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 : CON20008

VERSION PUBLIQUE[1]

1. INTRODUCTION

Vu ses compétences en tant que service de contrôle externe et autorité de surveillance compétente à l'égard des traitements de données effectués par la police intégrée structurée à deux niveaux (GPI), l'Organe de contrôle de l'information policière ('Organe de contrôle' ou 'COC') a décidé d'effectuer une visite auprès d'une zone de police de la province de Flandre occidentale (ci-après dénommée 'ZP FLOcc'). Le présent rapport présente les conclusions de l'enquête réalisée à l'occasion de cette visite.

1.1. 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)[2] a réformé l'Organe de contrôle de l'information policière en une autorité de surveillance 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 §1er et les chapitres II et III du titre 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 44/11/13 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'à côté de la protection de la vie privée et des données, le COC prête également attention à des éléments comme l'efficacité de la gestion de l'information et de l'intervention policière.

L'Organe de contrôle est compétent pour les services de police[3], pour l'inspection générale de la police fédérale et de la police locale (AIG)[4] et pour l'unité d'information des passagers (UIP)[5]. 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[6].

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.

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, 3e alinéa de la LFP, qui oblige tous les membres des services de police à alimenter cette banque de données.

---

[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] MB, 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 dénommée « RGPD » 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 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*).

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

[4] 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°, d de la LPD).

[5] Telle que visée au chapitre 7 de la loi du 25 décembre 2016 relative au traitement des données des passagers (art. 26, 7°, f de la LPD). *BELPIU* est l'acronyme de la dénomination anglaise *Belgian Passenger Information Unit*.

[6] Art. 4 §2, 4ième alinéa de la loi du 3 décembre 2017 portant création de l'Autorité de protection des données (LAPD).

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 44/11/13 de la LFP et à leurs mesures d'exécution.

Dans le cadre de l'utilisation de caméras non visibles, l'Organe de contrôle fonctionne en quelque sorte comme une commission « MAP »[7]. Conformément à l'article 46/6 de 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[8]. Les membres de l'Organe de contrôle et les membres du service d'enquête disposent à cet égard de compétences d'investigation et peuvent prendre des mesures correctrices[9].

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[10].

2. OBJET DE LA VISITE ET MÉTHODOLOGIE

Le 26 octobre 2020, l'Organe de contrôle a effectué de sa propre initiative ce que l'on appelle une visite technique restreinte[11] auprès de la ZP FLOcc. La visite ne faisait donc pas suite à une plainte (individuelle) ni ne découlait de l'existence d'indications (concrètes) d'un non-respect, par la zone de police visitée, de la législation et de la réglementation.

Vu l'ampleur et la nature des données et la forme des traitements dans le cadre de la création de banques de données particulières, des arrestations judiciaires par la police et de l'établissement du 'triptyque', de tels traitements de données impliquent une ingérence profonde dans la vie privée. Pour garantir une collecte correcte des informations, ces traitements sont régis par des conditions d'exécution qui sont décrites dans la législation (principalement dans la LFP), dans des arrêtés d'exécution et dans des directives (principalement la MFO-3). Le COC contrôle par conséquent si les banques de données particulières ont été créées selon les règles applicables et si les arrestations judiciaires et l'établissement du triptyque sont bien réalisés conformément à la réglementation applicable et aux exigences en termes de qualité.

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, cette visite se limite aux thèmes spécifiques suivants :

- banques de données particulières ;
- 'triptyque'[12] – arrestations judiciaires ;
- contrôle des journalisations de la BNG et du motif de la consultation ;
- situation/points d'attention concernant la 'validation centrale/option 35'.

La visite se décline en deux phases.

[7] MAP signifie « méthodes administratives particulières ».
[8] Art. 240, 4° de la LPD.
[9] Art. 244 et 247 de la LPD.
[10] Art. 248 de la LPD.
[11] Une visite technique est une enquête technique portant essentiellement sur les aspects policiers opérationnels et se consacrant à un ou plusieurs sujets spécifiques, par exemple 'le contrôle du triptyque', 'l'alimentation de la BNG' ou encore 'l'accès/la journalisation illicite' (voir aussi les articles 236 §3 et 239 de la LPD). Ces visites sont moins spécifiquement axées sur les aspects juridiques ou sur les aspects de la protection des données ou de la vie privée, bien que ceux-ci soient pris en compte également.
[12] 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).

Dans une première phase, les informations et documents nécessaires ont été demandés à la ZP FLOcc. 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.

La seconde phase consistait en la visite sur place (la visite proprement dite), qui se composait de plusieurs parties :

1) une introduction du COC et des membres présents de la ZP FLOcc;
2) une discussion au sujet des documents qui nous avaient été envoyés concernant les banques de données particulières de la ZP FLOcc;
3) une visite de la 'station FIT'[13];
4) une visite de la gestion opérationnelle;
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 §1er de la LFP prévoit 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;

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 LPD, les services de police devront solliciter au préalable l'avis du COC lorsque :

- le 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 (article 58);
- l'analyse d'impact relative à la protection des données (AIPD)[14]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 §1er 1° et 2°).

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.

[13] 'FIT' étant l'acronyme de ***F**ingerprint **I**mage **T**ransmission.*
[14] 'AIPD' étant l'acronyme de **A**nalyse d'**I**mpact relative à la **P**rotection des **D**onnées.

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.

3.4. Journalisation de la BNG

La police est tenue de conserver des fichiers de journalisation[15]. 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[16]. 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 conséquents essentiels pour le contrôle tant proactif que réactif, et ce tant au niveau interne qu'externe.

4. CONCLUSIONS DE L'ENQUÊTE

4.1. Banques de données particulières

Préalablement à la visite, l'Organe de contrôle a reçu un document de politique consacré à la création et à l'utilisation des banques de données particulières. Le COC a constaté que la ZP FLOcc n'avait élaboré ce document qu'après l'annonce de la visite projetée par le COC. À la lecture de ce document, il apparaît que son contenu satisfait à ce que la LFP stipule comme cadre légal, et constitue un point de départ pour la mise en œuvre d'un plan d'action visant à évaluer et à implémenter les banques de données particulières. **Ce document de politique peut dès lors 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.**

Les banques de données particulières reprises en annexe du document de politique susmentionné ont selon la zone de police été mises en service il y a déjà 10 à 15 ans. Par conséquent, il va falloir passer en revue toutes ces banques de données particulières selon le plan par étapes prévu dans le document afin de vérifier si elles satisfont ou non aux dispositions légales. Cet exercice sera selon la ZP FLOcc réalisé par la cellule de sécurité de l'information (CSI), qui se compose de personnes clés de la zone de police disposant des compétences requises. Après la première évaluation, les banques de données particulières retenues ainsi que les nouvelles banques de données particulières qui seront créées par la suite seront soumises à une évaluation trimestrielle réalisée par la CSI.

Il ressort par ailleurs du document de politique que si une banque de données particulière est retenue, elle sera enregistrée dans le REGPOL[17]par le délégué à la protection des données. Le fait qu'aucun arrêté d'exécution n'ait encore été publié pour rendre obligatoire l'enregistrement des données dans le REGPOL ne dispense en effet pas la zone de police de l'obligation de tenir à jour les banques de données dans un propre registre des traitements. **La zone de police a de toute façon indiqué avoir l'intention de déclarer les banques de données dans le REGPOL; il est aussi apparu qu'elle ne disposait pas d'un registre propre.** Par conséquent, aucune banque de données particulière n'avait encore été enregistrée en date du 22/10/20, ni n'avait dans le passé été déclarée auprès du COC alors que l'ancien article 44/11/3 §3 imposait déjà cette obligation[18].

[15] Article 56 § 1 LPD, en exécution de l'article 25 de la directive police & justice.
[16] Article 56 § 2 LPD.
[17] REGPOL est le registre national des activités de traitement de données à caractère personnel tel que visé à l'article 145, 2e alinéa de la loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux (le support technique de ce registre est assuré par la police fédérale).
[18] Tel qu'il s'appliquait jusqu'au 29 juin 2019, date de l'entrée en vigueur de la loi du 22 mai 2019 modifiant diverses dispositions en ce qui concerne la gestion de l'information policière qui a abrogé cette déclaration en modifiant notamment ce paragraphe 3 (cf. article 14).

Bien qu'il faille encore procéder à l'évaluation des banques de données particulières déjà utilisées au sein du corps, la direction du corps est consciente que la zone de police ne satisfait pas aux règles en matière d'actualisation des données, de conservation et de suppression des données, etc.

Tout comme le COC, la zone de police est favorable à l'idée, dans le cadre d'un bon échange des données, d'alimenter le plus possible les banques de données de base et de ne recourir à une banque de données particulière que dans le respect des critères définis dans la loi.

Sur la base des informations communiquées lors de la visite, le COC en arrive aux conclusions suivantes en ce qui concerne les banques de données particulières énumérées :

- il n'y a qu'un seul gestionnaire d'applications chargé de la création des banques de données particulières;
- la zone de police n'a pas été en mesure de présenter pour les banques de données existantes d'organigrammes reflétant les *workflows* au sein des banques de données particulières. Les analyses fonctionnelles sont réalisées *on the spot* en concertation avec celui qui a besoin ou prétend avoir besoin d'une banque de données particulière, mais elles ne sont documentées nulle part. Or, de tels organigrammes permettent de déterminer s'il ne serait pas préférable d'enregistrer les données contenues dans une banque de données particulière dans par exemple une banque de données de base;
- **il n'est prévu pour aucune des banques de données de délais en vue de l'évaluation des données conservées ;**
- **les banques de données peuvent être consultées sans qu'il ne faille mentionner le motif de la consultation.**

Or, la planification d'évaluations régulières constitue une bonne pratique, et l'obligation de mentionner le motif de la consultation est prévue par les articles 56 §1er, 2 et 3 de la LPD *juncto* l'article 44/11/3 §4 de la LFP.

La ZP FLOcc indique dans le document de politique qu'il convient de prévoir une journalisation des traitements pour chaque banque de données particulière. Le corps prévoira également des profils spécifiques qui pourront utiliser les fichiers de journalisation, de manière à tenir compte de l'importance de tirer des conclusions adéquates des résultats de la journalisation. La zone de police précise que des données de journalisation sont disponibles pour les banques de données particulières concernées ou peuvent être mises à disposition à la demande du COC. À l'heure actuelle, ces données de journalisation sont uniquement accessibles à certains profils spécifiques au sein de la zone de police.

4.2. Triptyque

En prévision de la visite, une liste des arrestations judiciaires de la ZP FLOcc avait été demandée au préalable. Dans cette liste, cinq arrestations judiciaires ont été arbitrairement sélectionnées afin de vérifier si le triptyque avait été établi conformément aux directives et aux exigences en termes de qualité.

En outre, l'encodage des données requises dans ISLP a également été contrôlé afin de vérifier si le flux entre ISLP[19]et la BNG[20]s'était déroulé correctement et si les personnes avaient été encodées correctement.

Ce contrôle par échantillonnage restreint a révélé que le triptyque n'est pas systématiquement établi au sein de la zone de police. Alors que les directives ne laissent planer aucun doute sur l'obligation d'établir un triptyque pour chaque arrestation judiciaire, il s'est avéré **dans quatre cas sur les cinq 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[21] 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 fait absolument partie.

En ce qui concerne l'enregistrement dans ISLP des personnes physiques faisant l'objet d'une arrestation judiciaire, le COC constate que l'on retrouve dans quatre cas sur les cinq une base correcte d'enregistrement. Selon la zone de police,

[19] Banque de données de base telle que visée à l'article 44/11/2 de la LFP.
[20] Banque de données Nationale Générale telle que visée à l'article 44/7 de la LFP.
[21] Numéro identique dans ISLP qui fait référence aux empreintes digitales relevées.

le fait qu'un intéressé ne puisse pas être retrouvé dans le système ISLP de la ZP FLOcc est dû au fait que le suspect a été privé de sa liberté par une autre zone ou un autre service.

La zone de police avait dans l'intervalle réalisé le même exercice pour une liste de 50 personnes privées de leur liberté par la zone de police. Il en est ressorti que **dans la moitié des cas, le triptyque n'avait pas été établi ou n'était pas complet**. **Le COC ne peut donc que constater, comme indiqué plus haut, que la tâche légale prévoyant l'établissement du triptyque n'a pas été réalisée conformément aux directives en vigueur, ou du moins pas correctement**, ce qui compromet la transmission des données à la Banque de données Nationale Générale (BNG) et donc aussi l'efficacité du traitement des données par et pour la police intégrée dans son ensemble.

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

L'élément suivant examiné dans le cadre de ce contrôle technique est la journalisation des consultations de la BNG réalisées par la ZP FLOcc, qui doit également permettre de vérifier quel était le motif de la consultation. Les collaborateurs de la police peuvent consulter de plusieurs manières des informations opérationnelles de la BNG pour s'acquitter efficacement de leurs tâches.

La police est tenue de conserver des fichiers de journalisation[22]. 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[23].

La zone de police elle-même n'avait encore jamais consulté de journalisations jusqu'à la date de la visite. **Elle ne réalisait pas non plus de contrôles proactifs en vue de détecter d'éventuelles consultations illicites.**

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.

4.4. Validation centrale

Un dernier aspect qui a été examiné avait trait à la réalisation de ce que l'on appelle une 'validation centrale'[24]au sein de la zone de police.

Selon la zone de police, cette validation centrale est réalisée chaque jour.

4.5. Constatations additionnelles

En dépit du fait qu'il s'agissait d'une visite technique restreinte, nous avons par ailleurs constaté durant notre visite du siège central de la zone de police quelques éléments qui nécessitent un suivi et qui pourraient potentiellement faire l'objet d'une enquête et/ou d'un suivi complémentaire.

4.5.1. Traitement de données biométriques à des fins non opérationnelles

Le COC a constaté à certains accès la présence d'appareils d'enregistrement recourant à la biométrie (empreintes digitales) qui sont utilisés pour gérer l'accès aux locaux et/ou pour enregistrer le temps de travail.

Interrogée à ce sujet, la zone de police a déclaré recourir à des données biométriques pour l'accès à certains locaux. Les données biométriques ne sont pas utilisées à des fins d'enregistrement du temps de travail. Le COC a exposé les raisons pour lesquelles il estime que l'utilisation de données biométriques n'est pas admissible. L'enregistrement de l'utilisateur dans le système sous-entend la collecte des caractéristiques biométriques pertinentes de la personne concernée, lesquelles sont liées aux données conservées auprès du service du personnel. Le principal motif de l'introduction d'un système de contrôle est à mettre en relation avec l'aspect de l'authentification, à savoir la possibilité

[22] Article 56 §1er de la LPD mettant en œuvre l'article 25 de la Directive Police & Justice.
[23] Article 56 §2 de la LPD.
[24] 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 prouver que la personne qui veut accéder au local est bien la personne identifiée comme telle. Une alternative consiste à recourir à un badge personnel.

Ce code unique contient alors la représentation numérique des empreintes digitales, qui sont incontestablement liées aux données biométriques de l'intéressé. Le fait que l'empreinte digitale soit conservée non chiffrée ou sous la forme d'un '*template*' ou 'gabarit' (ce code unique) ne fait aucune différence: il s'agit toujours de données biométriques.

Le COC insiste sur le fait qu'il n'existe aucune base légale justifiant de recourir à la biométrie pour la gestion des accès et/ou l'enregistrement du temps de travail (ni pour quelque autre application relevant du RGPD). **Ni le consentement de la personne concernée ni des motifs d'intérêt public important ne peuvent entrer en ligne de compte.**

4.5.2. Utilisation de caméras

Il a en outre été constaté que dans le local du dispatching de la zone de police se trouvait un grand écran mural prouvant que la zone de police dispose d'un réseau étendu de caméras.

En vertu de la loi du 21 mars 2018[25], le recours à la surveillance par caméra par les services de police est régi depuis le 25 mai 2018 par la LFP. La loi du 21 mars 2018 prévoit toutefois un régime transitoire de 12 mois afin de laisser aux services de police le temps de se conformer aux modifications de la législation. Lorsque la police recourt à la surveillance par caméra, ce sont donc les dispositions de la LFP qui s'appliquent, sauf lorsque l'utilisation des caméras est régie par une autre législation. Avant de pouvoir introduire la surveillance par caméra sur le territoire d'une commune, un service de police a besoin de l'accord de principe du Conseil communal[26]. Aucune autorisation n'est par contre requise pour l'utilisation de caméras dans des lieux fermés dont la police est elle-même le gestionnaire, comme un commissariat de police[27]. Il est important de souligner que si l'autorisation du Conseil communal avait déjà été obtenue en application de la loi relative à la surveillance par caméra (l'ancienne) avant la modification légale du 21 mars 2018, elle ne doit pas être obtenue à nouveau[28]. Ce consentement reste donc valable. En revanche, ce même consentement ne peut pas être utilisé pour l'utilisation de nouveaux types de caméras introduits par la loi du 21 mars 2018. La LFP impose notamment des conditions spécifiques pour l'utilisation de caméras fixes mobiles, qui requiert une décision du Conseil communal[29]. Dans ce cas, une nouvelle autorisation ou une autorisation complémentaire du Conseil communal doit donc être obtenue.

Le COC a constaté que la ZP FLOcc n'était pas en mesure de présenter d'autorisation du Conseil communal pour l'utilisation des caméras. En conséquence, l'utilisation des caméras ne satisfait actuellement pas à toutes les conditions légales. Dans sa réponse au projet de rapport, la P ZP FLOcc a fait savoir que *« le nécessaire a été fait début novembre pour obtenir cette autorisation des Conseils communaux. Le sujet a été abordé par le Collège de police à la mi-octobre. Dans l'intervalle, 3 consentements ont déjà été reçus, et le point figure à l'ordre du jour de la prochaine assemblée des Conseils communaux des villes et communes dont nous n'avons pas encore obtenu l'autorisation* (traduction libre)».

Le COC souligne que les conditions légales – l'obtention des décisions requises du Conseil communal, les analyses d'impact relatives à la protection des données, la déclaration dans le REGPOL, etc. – doivent être remplies **avant** la mise en service des caméras. Le consentement éclairé des Conseils communaux, en particulier, qui doit s'assortir d'une analyse d'impact relative à la protection des données[30], est essentiel – certainement du point de vue des droits fondamentaux – étant donné qu'il est l'expression de la prise de décision démocratique locale et donc de la surface portante à ce niveau.

[25] Loi du 21 mars 2018 modifiant la loi sur la fonction de police, en vue de régler l'utilisation de caméras par les services de police, et modifiant la loi du 21 mars 2007 réglant l'installation et l'utilisation de caméras de surveillance, la loi du 30 novembre 1998 organique des services de renseignement et de sécurité et la loi du 2 octobre 2017 réglementant la sécurité privée et particulière, *M.B.* 16 avril 2018.

[26] Article 25/4 §1er, 1° de la LFP.

[27] Exposé des motifs de cette loi, p. 21 (Doc. Parl. *Chambre* 2017-2018, n° 54-2588/001).

[28] Article 88 de la loi du 21 mars 2018 et Exposé des motifs de cette loi, p. 113-114 (Doc. Parl. *Chambre* 2017-2018, n° 54-2588/001).

[29] Article 25/4 §2, 2e alinéa de la LFP.

[30] Qui doit également contenir l'analyse d'impact et de risques au niveau de la protection de la vie privée et au niveau opérationnel, notamment quant aux catégories de données à caractère personnel traitées, à la proportionnalité des moyens mis en œuvre, aux objectifs opérationnels à atteindre et à la durée de conservation des données nécessaire pour atteindre ces objectifs (article 25/4 §2, 2e alinéa de la LFP).

5. CONCLUSION – REQUÊTES, RECOMMANDATIONS ET MESURES CORRECTRICES

Après l'annonce de la visite, la zone de police a commencé à élaborer la note temporaire du corps consacrée aux banques de données particulières. La note du corps décrit correctement les dispositions légales régissant la création d'une banque de données particulière. 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 zone de police, 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.

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, la zone de police ne manque 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.

L'Organe de contrôle

prie la ZP FLOcc

1) Requête

de transmettre un nouveau point de la situation concernant les banques de données particulières dans un délai de maximum 4 mois à compter de la réception du présent rapport;

émet les recommandations suivantes :

2) Recommandation

le COC recommande que la CSI se réunisse régulièrement afin d'assurer les évaluations et le suivi nécessaires des banques de données particulières. Les données ne peuvent être traitées que lorsqu'elles sont adéquates, pertinentes et limitées à ce qui est nécessaire. Le COC recommande de prévoir pour les banques de données particulières une évaluation régulière et, dans la mesure du possible, des délais de conservation maximums;

3) Recommandation

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'authentification multi-facteurs si cette possibilité technique peut être prévue. Ce système permet en effet de réduire les risques inhérents à l'utilisation de mots de passe ;

4) Recommandation

l'Organe de contrôle insiste auprès de la zone de police pour que seule l'utilisation de comptes d'utilisateur nominatifs/individuels soit autorisée dans le cadre de la gestion opérationnelle.
L'utilisation d'un compte d'utilisateur générique pour l'administration du système doit être limitée le plus possible et n'est admise que lorsqu'il s'agit d'une exigence technique. Les utilisateurs disposant de droits d'accès étendus, comme les administrateurs système et les gestionnaires d'applications (les 'utilisateurs privilégiés'), doivent s'acquitter de leurs tâches journalières au moyen d'un compte d'utilisateur nominatif. Les comptes génériques partagés comportent en effet

un risque qu'en cas d'abus, il ne soit pas possible de déterminer qui en est responsable. De plus, un utilisateur privilégié animé de mauvaises intentions est en principe en mesure, vu ses droits d'accès étendus, d'effacer les traces de ses activités par exemple en adaptant ou en supprimant intégralement les fichiers de journalisation du système ;

5) Recommandation

Conformément à l'article 28, 6° de la loi relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, il y a lieu de prévoir les mesures techniques ou organisationnelles appropriées pour garantir la sécurité des banques de données particulières, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle. Le COC recommande de créer les banques de données particulières selon une procédure étalonnée et en particulier conformément à la fiche technique, de manière à satisfaire aux exigences de sécurité stipulées par l'article 28, 6° de la LPD;

6) Recommandation

conformément à la directive ministérielle MFO-3, 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/…);

7) Recommandation

bien que l'Organe de contrôle constate que la validation centrale ait été effectuée régulièrement, il est souhaitable d'éviter toute accumulation de retards. L'objectif doit viser à limiter le nombre de rejets à 100 lignes. Le COC recommande de prévoir un(e) remplaçant(e) pour la personne chargée du traitement des rejets;

ordonne les mesures correctrices suivantes à la ZP FLOcc,

Vu les articles 221 §1er et 247, 4°, 5° et 6° de la LPD,

8.a) 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 ;

8.b) déclarer les banques de données particulières et les caméras utilisées dans la zone de police 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 ;

8.c) prévoir pour la consultation des banques de données particulières un champ à compléter pour spécifier le motif de la consultation. L'utilisation de cases à cocher ne suffit pas à obtenir une donnée identifiable, ni donc à satisfaire aux dispositions légales des articles 56 §1er, 2 et 3 de la LPD *juncto* l'article 44/11/3 §4 de la LFP. L'Organe de contrôle fixe le délai de mise en œuvre à 6 mois à compter de la prise de connaissance de la présente mesure correctrice ;

8.d) élaborer un règlement/une politique prévoyant un mécanisme de contrôle périodique et effectif du monitoring d'éventuelles consultations (il)licites 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 zone de police de procéder à un contrôle obligatoire des journalisations deux fois par an et de tenir les résultats à la disposition du COC;

8.e) consulter régulièrement les journalisations de la BNG et procéder à des contrôles proactifs, par échantillonnage (2x/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 ;

8.f) dans le courant de 2021, ou au plus tard dans un délai d'un an à compter de la prise de connaissance de la présente mesure correctrice, ne plus recourir au contrôle biométrique des accès et veiller à ce qu'au terme du délai susmentionné, il ne subsiste plus qu'un système alternatif ne recourant pas au traitement de données biométriques ;

9) veiller à ce que, pour l'utilisation des différents types de caméras – dont les caméras de surveillance et les caméras *ANPR* fixes et mobiles –, les décisions des Conseils communaux qui sont requises par la loi, accompagnées de l'analyse d'impact et de risques visée à l'article 25/4 §2, 2e alinéa de la LFP, aient été adoptées, et informer le COC dès que toutes les décisions des Conseils communaux auront été obtenues, et ce dans les quatre mois à compter de la prise de connaissance de la présente mesure correctrice ;

Dit pour droit que la date d'entrée en vigueur des mesures correctrices et la date de prise de connaissance desdites mesures telles que visées aux points 8.a) à f) inclus et 9 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 §1er, alinéa premier, et §2 de la LPD).

Ainsi décidé par l'Organe de contrôle de l'information policière le 12 janvier 2021.

Pour l'Organe de contrôle,

Philippe Arnould
Président