l'accent est mis sur le respect d'autres dispositions légales ou réglementaires et le COC examine également pour le thème à analyser un ou plusieurs des trois E classiques en matière d'audit : *Efficiency, Effectiveness et Economy*.

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

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

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

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

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

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

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

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

En ce qui concerne l'utilisation de caméras non visibles, le COC agit comme une sorte de commission « MPA »[10]. Selon l'article 46/6 LFP, toute autorisation et modification de l'utilisation non visible de caméras dans les cas visés à l'article 46/4 doit être notifiée au COC, sauf lorsque l'utilisation de caméras est effectuée sous l'autorité d'un magistrat. Dans ce cadre, le COC examine si les conditions de la décision de mise en œuvre ou de la prolongation de la mesure sont remplies.

En outre, le COC traite les plaintes relatives à l'application de la législation qui concerne le traitement des données personnelles par les service de police [11]. A cette fin, les membres du COC et les membres du service d'enquête (DOSE)[12] disposent de pouvoirs d'enquête et des mesures correctrices peuvent être prises[13].

Certaines décisions du COC peuvent faire l'objet d'un recours dans un délai de 30 jours devant la Cour d'Appel du lieu de résidence ou du siège social du plaignant, qui traitera l'affaire comme une procédure interlocutoire conformément aux articles 1038, 1040 et 1041 du Code judiciaire[14].

2 ORGANISATION ET METHODOLOGIE DU CONTRÔLE

3. Le 21 janvier 2021, l'Organe de contrôle a effectué, de sa propre initiative, un contrôle technique[15] de la zone de police Hainaut. Le contrôle n'est donc pas le résultat d'une plainte (individuelle) ou de l'existence d'indications (concrètes) de non-respect des lois et règlements par la zone de police contrôlée.

4. Tenant compte du champ d'application, de la nature des données et de la forme du traitement dans le cadre de la création de banques de données particulières, de l'utilisation de la BNG, des arrestations judiciaires au sein des forces de police et du 'triptyque' y afférent, ces traitements de données représentent une atteinte considérable à la vie privée. En vue d'une collecte correcte des informations, ces processus sont liés à des conditions d'application qui sont décrites dans la législation (principalement la LFP et la LPD), les arrêtés, ainsi que les lignes directrices (y compris principalement la MFO3[16] et le Vademecum[17]). Le COC examine si les banques de données particulières ont été créées conformément aux règles applicables, si les arrestations judiciaires et l'exécution du triptyque ont été effectués conformément à la règlementation applicable et de manière qualitative, et comment l'utilisation de la BNG fonctionne dans la zone.

[10] **M**éthodes **P**articulières en police **A**dministrative.
[11] Art. 240, 4° et 247 LPD.
[12] **D**ienst **O**nderzoek / **S**ervice d'**E**nquête.
[13] Art. 244 et 247 LPD.
[14] Art. 248 LPD.
[15] Comme son nom l'indique, un contrôle technique est une enquête technique essentiellement opérationnelle portant à chaque fois sur un ou plusieurs sujets spécifiques, tels que le 'contrôle du triptyque', 'l'alimentation de la BNG', 'l'accès illicite' et la 'journalisation' (voir également l'article 236 §3 et l'article 239 LPD). Ce type de suivi est moins axé sur les aspects juridiques ou les aspects de la protection des données ou de la vie privée sans pour autant les perdre de vue (voir également note de bas de page 1).
[16] Directive commune MFO3 du 14 juin 2002 du Ministre de la Justice et de l'Intérieur relative à la gestion de l'information de police judiciaire et de police administrative, *M.B.*, 18 juin 2002.
[17] Le guide pour un enregistrement uniforme et de qualité en BNG.

5. Avec ce type de contrôle technique, le COC vise à obtenir un aperçu des processus de travail de la zone de police en ce qui concerne la gestion de l'information policière. *In casu*, le contrôle était limité aux thèmes spécifiques suivants:

- Banques de données particulières:
    - le processus de l'alimentation et la saisie ;
    - la relation avec d'autres banques de données policières ;
    - le processus de la ventilation (vérifications des délais de conservation)
        - gestion d'accès et traçabilité
        - sécurité de l'information ;
- Consultations (traitement) illégitimes des banques de données - Contrôle des *loggings*[18]
- Fonctionnement et alimentation de la BNG: option 35[19] – validation centrale: état des lieux/points d'attentions
- Triptyque.

6. Le contrôle est scindé en deux phases:

2.1 La première phase

Dans un premier temps, la zone de police concernée est informée du contrôle et des questionnaires et documents sont échangés. En fonction du contenu des réponses et des documents, des questions supplémentaires spécifiques sont posées en vue d'une enquête plus approfondie pendant le contrôle. En l'occurrence, le COC a envoyé un premier questionnaire le 25-02-2020 pour un contrôle le 31-03-2020. Le 12-03-2020, la ZP Hainaut a renvoyé les éléments de réponse. Toutefois, en tenant compte de la situation COVID, il a été décidé d'un commun accord de postposer le contrôle à une date ultérieure. Le 03-08-2020, le COC a repris contact avec la ZP Hainaut et la date du 21-10-2020 a été retenue pour le contrôle sur place.

Suite au départ imprévu du DPO de la ZP Hainaut, la zone a demandé le 03-09-2020 de postposer le contrôle au 10-11-2020. Suite aux évolutions de la crise sanitaire au sein de la zone de police (absence de 25% des effectifs), la zone de police a demandé le 29-10-2020 à nouveau à postposer le contrôle. Une proposition de faire le contrôle via Teams n'a pas été retenue car l'objectif d'un contrôle technique ne peut pas être atteinte de manière virtuelle. Le 06-11-2020, la date du 21-01-2021 a été retenue pour le contrôle sur place.

Le COC a reçu les documents suivants :

- Le 12-03-2020: éléments de réponses au questionnaire, copie de la liste GBO[20], fichiers des consultations abusives, et le plan d'action DPO 2018, bilan 09-03-2020
- Le 03-09-2020, une liste des privations de liberté a été sollicitée afin de faire des vérifications dans le cadre du triptyque. Cette liste a été envoyée au COC le 04-11-2020.

2.2 La deuxième phase

La deuxième phase consiste à la réalisation du contrôle en lui-même.

En l'occurrence, le contrôle s'est déroulé comme suit:

1. Introduction du COC et des membres de la zone de police présents
2. Questions sur les banques de données particulières
3. Evaluation du contrôle des loggings BNG sur base d'une semaine de consultations en janvier 2020
4. Examen du fonctionnement et de l'alimentation de la BNG

[18] La **journalisation** (en anglais *logging*) est l'action de relever dans un journal (en anglais *log*) tous les évènements qui se produisent dans un système informatique pendant son fonctionnement. La journalisation permet d'effectuer des analyses diverses, généralement statistiques et de faire des hypothèses sur les dysfonctionnements ou les pertes de performance d'un système.

[19] L'option 35 est l'action automatisée par laquelle le gestionnaire fonctionnel permet aux données/entités relatives à un fait concret d'être encodées dans la BNG.

[20] Abréviation pour les banques de données particulières.

5. Vérification de l'exécution du triptyque

3 CADRE JURIDIQUE

3.1 Les banques de données particulières (GBO)

7. L'art. 44/11/3 LFP stipule que la création d'une banque de données particulière (GBO) n'est possible que si l'exercice des missions de police administrative et de police judiciaire nécessite que les services de police structurent les données à caractère personnel et les informations visées à l'art. 44/1 LFP de manière à ce qu'elles puissent être consultées directement (il s'agit donc d'une banque de données 'opérationnelle').

8. La création d'une GBO par les services de police doit, conformément à l'article 44/11/3 LFP, répondre aux critères repris ci-dessous:

- être créée dans des circonstances spécifiques;
- être créée dans le cadre de missions de police administrative ou judiciaire;
- être créée pour des besoins (opérationnels) particuliers.

L'article 44/11/3 §2 LFP prévoit aussi que la création d'une GBO soit 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;

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.

9. Les finalités et les conditions de la création d'une GBO sont donc clairement définies par la loi. Ces dispositions légales sont également le point de départ pour que le COC considère une banque de données comme une GBO. Avant d'inclure cette banque de données dans le registre national des traitements[21] (REGPOL) ou dans un registre local, le responsable du traitement doit passer en revue ces critères, les cocher et fournir les explications ou commentaires nécessaires.

10. Conformément aux art. 58 et 59 LPD, les services de police doivent solliciter l'avis du COC lorsque :

- un type de 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 (art. 58);
- l'analyse d'impact relative à la protection des données (AIPD) indique que le traitement présenterait un risque élevé si le responsable du traitement ne prenait pas de mesures pour atténuer le risque; ou lorsque 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 (art. 59 §1, 1° et 2° LPD).

11. La GPI ne peut donc reprendre les arguments suivants afin de pouvoir créer une banque de données particulière:

- la trop grande charge de travail nécessaire pour la saisie, l'alimentation et le transfert des données vers la BNG;
- le manque de connaissances de l'utilisation de la BNG ou d'une banque de données de base;

[21] Art. 55 LPD et art. 145 LPI.

- le manque de convivialité (supposé) de la BNG ou d'une banque de données de base.

3.2 L'accès et les traitements illégitimes aux banques de données

12. La consultation d'une banque de données policière ou d'une banque de données accessible aux services de police constitue un traitement au sens de la LPD[22].

Dès lors, la règle de principe de l'article 44/1 de la LFP qui prévoit que « *les services de police peuvent traiter des informations et des données à caractère personnel pour autant que ces dernières présentent un caractère adéquat, pertinent et non excessif au regard des finalités de police administrative et judiciaire pour lesquelles elles sont obtenues et pour lesquelles elles sont traitées ultérieurement* » doit être appliquée aux consultations de ces banques de données.

Un fichier de journalisation doit être mis en place pour certains traitements dont la consultation, la communication et l'effacement de données. Ce fichier doit permettre d'établir notamment le motif, la date et l'heure du traitement, les catégories de personnes qui ont consulté les données et si possible leur identification[23].

L'article 44/4 §2, alinéa 2 de la LFP implémente cette obligation au niveau des services de police et reprend les conditions énoncées ci-dessus.

L'article 28 de la LPD, qui énonce les principes de traitement, indique que les données à caractère personnel sont traitées de manière licite et loyale, c'est-à-dire d'une part que le traitement doit être nécessaire à l'exécution d'une mission effectuée par les services de police pour les finalités énoncées à l'article 27 de la LPD, et d'autre part que le traitement doit être fondé sur une obligation légale ou réglementaire[24].

Parmi les principes de traitement se trouve également l'interdiction de traiter les données de manière incompatible avec les finalités pour lesquelles elles ont été collectées[25].

Les services de police sont tenus d'établir des fichiers de journalisation. Une journalisation est un instrument idéal pour vérifier la preuve de la/l'(il)licéité du traitement et pour garantir l'intégrité et la sécurité des données. En effet, le motif de traitement doit permettre à celui qui a traité les données de démontrer que le traitement effectué – ici la consultation – répond au prescrit des articles 44/1 de la LFP et 28 de la LPD.

À cet égard, les journalisations sont également importantes dans le cadre de procédures disciplinaires internes ou d'enquêtes administratives. La consultation illégale est une des infractions disciplinaires les plus fréquemment commises. Les journalisations sont donc importantes à des fins de contrôle proactif et réactif, tant au niveau interne qu'externe. Leur importance est également démontrée par la récente décision du Comité de Direction de la police fédérale de rendre obligatoire la raison de la consultation[26].

La problématique liée à l'accès/au traitement illégitime dans les banques de données policière et accessibles aux services de police n'est pas un phénomène nouveau. Il s'agit là d'un type d'estompement de la norme présent au sein des services de police et qui a déjà été mis en évidence à plusieurs reprises. Le dernier rapport annuel du conseil de discipline de la police intégrée[27] indique que la transgression disciplinaire la plus fréquente est l'usage irrégulier des banques de données.

[22] Art. 26, 2° LPD.
[23] Art. 56 LPD.
[24] Art. 33 LPD.
[25] Voir également : Organe de contrôle de l'information policière, *Avis d'initiative relatif au cadre juridique (de protection des données) lors de consultations illicites de banques de données par les membres de la police intégrée, de l'AIG et de l'Unité d'information des passagers*, 13 décembre 2018, DD180009 (consultable sur www.organedecontrole.be).
[26] Comité de Direction du 21 septembre 2020, point 3, numéro de référence CG/2020/4855.
[27] Rapport Conseil de Discipline de la police intégrée 2018.

Les banques de données à la disposition des fonctionnaires de police sont assez nombreuses, les principales sont : la BNG[28] , le RRN[29], le RCA[30], le SIDIS[31], et la DIV[32] sans oublier l'ISLP[33] et le FEEDIS[34] , ainsi que d'autres banques de données plus spécifiques comme par exemple la banque de données FTF[35] , et BELPIU[36] au niveau national ou d'autres banques de données particulières répondant à des spécificités locales ou encore des banques de données internationales comme SIS II[37] ou celles d'Interpol.

Dans leurs missions quotidiennes les fonctionnaires de police sont amenés à accéder et à interroger ces différentes banques de données à de nombreuses reprises. Ces contrôles doivent s'effectuer en respectant le cadre légal et répondre à un but légitime. Le principe communément appelé '*la raison d'en connaitre' (need to know)* est applicable en cette matière.

En outre, une note interne permanente de la police fédérale rappelle ces règles et les éventuelles sanctions disciplinaires et/ou pénales qui s'appliquent en cas de consultation illégitime[38].

3.3 Le flux de l'information et l'alimentation de la BNG

13. La gestion et le traitement de l'information de police judiciaire et de police administrative sont réglés par la LFP[39].

Au niveau de la police locale, c'est le chef de corps qui porte les responsabilités suivantes en matière de traitement de l'information de police judiciaire et administrative :

- le contrôle de la qualité de l'information traitée et transmise, en ce compris la mise à jour;
- la garantie de l'exhaustivité de l'information traitée et transmise;
- le contrôle du respect des procédures correctes.

Le concept de la BNG dans sa totalité[40] vise à fournir l'information exacte au bon moment et au bon endroit, avec pour but une exécution plus efficiente et plus effective des missions de police. Le principe de base du concept total est l'intégration des besoins en information de manière transparente dans les activités policières opérationnelles. Pour alimenter la banque de données nationale générale, il suffit que chaque policier exécute correctement sa mission d'information policière.

La manière dont la BNG est alimentée par les différents services de police influence considérablement la qualité des informations présentes dans cette banque de données opérationnelle. Les règles d'alimentation de la BNG sont énoncées dans la directive MFO3 et le Vademecum[41].

---

[28] La BNG est la banque de données relationnelle policière dans laquelle des entités (Personnes, organisations, moyens de transport, lieux, objets et numéros) sont enregistrées pour autant qu'elles puissent être au moins reliées à un fait infractionnel ou à une enquête judiciaire et que les conditions pour l'enregistrement soient remplies.

[29] **R**ijks**R**egister/**R**egistre **N**ational. Le RRN désigne le système de traitement d'informations qui assure l'enregistrement, la mémorisation et la communication d'informations relatives à l'identification des personnes physiques c'est-à-dire les citoyens.

[30] **R**egistre **C**entral des **A**rmes.

[31] **S**ystème d'**I**nformation des **D**étentions / **D**etentie **I**nformatie**S**ysteem.

[32] La DIV est la banque de données de l'immatriculation des véhicules.

[33] ***I****nformation* ***S****ystem* ***L****ocal* ***P****olice*. ISLP est une banque de données de base, utilisée par la plupart des services de police fédérale et locale afin d'assurer les fonctionnalités de base.

[34] ***F****eeding* ***I****nformation* ***S****ystem*. FEEDIS est une banque de données de base qui rassemble deux applications permettant la rédaction, la gestion des documents, l'alimentation du système central (BNG) et le rapportage d'information en matière judiciaire. Ces applications, "Feedis - PV judiciaires & Requêtes" et "Feedis - RIR" sont destinées aux membres de la police judiciaire fédérale chargés de missions de police judiciaire.

[35] ***T****errorist* ***F****ighters* (Combattants Terroristes).

[36] La Banque de données de l'Unité d'Informations des Passagers.

[37] Système d'Information Schengen de la 2ième génération.

[38] Note permanente de la police fédérale*, Consultation des banques de données policières ou mises à disposition des services de police*, 9 octobre 2007, CGO-2007/3141.

[39] Art 44/1 et suivants LFP.

[40] Directive commune MFO3, *op.cit.*.

[41] Le Vademecum Police Judiciaire reprend en détails les règles de saisie et de l'alimentation de la BNG.

3.4 Le triptyque

14. Les règles relatives à l'exécution du triptyque proviennent de la directive MFO3[42]. L'exécution du triptyque est essentielle pour apporter la bonne information au bon moment et au bon endroit en vue d'une exécution plus efficace et plus efficiente des missions de police judiciaire et administrative.

15. Le triptyque judiciaire est réalisé afin d'aider à l'identification des individus et se compose :

- de la description individuelle de la personne (MFO3, fiche B03 - Notice individuelle) ;
- des empreintes digitales et palmaires (MFO3, fiche B04 - Empreintes digitales et palmaires et les traces papillaires) ;
- des photos de la personne (MFO3, fiche B05 - La prise et le traitement des photos de personnes dans le domaine judiciaire).

16. Le triptyque est établi dans le cadre des missions de police judiciaire et, le cas échéant, dans le cadre de la loi du 15 décembre 1980 sur l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers (loi sur les étrangers).

17. La notion 'personne' signifie dans ce contexte:

- l'auteur, le coauteur, le complice ou le suspect (catégorie "*SUSPECT*");
- la personne qui n'a pas de titre de séjour légal ou qui n'a pas de documents d'identification, à l'exception du mineur étranger non accompagné (« *MENA* ») ou du demandeur d'asile (catégorie "*SUSPECT*");
- la victime, la personne lésée, le témoin ou le(s) membre(s) des services de police ou de secours présents sur la scène du crime (catégorie "*NON SUSPECT*"). Chaque cadavre est considéré comme appartenant à la catégorie "*non suspect*" (lors de la prise d'empreintes digitales et palmaires);
- la personne disparue (prise de photos);
- la personne disparue ou la personne qui fait l'objet d'une mesure à prendre (rédaction d'une description individuelle).

18. La prise d'empreintes d'un suspect est **obligatoire** si la personne concernée a plus de 14 ans et si elle est soit:

- entendue et pour laquelle un lien avec un fait concret est confirmé (prouvé) ou si la personne fait l'objet de soupçons sérieux des services de police (pour autant qu'il ne s'agisse pas d'un fait concret du type 4[43]);
- privée de liberté (à partir du moment où, pour les besoins de l'enquête, la personne concernée n'est plus libre d'aller et de venir à son gré);
- mise à la disposition de l'autorité judiciaire ou de l'Office des Etrangers;
- à écrouer dans un établissement pénitentiaire suite à une ordonnance ou une décision judiciaire.

19. Pour les mineurs de moins de 14 ans, le magistrat en charge du dossier doit en outre avoir donné son autorisation pour effectuer le triptyque de l'identification judiciaire. Cette autorisation est à mentionner dans le procès-verbal.

20. En cas de séjour illégal, le triptyque judiciaire **DOIT** toujours être appliqué[44].

4 RESULTATS DU CONTRÔLE

[42] Directive commune MFO3, *op.cit.*.
[43] Un fait concret de type 4 est un fait concret qui en raison de la constitution d'une image complète relative aux entités liées, et en raison des objectifs de gestion, est toujours enregistré dans la BNG.
Le fait, qu'il n'existe pas (encore) de liaisons (couplages) avec d'autres entités (suspect, préjudice...), n'a aucune incidence sur l'enregistrement en BNG. Les faits sont saisis sur base du principe que des données relatives aux autres entités (suspects, préjudice,...) suivront, au fur et à mesure que le temps avancera (PV subséquent).
Le fait de type 4 fait l'objet d'une saisie limitée (pas de modus operandi, traces, …).
[44] Directive commune MFO3, *op.cit.*, Fiche B04.

4.1 Situation du DPO au sein de la ZP Hainaut

21. Lors du contrôle du 21-01-2021, la ZP Hainaut a porté à la connaissance de l'Organe de contrôle les informations exposées ci-dessous.

En date du 20-04-2020, la DPO a informé la ZP Hainaut qu'elle souhaitait quitter la zone pour un stage d'un an débutant le 1er juin 2020. Cette dernière avait déjà été absente de la zone de police suite à la crise COVID et pour des congés entre le 16 et le 31 mars et du 11 au 21 avril 2020. Ensuite, l'intéressée pouvait bénéficier de ses congés annuels qu'elle a sollicités du 23 avril au 30 mai (sauf le 08-05-2020 pour dernier jour de reprise/remise). Elle n'a donc presté que 3 jours entre le 20-04-2020 et le 01-06-2020.

La juriste de la ZP Hainaut a été désignée DPO début juin 2020 mais cette dernière n'avait suivi aucune formation en matière de DPO/RGPD et héritait de la reprise de l'ensemble des dossiers, qu'elle cumulait en plus de ses autres fonctions.

La ZP Hainaut a également décidé de recruter un Niveau B afin de renforcer la cellule juridique. Toutefois, jusqu'à présent, personne n'a réussi les tests.

22. La ZP Hainaut a souhaité insister sur l'autonomie dont doit bénéficier un DPO en précisant que cette autonomie est essentielle pour les avis qu'un DPO doit remettre, qu'il doit être indépendant et autonome à cet effet. Toutefois, la ZP Hainaut a ajouté que son rôle ne doit pas se limiter à remettre des avis, le DPO doit aussi pouvoir contribuer à remettre des propositions, à accompagner les services dans la mise en œuvre de processus RGPD, effectuer des contrôles en matière RGPD. La ZP Hainaut a également indiqué que de multiples interprétations sont effectuées au niveau des DPO à propos de la manière d'exécuter leurs missions et qu'une uniformisation serait opportune. La ZP Hainaut déplore le manque de directives/conseils émanant de la police intégrée dans la mise en conformité LPD et l'absence d'outils pour cette mise en conformité.

Recommandation

Le COC recommande à la ZP Hainaut de prendre connaissance de l'avis d'office concernant le contenu de la fonction de délégué à la protection des données ou DPO[45], et de prévoir des formations pour les personnes clés en matière des protections des données.

4.2 Les banques de données particulières

23. A la date de 21-02-2020, la ZP Hainaut n'avait déclaré que 4 banques de données particulières dans REGPOL. La ZP a reconnu le 12-03-2020 l'existence de plusieurs autres banques de données particulières dont la mise en conformité est en cours. Une liste a été fournie au COC. Lors du contrôle du 21-01-2021, une partie de la liste a été examinée. Il s'avère que la zone de police est toujours en train d'identifier et de mettre en conformité les différents traitements en ce compris au niveau des banques de données particulières. Il s'avère également que la liste est nommée « GBO », mais qu'il s'agit en réalité d'une liste reprenant un ensemble de traitements de données à caractère personnel dont quelques-uns pourraient être considérés comme une banque de données particulière. La ZP Hainaut travaille sur plusieurs axes:

- L'identification des traitements, y compris les banques de données particulières;
- La déclaration de ces traitements dans le registre REGPOL;
- Afin de permettre un suivi des différentes étapes en interne, l'enregistrement de ces traitements dans un registre de traitements en RIO[46];

[45] Organe de contrôle de l'information policière, *Avis d'office concernant le contenu de la fonction de délégué à la protection des données ou DPO*, 14 avril 2020, DD200018 (consultable sur www.organedecontrole.be).
[46] **R**egistre **I**n **O**ut est une application/banque de données permettant l'enregistrement et la consultation des données relatives à la correspondance entrante (In), sortante (Out) et interne ainsi qu'aux suivis de son traitement au sein d'une unité.

- La cas échéant, évaluer si le traitement ne peut pas se faire dans un processus existant, la politique de la zone de police étant de limiter le nombre de GBO à ce qui est strictement nécessaire et de privilégier un traitement dans les banques de données de base (ISLP) et la BNG.

24. xxx

25. Avant de recourir à une banque de données concernant un traitement à risque, la zone de police n'avait pas encore réalisé d'AIPD (aussi DPIA[47]) au début de l'année 2020. Le 12-03-2020, de telles analyses étaient prévues mais pas encore réalisées. A la date de la visite le 21-01-2021, plusieurs AIPD avaient été soumises au COC et sont en cours de traitement au moment de la rédaction du présent rapport[48]. Certaines ont déjà fait l'objet d'une analyse *prima facie*[49] du COC et sont en cours d'adaptation par la DPO de la ZP Hainaut. Dans ce cadre, la ZP Hainaut a adressé un courrier à une centaine de fournisseurs afin de pouvoir conclure des accords de traitement. Pour l'instant, un seul fournisseur a réagi. La ZP Hainaut se montre favorable à un modèle d'AIPD propre à la GPI plutôt qu'à un modèle proposé par la CNIL[50] et souhaiterait également promouvoir une politique « uniformisée » et standardisée pour les outils communs GPI dans REGPOL (GALOP, RIO3, …).

26. Les principes d'accès aux GBO sont identifiés et les accès sont donnés de manière restreinte. Le login et le mot de passe individuels sont privilégiés mais pas systématisés dans toutes les GBO. Les données sont gardées essentiellement sur des serveurs internes mais pas de manière chiffrée. Des directives internes sont en cours d'élaboration.

27. Un bilan de sécurité pour le réseau internet a été effectué, en suite de quoi une demande d'analyse de vulnérabilité et de mise en sécurité par une société externe a été budgétée en 2020 (100.000 €) et sera exécutée par la firme xxx fin janvier 2021. Les droits d'accès des utilisateurs ne sont pas régulièrement analysés. Toutefois, une réflexion a été menée dans le courant de l'année 2020 concernant les droits d'accès de GALOP, ISLP ainsi que de la BNG et le suivi se fait dorénavant dans GALOP. Les systèmes de *badging* ont également été examinés et sont suivis maintenant via GALOP.

Recommandation

Le COC reconnaît que l'application REGPOL soit peu conviviale. Toutefois, étant donné que la ZP Hainaut choisit d'utiliser ce registre pour matérialiser l'obligation légale de tenir un registre des activités de traitement à côté d'un registre propre via l'application RIO3, le COC demande à la ZP Hainaut de bien veiller à ce que les deux registres soient synchronisés.

Le cas échéant, la ZP Hainaut pourrait transmettre ses remarques par rapport à l'utilisation du registre REGPOL à la police fédérale (CG/ISPO, éventuellement via la CPPL).

Demande

Le COC constate que l'application RIO est utilisée in concreto pour des finalités titre 1 (données administratives/non opérationnelles) et titre 2 (données opérationnelles) LPD au sein de la ZP Hainaut. Par finalité titre 2 LPD, le COC comprend d'une part, la saisie du document directement dans RIO, et d'autre part la vérification du suivi opérationnel du RIR par le membre du personnel de la ZP. Par finalité titre 1 LPD, le COC comprend la trace documentaire.

Le COC demande à la ZP Hainaut d'évaluer dans quelle mesure les traitements titre 2 LPD pourraient être retirés de cette application. Le COC pourrait accepter l'utilisation de RIO pour les finalités titre 1 et titre 2 LPD identifiées ci-dessus à condition :

1) *que la ZP Hainaut fournisse une analyse qui démontre qu'il n'est techniquement pas faisable et opérationnellement pas souhaitable de retirer les traitements titre 2 LPD de RIO ;*
2) *que la banque de données RIO soit identifiée comme une banque de données particulière, au vu des possibilités offertes par la LFP et la GPI ;*
3) *que les finalités d'utilisation titre 1 et titre 2 LPD soient déclarées en REGPOL ;*

[47] ***D****ata* ***P****rotection* ***I****mpact* ***A****ssessment.*

[48] Il s'agit des AIPD *Bodycam* (DI200005), Caméras fixes et fixes temporaires (amovibles) (DI210003) et Drônes (DI210004).

[49] La méthodologie consiste à analyser les AIPD soumises par les services de police sur base de quelques critères qui dépendent de l'objet de l'AIPD. Cette analyse *prima facie* du COC ne constitue donc pas un avis formel au sens de l'article 59 LPD.

[50] **C**ommission **N**ationale de l'**I**nformatique et des **L**ibertés (Autorité de protection des données de la France).

4) *de prendre les mesures techniques et organisationnelles nécessaires afin que les traitements titre 2 se limitent à ce qui est pertinent, adéquat et non-excessif ;*
5) *qu'une politique d'accès, de journalisation et de conservation des données soit établie.*

Demande

Le COC demande à la ZP Hainaut de continuer à inventorier les traitements effectués au sein de la zone en donnant une priorité aux banques de données particulières, en identifiant la finalité, les circonstances exceptionnelles, les besoins opérationnels spécifiques et le domaine visé. Dans ce cadre, il faut enregistrer l'utilisation de l'outil XRY téléphonie comme une banque de données particulière.

Demande

Le COC demande à la ZP Hainaut d'évaluer en même temps si les traitements effectués dans une banque de données particulière ne peuvent pas se faire dans une banque de données de base ou dans la BNG.

Demande

Le COC reconnait les efforts déjà réalisés au niveau de la rédaction des AIPD et demande à la ZP Hainaut de continuer dans la même direction en tenant compte des remarques prima facie du COC.

4.3 Logging

28. Avant la visite de la ZP *Hainaut*, une analyse du logging ou de la journalisation des applications 'BNG Consultation' (PLC), 'BNG Contrôle' (PCT), 'BNG Circulation' (TEC), 'BNG Police Administrative' (BPC) et 'Registre National' (RRN), y compris le nombre ainsi que la nature du motif de consultation (MOT) pour une période de 5 jours (entre le 06-01-2020 et le 10-01-2020 compris) a été effectuée.

29. Au début de l'année 2020, il n'y avait pas encore de directive interne relative à la motivation d'une consultation des banques de données. Toutefois, il est régulièrement rappelé au membres du personnel de motiver leurs consultations.

30. Depuis 2017, la ZP Hainaut dispose d'un plan d'action en matière de consultations illégitimes des banques de données[51]. Des rappels aux membres du personnel ainsi que des contrôles ont été effectués.

31. Des contrôles de l'utilisation d'ISLP sur base de la journalisation sont effectués régulièrement.

Lorsqu'il s'agit d'une consultation à des fins personnelles ou lorsque le résultat de la consultation a été communiqué à une tierce personne, un PV est systématiquement rédigé.

La gestion reste interne lorsqu'il n'y a pas d'implication d'une tierce personne à savoir par exemple lorsqu'un policier fait des recherches sur des noms inexistants comme «*Mickey Mouse*» ou «*Marilyn Monroe*», ou quand un policier se consulte lui-même. Pour le reste, d'après la ZP, dès qu'il y a «*un élément moral*» un PV est systématiquement rédigé. Depuis 3 ans, sur 14 consultations illégitimes constatées, 9 PV ont été rédigés. Les 5 autres cas n'avaient pas d'élément moral ou d'implication d'une personne extérieure.

En ce qui concerne la consultation par un membre de la GPI de ses propres données dans les bases de données policières la non rédaction d'un PV n'est pas acceptable. En effet, le COC souligne que les motifs intrinsèques d'une consultation illégitime (et donc d'un traitement illégal) ne sont pertinents pour juger de l'opportunité de dresser un PV. Même les consultations par 'simple curiosité' ou des consultation sur soi-même comme soi-disant 'test' p.ex. constituent des infractions pénales et il n'appartient pas à la zone de police de faire un classement sans suite policière ou de faire une évaluation sur le vrai motif de la consultation. Certes, les motifs peuvent jouer un rôle sur la décision du MP (ou du juge pénal), de commencer une enquête disciplinaire ou encore être déterminants pour choisir la sanction disciplinaire appropriée (avertissement seulement p.ex. pour de tels comportements), mais il est clair qu'au moins un PV doit être dressé.

[51] Voir les références internes à la ZP: OGC 3/2017 + RIO 2019/7261 + 2019/532.

Recommandation

Globalement, l'analyse effectuée par le COC en combinaison avec les explications fournies par la ZP Hainaut ne montrent pas une situation inquiétante. Il est évident que des actions de sensibilisation et de contrôle en la matière resteront un point d'attention permanent et qu'une attention particulière doit être accordée à la clarté du motif de consultation utilisé. Le COC suggère que le motif soit complété par le numéro du procès-verbal, le numéro de la fiche information ou intervention, le numéro du rapport d'information ou éventuellement d'autres détails permettant une traçabilité aisée en cas de vérification. Cette manière d'agir permet en cas de contrôle de vérifier que l'entité consultée en banque de données correspond à celle présente dans le dossier indiqué en référence.

Recommandation

Le COC recommande à la ZP Hainaut de continuer à procéder à des contrôles systématiques et proactifs de l'utilisation et/ou de la consultation des banques de données policières accessibles aux services de police, notamment en effectuant des contrôles mensuels ou trimestriels des motifs de consultation. Le COC incitera les responsables de la GPI à faciliter ces contrôles en fournissant des outils appropriés. La COC demande que les résultats des contrôles soient mis à sa disposition. Afin de rendre les contrôles utiles, il faut que la ZP Hainaut prenne contact avec la DRI afin de régulariser l'attribution des stations de travail par sous-unité.

Demande

Le COC demande qu'un PV soit rédigé pour chaque consultation ou traitement illégitime d'une banque de données policière ou d'une banque de données à disposition du membre de la zone de police. Il est nécessaire de notifier à l'avance les membres du personnel de cette politique en matière de consultations ou traitements illégitimes p.ex. dans une note de service.

Mesures correctrice

Le COC avertit la ZP Hainaut que la pratique qui consiste de ne pas dresser un PV dans certain cas, c-à-d lorsque le membre du personnel se consulte lui-même après une analyse par la hiérarchie de 'l'élément moral' de l'infraction pénale, est susceptible de violer la règlementation aux traitements des données à caractère personnel, l'article 15, 1° LFP et les règles du Code d'Instruction Criminelle.

4.4 Fonctionnement et alimentation de la BNG

32. Le questionnaire BNG tel qu'utilisé par le COC permet d'avoir une idée de la manière dont la zone de police en question traite un certain nombre d'aspects de la BNG. Les questions spécifiques permettent d'obtenir une image du fonctionnement interne, de l'utilisation des profils, du déroulement des évaluations et de l'utilisation tactique de la BNG.

33. xxx

34. Au sein de la ZP Hainaut, il n'y a pas de politique proactive en matière d'effacement ou d'archivage des données de la BNG. Les standards de la GPI sont appliqués à savoir que les PV de désignalement qui sont communiqués à la zone de police et qui sont en liaison avec un traitement pour lequel la zone de police est l'unité responsable sont traités par le CIL et se traduisent par la ventilation du signalement (donc de la mesure) en question. D'autres applications gérées au niveau de la province du Hainaut permettent le suivi des mesures à prendre relatives aux auditions et permettent donc également un contrôle sur les mesures à prendre dans ce cadre.

35. Au niveau des RIR, le suivi administratif des envois et des réceptions se matérialise via l'application du suivi administratif des communications RIO. Cette procédure de travail implique que des informations opérationnelles soient traitées dans une banque de données dont la finalité n'est pas prévue pour gérer les informations policières opérationnelles. Le ZP Hainaut réalise le problème que cela pose au niveau de la ventilation et a demandé à DRI de prévoir une solution au niveau de la ventilation des RIR. En outre, des problèmes ne sont pas à exclure au niveau de la consultation des informations opérationnelles par des membres du personnel qui n'ont pas un rôle à jouer dans la gestion de l'information policière opérationnelle.

36. xxx

37. Actuellement, la ZP Hainaut n'a aucune idée du nombre d'entités en BNG telles que des faits concrets ou faits non-concrets, des enquêtes et des personnes dont la zone de police est l'unité responsable. Par conséquent, la ZP Hainaut n'a pas non plus idée du nombre d'erreurs potentielles par entité identifiée en BNG. Cela se traduit, entre autres, par le fait qu'il n'y a actuellement aucun aperçu du nombre de mesures à prendre, de sorte qu'un contrôle de qualité sur des questions telles que la date de fin ou la pertinence de la mesure n'est pas possible. Outre les aspects liés à la protection des données (exactitude des informations et des données personnelles) et à l'impact sur les droits fondamentaux des citoyens, cela a également des implications possibles sur la mise en œuvre correcte des mesures à prendre, que ce soit ou non sous la forme de corrélations à travers le fonctionnement du système *ANPR*[52]. Dans ce cas, un tableau centralisé contenant ces données par paramètre ainsi que les clés techniques serait très utile.

38. La ZP Hainaut utilise à la fois un PV portant le code de prévention 45 et le RIR pour divulguer les faits non concrets. Bien que cela se produise souvent à la demande du procureur, cela a des effets négatifs dans le domaine de la protection des données car (1) des informations essentiellement non concrètes sont saisies dans l'environnement destiné aux informations concrètes et deviennent donc accessibles aux membres du personnel ayant un profil d'accès différent et (2) des délais de conservation différents s'appliquent selon la nature concrète ou non d'une information.

39. xxx

40. xxx

4.5 Triptyque

41. Une liste des arrestations judiciaires de la ZP Hainaut a été demandée avant la visite. Au total, 298 entités ont été impliquées. De cette liste, 20 entités ont été contrôlées en BNG par le COC en vue d'évaluer les éléments du triptyque judiciaire (prise d'empreintes, description physique et photo).

42. Les locaux dans lesquels les personnes arrêtées sont accueillies et où entre autres le triptyque judiciaire est exécuté ont été visités par le COC. Dans la même infrastructure, des locaux sont prévus pour les entretiens confidentiels entre les avocats et les personnes impliquées. Le bâtiment date d'une époque où l'exercice des droits fondamentaux se faisait d'une manière différente de celle d'aujourd'hui. Il est clair que la ZP Hainaut a fait un effort en tenant compte des circonstances pour que les processus qui sont propres à l'accueil des personnes arrêtées soient exécutés en tenant compte de la dignité humaine. Toutefois, les locaux disponibles pour les entretiens confidentiels n'offrent pas beaucoup de discrétion. Le local dispose en effet de grandes fenêtres qui exposent ses occupants à la vue des passants occasionnels même si ce passage est normalement uniquement emprunté par du personnel policier. Il n'y a pas non plus un flux fluide entre l'entrée du bâtiment, le local du triptyque, les cellules et les locaux d'audition[53].

xxx

43. Sur les 20 dossiers examinés, 13 ont fait l'objet de remarques de la part du COC car le triptyque était incomplet.

xxx

44. L'exécution du triptyque judiciaire présente des avantages pour l'organisation de la GPI. En l'absence des outils permettant de vérifier systématiquement la qualité de la BNG *sensu lato*, chaque triptyque est l'occasion de vérifier l'état d'une personne dans la BNG au regard de la photo, de la description individuelle et des empreintes digitales. Le triptyque permet de vérifier si la personne a déjà fait l'objet d'un triptyque, de déterminer si cette personne a déjà été enregistrée dans la BNG et donc d'identifier ses antécédents mais aussi de décider (aussi selon le retour du SIJ[54]) de procéder ou non aux premières opérations / mesures dans le cadre de l'infraction pour laquelle le triptyque a été réalisé. Le cas échéant, une fusion des entités en BNG est toujours possible.

Recommandation

[52] ***A**utomatic **N**umber **P**late **R**ecognition (en français souvent LAPI pour **L**ecture **A**utomatique des **P**laques d'**I**mmatriculation en abrégé).*
[53] Nous précisons que des travaux ont débuté le 1er mars 2021 à l'Accueil et que ces aménagements étaient déjà prévus avant la visite du COC mais qu'ils n'ont débuté que ce 1er mars.
[54] **S**ervice d'**I**dentification **J**udiciaire.

Le COC recommande à la ZP Hainaut de profiter de l'exécution du triptyque judiciaire pour vérifier la qualité de l'enregistrement en BNG de la personne faisant l'objet du triptyque au regard de la description individuelle, de la photo et des empreintes digitales, et de procéder à la fusion de l'entité s'il s'avère que cette personne a été enregistrée plus d'une fois en BNG.

Demande

Le COC demande à la ZP Hainaut de veiller, lors des processus d'étude pour des nouveaux bâtiments ou des rénovations dans le futur, à ce que l'architecture tienne compte des adaptations nécessaires pour que les processus d'accueil des personnes arrêtées puissent avoir lieu dans les meilleures circonstances possibles.

Demande

Le COC demande à la ZP Hainaut d'étudier la possibilité d'avoir une connexion avec les banques de données policières dans le local du triptyque afin de faciliter des vérifications sur place et pour le confort du personnel.

5 CONCLUSIONS – RECOMMANDATIONS, DEMANDES ET MESURES CORRECTRICES

45. La ZP Hainaut a collaboré de manière transparente et constructive avec le COC entre le moment de l'annonce du contrôle technique début de l'année 2020 et la visite en janvier 2021. Le fait que la visite même ait été postposée à plusieurs reprises suite à la crise sanitaire due au COVID 19 n'a pas empêché la zone de police de déjà entrer en communication avec le COC, de lui faire part de ses difficultés via les questions posées et les réponses fournies, et de commencer un processus d'amélioration des problèmes rencontrés.

46. L'effort fourni au niveau des AIPD a donné lieu à la rédaction de 4 AIPD actuellement en cours d'analyses par le COC. Les modifications sont en cours de traitement par la DPO de la ZP Hainaut au moment de la rédaction du présent rapport.

47. Les trois axes de travail au niveau des GBO doivent, à terme, réduire le nombre des banques de données particulières et mettre en ordre celles qui continueront à exister momentanément.

48. L'analyse des journalisations au niveau de la BNG ne démontre pas un grand problème pour l'instant. Toutefois, il est évident que des contrôles par rapport à l'utilisation correcte des banques de données policières et accessibles aux services de police resteront un point d'attention permanent.

49. L'alimentation, l'utilisation et le fonctionnement de la BNG sont acceptables en tenant compte des possibilités techniques et des outils mis à la disposition par la police fédérale.

POUR CES RAISONS,

L'Organe de contrôle,

émet les <u>recommandations</u> suivantes :

1. <u>Recommandation</u>

le COC recommande à la ZP Hainaut de prendre connaissance de l'avis d'office du COC concernant le contenu de la fonction de délégué à la protection des données ou DPO et de prévoir des formations pour les personnes clés en matière de protection des données ;

2. <u>Recommandation</u>

Étant donné que la ZP Hainaut choisit d'utiliser le REGPOL pour matérialiser l'obligation légale de tenir un registre des activités de traitement à côté d'un registre propre via l'application RIO3, le COC demande à la ZP Hainaut de bien veiller à ce que les deux registres soient synchronisés.

Le cas échéant, la ZP Hainaut pourrait transmettre ses remarques par rapport à l'utilisation du registre REGPOL à la police fédérale (CG/ISPO, éventuellement via la CPPL) ;

3. <u>Recommandation</u>

l'analyse effectuée par le COC en combinaison avec les explications fournies par la ZP Hainaut ne montre certainement pas une situation inquiétante par rapport aux analyses relatives aux journalisations de la BNG. Il est évident que des actions de sensibilisation et de contrôle en la matière resteront un point d'attention permanent et qu'une attention particulière doit être accordée à la clarté du motif de consultation utilisé. Le COC suggère que le motif soit complété par le numéro du procès-verbal, le numéro de la fiche information ou intervention, le numéro du rapport d'information, ou éventuellement d'autres détails permettant une traçabilité aisée en cas de vérification. Cette manière d'agir permet en cas de contrôle de vérifier que l'entité consultée en banque de données correspond à celle présente dans le dossier indiqué en référence ;

4. Recommandation

le COC recommande à la ZP Hainaut de continuer à procéder à des contrôles systématiques et proactifs de l'utilisation et/ou de la consultation des banques de données utilisées par les services de police, notamment en effectuant des contrôles mensuels ou trimestriels des motifs de consultation. Le COC incitera les responsables de la GPI à faciliter ces contrôles en fournissant des outils appropriés. La COC demande que les résultats des contrôles soient mis à sa disposition. Afin de rendre les résultats utiles, il faut que la ZP Hainaut prenne contact avec DRI afin de régulariser l'attribution des stations de travail par sous-unité.

5. Recommandation

le COC recommande à la ZP Hainaut de profiter de l'exécution du triptyque judiciaire pour vérifier la qualité de l'enregistrement en BNG de la personne faisant l'objet du triptyque, au regard de la description individuelle, de la photo et des empreintes digitales, et de procéder à la fusion de l'entité s'il s'avère que cette personne a été enregistrée plus d'une fois en BNG.

demande à la ZP Hainaut :

1. Demande

Le COC constate que l'application RIO est utilisée *in concreto* pour des finalités titre 1 (données administratives/non opérationnelles) et titre 2 (données opérationnelles) LPD au sein de la ZP Hainaut. Par finalité titre 2 LPD, le COC comprend d'une part, la saisie du document directement dans RIO, et d'autre part la vérification du suivi opérationnel du RIR par le membre du personnel de la ZP. Par finalité titre 1 LPD, le COC comprend la trace documentaire.

Le COC demande à la ZP Hainaut d'évaluer dans quelle mesure les traitements titre 2 LPD pourraient être retirés de cette application. Le COC pourrait accepter l'utilisation de RIO pour les finalités titre 1 et titre 2 LPD identifiées ci-dessus à condition:

- que la ZP Hainaut fournisse une analyse qui démontre qu'il n'est techniquement pas faisable et opérationnellement pas souhaitable de retirer les traitements titre 2 LPD de RIO ;
- que la banque de données RIO soit identifiée comme une banque de données particulière, au vu des possibilités offertes par la LFP et la GPI ;
- que les finalités d'utilisation titre 1 et titre 2 LPD soient déclarées en REGPOL ;
- de prendre les mesures techniques et organisationnelles nécessaires afin que les traitements titre 2 se limitent à ce qui est pertinent, adéquat et non-excessif ;
- qu'une politique d'accès, de journalisation et de conservation des données soit établie.

2. Demande

le COC demande à la ZP Hainaut de continuer à inventorier les traitements effectués au sein de la zone, avec une priorité aux banques de données particulières, en identifiant la finalité, les circonstances exceptionnelles, les besoins opérationnels spécifiques et le domaine visé ;

3. Demande

le COC demande à la ZP Hainaut d'évaluer en même temps si les traitements effectués dans une banque de données particulière ne peuvent pas se faire dans une banque de données de base ou dans la BNG ;

4. Demande

le COC reconnait les efforts déjà faits au niveau de la rédaction des AIPD et demande à la ZP Hainaut de continuer cet effort, en tenant compte des remarques *prima facie* du COC ;

5. Demande

Le COC demande qu'un PV soit rédigé pour chaque consultation ou traitement illégitime d'une banque de données policière ou d'une banque de données à disposition du membre de la zone de police. Il est nécessaire de notifier à l'avance les membres du personnel de cette politique en matière de consultations ou traitements illégitimes p.ex. dans une note de service.

6. Demande

le COC demande à la ZP Hainaut de veiller, lors des processus d'étude pour des nouveaux bâtiments ou des rénovations dans le futur, à ce que l'architecture tienne compte des adaptations nécessaires pour que les processus d'accueil des personnes arrêtées puissent avoir lieu dans les meilleures circonstances possibles ;

7. Demande

le COC demande à la ZP Hainaut d'étudier la possibilité d'avoir une connexion avec les banques de données policières dans le local du triptyque afin de faciliter les vérifications sur place.

Prends la mesure correctrice suivante envers la ZP Hainaut,

Vu les articles 221 § 1 en 247, 2° LPD,

Mesure correctrice

Le COC **avertit** la ZP Hainaut que la pratique qui consiste de ne pas dresser un PV dans certain cas, c-à-d lorsque le membre du personnel se consulte lui-même après une analyse par la hiérarchie de 'l'élément moral' de l'infraction pénale, est susceptible de violer la règlementation aux traitements des données à caractère personnel, l'article 15, 1° LFP et les règles du Code d'Instruction Criminelle.

demande à la ZP Hainaut un état de la situation par rapport aux recommandations et aux demandes dans les 12 mois après la date de la transmission du présent rapport ;

Dit pour droit que la date d'entrée en vigueur de la mesure correctrice et la date de prise de connaissance des recommandations et demandes doivent être comprises comme étant la date de la transmission du présent rapport (par e-mail) de l'Organe de contrôle augmentée de deux jours.

Ainsi décidé par l'Organe de contrôle de l'information policière le 24 juin 2021

Koen Gorissen	Frank Schuermans	Philippe Arnould
Membre-Conseiller	Membre-Conseiller	Président
SIGNÉ	SIGNÉ	SIGNÉ

Copie:

- Bourgmestre de xxx

- Procureur du Roi xxx

*

* *