**Avis COC-DPA-A n° 009/2018 du 12 décembre 2018**

DA180009

**Objet : *avis concernant l'avant-projet de loi relatif à la gestion de l'information policière et modifiant la loi sur la fonction de police et la loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux***

L'Organe de contrôle de l'information policière (ci-après "le COC" ou "l'Organe de contrôle").

Vu la loi du 30 juillet 2018 *relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel* (M.B. du 5 septembre 2018, ci-après la "LPD"), en particulier l'article 71 et le titre VII.

Vu la loi du 5 août 1992 *sur la fonction de police* (ci-après la "LFP"), en particulier l'article 44/6.

Vu la demande du 19 novembre 2018 de Monsieur Jambon, Vice-premier ministre et Ministre de la Sécurité et de l'Intérieur, en vertu de la LPD précitée, concernant un "*avant-projet de loi relatif à la gestion de l'information policière et modifiant la loi sur la fonction de police et la loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux*" (ci-après "l'avant-projet").

Vu le rapport de Monsieur Frank Schuermans, membre-conseiller de l'Organe de contrôle.

Émet, le 12 décembre 2018, l'avis suivant :

## I. Remarque préalable concernant la compétence de l'Organe de contrôle

À la lumière respectivement de l'application et de la transposition du Règlement 2016/679[1] et de la Directive 2016/680[2], le législateur a profondément modifié les tâches et les missions de l'Organe de contrôle. L'article 4, § 2, troisième alinéa de la loi organique du 3 décembre 2017 *portant création de l'Autorité de protection des données*[3] dispose que pour les services de police au sens de l'article 2, 2° de la loi du 7 décembre 1998 *organisant un service de police intégré, structuré à deux niveaux*[4], les compétences, missions et pouvoirs d'autorité de contrôle tels que prévus par le Règlement 2016/679 sont exercés par l'Organe de contrôle.

Cela signifie notamment que l'Organe de contrôle est également compétent lorsque des services de police traitent des données à caractère personnel qui ne relèvent pas des missions de police administrative et judiciaire, par exemple dans le cadre de finalités socio-économiques ou de traitements de ressources humaines.

L'Organe de contrôle doit être consulté dans le cadre de la préparation d'une législation ou d'une mesure réglementaire liée au traitement de données à caractère personnel par les services de police de la police intégrée (voir l'article 236, § 2 de la LPD[5], l'article 36.4 du RGPD et l'article 28.2 de la Directive Police et Justice). Dans ce cadre, l'Organe de contrôle a pour mission d'examiner si l'activité de traitement envisagée par les services de police est conforme aux dispositions des Titres 1er (pour les traitements non opérationnels) et 2 (pour les traitements opérationnels) de la LTD[6].

En ce qui concerne en particulier les activités de traitement dans le cadre des missions de police administrative et/ou de police judiciaire, l'Organe de contrôle émet un avis, soit d'initiative, soit à la demande du gouvernement ou de la Chambre des représentants, d'une autorité administrative ou judiciaire ou d'un service de police concernant toute question relative à la gestion de l'information policière, telle que régie dans la section 12 du chapitre 4 de la loi *sur la fonction de police*[7].

En outre, à l'égard des services de police, de l'Inspection générale de la police fédérale et de la police locale telle que visée dans la loi du 15 mai 2007 sur l'Inspection générale et de l'Unité d'information des passagers visée au chapitre 7 de la loi du 25 décembre 2016, l'Organe de contrôle est également chargé du contrôle de l'application du Titre 2 de la LPD, du traitement de données à caractère personnel tel que visé aux articles 44/1 à 44/11/13 de la loi *sur la fonction de police*[8] et de toute autre mission qui lui est confiée par ou en vertu d'autres lois.[9]

## II. Objet de la demande

**1.** L'avant-projet a pour but d'adapter les règles relatives à la gestion de données à caractère personnel et d'informations par les services de police au nouveau cadre juridique européen et national en matière de protection des données. Il s'agit bien entendu du RGPD, de la Directive Police et Justice

---

[1] 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 ou RGPD).

[2] 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 la "Directive Police et Justice").

[3] En abrégé ci-après : "loi LPD".

[4] En abrégé ci-après : LPI.

[5] En abrégé ci-après : LPD.

[6] Article 59, § 1, 2°, deuxième alinéa de la LPD.

[7] Article 236, § 1 de la LPD.

[8] En abrégé ci-après : LFP.

[9] Article 236, § 3 de la LPD.

2016/680, de la LPD et de la loi APD. Le Titre 2 de la LPD fixe le cadre général. L'avant-projet a l'ambition de spécifier plus avant ce cadre général *in concreto* dans la législation opérationnelle et statutaire existante relative à la police intégrée. D'après l'Exposé des motifs, il faut assurer "*un degré élevé à la fois de protection et de sécurisation des données à caractère personnel et de leur traitement. Il convient notamment de désigner des responsables du traitement et des délégués à la protection des données, de définir des catégories de données, de mettre sur pied un cadre légal, notamment en recueillant des avis préalables aux traitements, en mettant un registre de ces traitements à la disposition de l'autorité de contrôle et en procédant à une journalisation des opérations de traitement.*"

## III. Examen du projet

**3.** Dans le présent avis, l'Organe de contrôle suit la chronologie de l'avant-projet mais ne se penche pas sur les adaptations purement techniques. Ces adaptations techniques concernent notamment le nouveau cadre juridique de l'Organe de contrôle prévu à l'article 71 et au Titre VII de la LPD.

Il convient toutefois de remarquer que dans la LFP, les termes "*Commission de la protection de la vie privée*" n'ont pas été remplacés dans tous les articles par l'Organe de contrôle ou "l'autorité de contrôle compétente" (par exemple à l'article 44/11/3bis, § 4 et § 8, à l'article 44/11/3ter, § 2, 2e alinéa et § 3, 1e et 2e alinéa de la LFP). L'Organe de contrôle demande de le faire. Dans l'en-tête de l'avant-projet, l'Organe de contrôle demande de renvoyer au présent avis.

De manière générale, l'auteur du projet doit revoir et corriger la version néerlandaise du projet. Il est évident que le texte original a été rédigé en français.

### III.1. Modifications de la loi du 5 août 1992 sur la fonction de police

**4.** Le premier alinéa du projet d'article 44/1, § 2 (article 4 de l'avant-projet) présente peu de plus-value vu les alinéas 2 et 4. En soi, il fait double emploi. Les termes "*objet principal*" devraient de préférence au moins être remplacés, par exemple par "*pour autant que l'on ne vise pas le traitement des données à caractère personnel visées à l'article 34 de la même loi*". Même une finalité "principale" reste en effet une finalité. Soit c'est une finalité, soit ce n'en est pas une. Mais on ne peut pas absolument exclure que ces données soient traitées *indirectement*. Il est dès lors recommandé d'expliquer dans l'Exposé des motifs qu'il s'agit d'un traitement qui n'est pas intrinsèquement visé, mais qu'il s'agit d'un élément dans la collecte de données dans le cadre de leurs missions policières opérationnelles (en ce qui concerne par exemple la fonction de police judiciaire : des données de santé lors d'un accident de la route ; des coups et blessures dont le motif est probablement la nature ou les origines de la victime ; en ce qui concerne par exemple la fonction de police administrative : une liste de groupements qui perturbent l'ordre public comme un groupement composé de salafistes qui sont connus pour leur aversion envers les valeurs démocratiques).

Le projet d'article 44/1, § 2 introduit la notion de "*données sensibles*". Il ne semble pas recommandé d'utiliser ici cette notion sans la définir. Celle-ci est certes utilisée couramment sur le terrain mais elle n'est pour le reste définie dans aucun texte réglementaire. Ni le RGPD, ni la Directive Police et Justice, ni la LPD n'utilisent cette notion. L'Organe de contrôle recommande dès lors d'éviter cette notion dans le corps du projet, mais il n'a pas d'objection à ce qu'on l'explique dans l'Exposé des motifs. Les termes juridiques corrects sont "*catégories particulières de données à caractère personnel*".

**5.** Dans le deuxième alinéa du projet d'article 44/1, § 2, l'Organe de contrôle recommande d'ajouter, entre les termes "*en complément*" et le terme "*d'autres*", les termes "*et en appui*" afin que la phrase devienne : "*Les données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale ainsi que les données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique sont traitées en complément* ***et/ou en appui*** *d'autres catégories de données visées à l'article 44/5.*" En général, ces données seront en effet plutôt en appui dans le travail policier quotidien, à des fins par exemple de preuve dans le cadre des missions de police judiciaire. Une même remarque s'applique au 3e alinéa qui traite de données biométriques et au 4e alinéa qui traite des données de santé (voir également la remarque au point 4).

**6.** Au 4e alinéa, les possibilités pour les services de police de traiter des données relatives à la santé, outre le caractère complémentaire (et d'appui, cf. point 5) du traitement, sont encore réduites par les termes "*et uniquement dans le but de comprendre le contexte lié à la personne concernée, ainsi que pour assurer la sécurité et protéger la santé de toute personne susceptible d'entrer en contact avec les personnes concernées dans le cadre de l'intervention policière.*" L'auteur du projet doit réfléchir à la question de savoir si tous les traitements de données relatives à la santé réalisés couramment dans la pratique par la police sont ainsi couverts. Le dernier segment ("*assurer la sécurité et protéger la santé de toute personne susceptible d'entrer en contact avec les personnes concernées dans le cadre de l'intervention policière")* ne requiert aucune précision, mais vise un cas d'application particulier et vise la protection de tiers (qu'ils soient ou non membres du personnel des services de police). Le premier segment ("*dans le but de comprendre le contexte lié à la personne concernée*") est par contre sujet à interprétation. Il est ainsi évident que la police doit pouvoir traiter des données relatives à la santé dans le cadre de la constatation de toutes sortes d'infractions contre l'ordre des familles et contre la moralité publique (Livre II, Titre VII du Code pénal), tant concernant un suspect qu'une victime. Il ne s'agit pas tant du "*contexte lié à la personne concernée*" mais simplement par exemple de son état de santé (porteur d'une maladie, patient cardiaque, historique de problèmes psychiatriques, etc.). L'Organe de contrôle estime à cet égard que les termes employés sont dès lors ambigus (il semble plutôt s'agir de circonstances externes), avec toutes les conséquences qui en découlent sur la régularité des futurs actes policiers d'information ou d'instruction, ou de manière plus générale sur la régularité de la procédure. Il semble préférable d'exclure les discussions à ce niveau et il incombe dès lors à l'auteur du projet de clarifier les choses. Cette clarté peut consister simplement à faire référence à la nécessité de traiter des données relatives à la santé pour l'exercice de leurs missions de police administrative ou judiciaire et la protection de la santé de tiers.

**7.** L'article 44/3 (article 6 de l'avant-projet) est adapté afin de remplacer la fonction de conseiller en sécurité et en protection de la vie privée par celle de "Data Protection Officer" (DPO) ou délégué à la protection des données et doit être lu conjointement avec le projet d'article 144 de la loi relative à la police intégrée du 7 décembre 1998 (ci-après "LPI"). L'Organe de contrôle n'a pas de remarque particulière à formuler à cet égard étant donné que tout cela est conforme au nouveau cadre de protection des données.

**8.** L'article 44/4 de la LFP est remplacé intégralement (article 7 de l'avant-projet).

Le COC salue la désignation claire du responsable du traitement pour les trois types de banques de données (à savoir la BNG, les banques de données de base et les banques de données particulières). L'Organe de contrôle souligne toutefois la désignation des "autorités compétentes" à l'article 26, 7° de la LPD, à savoir "*les services de police au sens de l'article 2, 2°, de la loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux*". Les deux ministres de tutelle ont bien la responsabilité (politique) finale, mais les services de police doivent quand même au moins être

désignés comme responsables du traitement opérationnels en vertu de l'article 26, 7° de la LPD *juncto* l'article 2, 2° de la LPI, si pas être considérés comme responsables du traitement conjoints). Ils ont en effet une influence de fait sur le traitement et contribuent au moins à déterminer dans les faits les moyens mis en œuvre en vue des finalités visées. On peut également s'inspirer des termes "gestionnaire" et "responsable opérationnel" employés pour les banques de données communes, outre le responsable du traitement proprement dit. Une telle construction est préférée par le COC pour la BNG et les banques de données de base et même pour les banques de données particulières. Pour assurer une uniformité entre les différentes banques de données policières, le COC choisit de désigner comme responsable du traitement la zone de police (pour la police locale) et le Ministre de l'Intérieur et/ou de la Justice (pour la police fédérale). Le chef de corps, le commissaire général, le directeur général et les directeurs sont alors les responsables opérationnels et les gestionnaires. Ainsi, il y a une uniformité juridique dans la désignation du responsable du traitement, du responsable opérationnel et du gestionnaire pour l'ensemble des banques de données policières et communes.

Le 2e paragraphe prévoit que pour **toutes** les banques de données mentionnées à l'article 44/2 (à savoir la BNG, les banques de données de base, les banques de données particulières, les banques de données communes et les banques de données techniques), les deux ministres déterminent par directives – le COC aurait aimé lire "par directives contraignantes" - les mesures en vue d'assurer la gestion et la sécurité, et que pour tout traitement dans les banques de données précitées, des fichiers de journalisation soient établis pour les traitements les plus essentiels. Il n'est tout d'abord pas recommandé de paraphraser/copier l'actuel article 56 de la LPD dans le 3e alinéa du § 2 ; un simple renvoi à cet article 56 LPD suffit.

Ces fichiers de journalisation doivent ensuite permettre de générer les informations prévues par le projet de 3e alinéa (superflu) du § 2, ce que le COC salue dès lors qu'à l'heure actuelle, ce n'est pas possible de le faire avec autant de détails. Il s'agit donc d'une finalité ambitieuse qui devra également être concrétisée et pour laquelle les responsables du traitement pourront être interpellés. Ainsi par exemple, la mention d'un motif d'un traitement (par exemple dans la BNG) n'est jusqu'à présent pas encore une obligation à laquelle on ne peut échapper. À l'heure actuelle il s'agit d'une possibilité facultative qui n'est pas toujours respectée, mais rien n'empêche un agent de police d'indiquer un faux motif. En ce qui concerne les fichiers de journalisation, le COC souligne qu'il doit y avoir accès à tout moment, comme l'affirme aussi l'Exposé des motifs, même si un code utilisateur limité est prévu pour l'information.

Le projet de § 3 est également nouveau. Il impose aux ministres de l'Intérieur et de la Justice, chacun dans le cadre de leurs compétences, de déterminer par directive les règles d'accès des membres des services de police aux banques de données visées à l'article 44/2, § 1 et § 3. La circulaire MFO 3, qui est désespérément désuète depuis bien longtemps et qui n'a pas été adaptée suite aux modifications du cadre juridique en matière de gestion de l'information apportées par la loi de 2014[10], nécessite par cet avant-projet une mise à jour encore plus profonde, qui devra intégrer aussi cet aspect des règles d'accès. Les responsables du traitement pourront également être interpellés à ce sujet.

L'Exposé des motifs motive de manière étendue la raison pour laquelle des liens entre différentes banques de données policières et autres ou entre parties de celles-ci sont nécessaires dans son commentaire du projet de § 3bis de l'article 44/4 qui est une paraphrase de l'actuel § 3. Le COC comprend parfaitement le raisonnement mené mais insiste pour que les ministres de tutelle exercent aussi réellement cette compétence en formulant des directives et en n'acceptant pas que des liens

[10] Loi du 18 mars 2014 *relative à la gestion de l'information policière et modifiant la loi du 5 août 1992 sur la fonction de police, la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel et le Code d'instruction criminelle.*

soient établis sur le terrain qui ne soient pas encadrés par de telles directives, ce qui est le cas actuellement. L'exemple le plus évident est l'application INFOTHÈQUE au sein de laquelle les banques de données de base de dizaines de zones de police sont reliées en l'absence de telles directives. En l'espèce, c'est d'autant plus problématique que les banques de données de base précitées contiennent encore beaucoup d'informations non validées. La nécessité opérationnelle de disposer aussi dans certains cas d'informations non validées est évidente, mais la nécessité de règles contraignantes concernant l'accès et l'utilisation de ces données non validées sont d'autant plus indispensables. À cet égard, le COC renvoie à l'enquête de contrôle 2016/1 qu'il a menée.

Les exemples donnés dans l'Exposé des motifs vont encore bien plus loin et s'inscrivent dans le cadre du concept "I-police" où un fonctionnaire de police a accès sur le terrain via sa tablette ou son smartphone à une foule d'informations et de fichiers de données. On y trouvera aussi inévitablement des informations qui ne sont pas encore évaluées et/ou validées, ce qui, comme l'affirme l'Exposé des motifs à juste titre, est "*particulièrement important dans des situations de contrôle pouvant avoir des effets sur les droits et libertés des personnes*". Ceci devra être bien encadré par les directives annoncées. Entre-temps, en ce qui concerne INFOTHÈQUE par exemple, quelques conventions policières internes ont quand même été conclues, mais cela est largement insuffisant. L'application FOCUS, qui est notamment utilisée par la police d'Anvers et par laquelle l'inspecteur de police peut consulter directement sur sa tablette/son smartphone toutes sortes d'informations provenant de différentes banques de données, est également juridiquement problématique à l'heure actuelle, bien qu'en termes opérationnels, on ne puisse douter de sa plus-value. Il ne suffit donc pas de donner une délégation aux ministres de tutelle dans une législation ; elle doit aussi être **exécutée** en pratique, ce qui est d'autant plus le cas au regard du projet de 2e alinéa du § 3bis. Depuis 2014, force est de constater que les choses laissent à désirer à ce niveau.

Le COC souhaite dès lors exhorter les ministres de tutelle à concrétiser enfin les directives précitées qui devront, encore bien plus qu'auparavant, comporter toute une série d'éléments détaillés comme décrit précisément dans les projets de §§ 3, 3bis et 3ter de l'article 44/4 et dans l'Exposé des motifs y afférent.

En ce qui concerne enfin le projet d'article 44/4 § 3, 3bis et 3ter de la LFP, l'Organe de contrôle formule des réserves explicites quant à la question de savoir si l'avant-projet offre bien une base légale (suffisante) pour instaurer le futur concept "I-police", ce que l'Exposé des motifs s'empresse de supposer à tort (p. 14). À l'heure d'aujourd'hui, il n'est pas encore suffisamment évident de savoir ce que comportera précisément le concept précité (en réalité), empêchant *hic et nunc* le COC d'évaluer suffisamment sa compatibilité avec la LFP, la LPD et le RGPD.

**9.** À l'article 44/5, une 7e catégorie de données à caractère personnel qui peuvent être traitées à des fins de police administrative est ajoutée, à savoir "*les données relatives aux personnes faisant l'objet d'une mesure administrative prise par une autorité administrative compétente et que les services de police sont chargés de suivre en vertu de la loi*". Les finalités de la reprise de cette nouvelle catégorie dans la BNG et les banques de données de base sont commentées en détail dans l'Exposé des motifs.

La notion de "*mesure administrative*" n'est pas définie dans la LFP (voir les définitions à l'article 3[11]). Cette notion est toutefois utilisée à l'article 30 de la LFP (en ce qui concerne la saisie administrative, où la notion est néanmoins clairement utilisée dans sa signification la plus restreinte de mesure

[11] La notion de "mesure policière" est bien définie mais est clairement plus restreinte que celle de mesure administrative. Une mesure policière doit émaner d'une autorité de police administrative ou judiciaire, ce qui n'est pas nécessairement le cas pour une mesure administrative qui peut émaner par exemple d'une administration ordinaire.

policière (administrative) prise par un fonctionnaire de police). L'utilisation à l'article 44/9 (concernant l'archivage des données de la BNG) semble plus importante. Il y est question d'une "*mesure sur la base d'une décision d'une autorité administrative ou judiciaire compétente*" (cf. l'art. 44/9, § 1, 2e alinéa, a) et § 2, 4e alinéa, 1e tiret et 7e alinéa, 1e tiret), mais il faut partir du principe que le législateur parle ici d'une mesure prise par une autorité policière (administrative) au sens de l'article 3, 2° de la LFP.

L'Exposé des motifs établit toutefois clairement que l'on vise en l'espèce une catégorie encore plus large de décisions mais il reste quelque peu vague étant donné qu'il donne quelques exemples non exhaustifs. Quelques uns de ces exemples ne sont en outre pas une mesure administrative mais purement une sanction administrative, dont l'Exposé des motifs donne d'ailleurs aussi un exemple concret (à savoir les sanctions prévues dans la loi SAC du 24 juin 2013). Il est crucial de savoir **clairement** dans la loi quelles mesures et sanctions de quelles autorités peuvent être saisies dans la BNG et dans les banques de données de base. En ce sens, le COC propose de faire la clarté et de compléter le point 7° par le terme "*sanction*" et de reformuler légèrement comme suit : "*les données relatives aux personnes faisant l'objet d'une mesure administrative ou d'une sanction administrative prise par une autorité administrative compétente et que les services de police doivent surveiller par ou en vertu de la loi ou dont ils assurent le respect.*" De cette manière, on sait clairement qu'il ne s'agit pas uniquement de décisions prises par une autorité policière administrative (bourgmestre, gouverneur, ministre de l'Intérieur) mais par toute administration qui peut prendre une mesure ou une sanction dont la surveillance du respect ou de l'application relève des missions de la police, et ce par ou en vertu de la loi.

Les autres modifications de l'article 44/5 ne donnent pas lieu à des remarques spécifiques.

**10.** À l'article 44/9 concernant l'archivage et l'effacement des données dans la BNG, quelques modifications sont apportées (que l'on appelle souvent dans le jargon policier "*ventilation*"). On prévoit que la nouvelle catégorie de mesures administratives (et de sanctions, cf. plus haut) soit ventilée après 3 ans au plus tard. Contrairement à ce que mentionne l'Exposé des motifs, il ne s'agit pas d'une "adaptation technique". Le COC prend acte du choix du délai le plus court de 3 ans qui est en effet un délai maximal. Il incombe à l'auteur du projet d'évaluer si la ventilation après 3 ans correspond dans tous les cas à la durée de la mesure. Le COC ne connaît pas toutes les mesures potentielles existantes que la police doit surveiller mais constate néanmoins que les plus récurrentes sont d'une durée inférieure à 3 ans (fermeture d'institution, suspension d'autorisation d'exploitation, interdiction de lieu, ...). Mais ce n'est pas toujours le cas. On constate ainsi que la source authentique des interdictions de stade administratives (loi football) qui se trouve au SPF Intérieur prévoit un délai de conservation de 5 ans[12] étant donné qu'une interdiction de stade (administrative) à titre de sanction peut être infligée pour une durée allant jusqu'à cinq ans maximum.

Dans la pratique, le COC constate quoi qu'il en soit que, sauf pour des adaptations ponctuelles à l'occasion par exemple d'une demande d'accès indirect, les délais de ventilation maximaux utilisés à l'article 44/9 sont bel et bien épuisés. Vu la masse de données, l'obligation du responsable du traitement (en l'espèce les services de la police intégrée) d'archiver dès que les données présentent un caractère non adéquat, non pertinent ou excessif est en pratique manifestement tout à fait irréalisable.

En pratique, il apparaît en outre que les règles de ventilation qui sont déjà d'application depuis 2014 ne sont appliquées que depuis très récemment et de surcroît de manière très partielle seulement, ce

---

[12] Article 1, § 4 de l'arrêté royal du 7 décembre 1999 *contenant l'établissement d'un fichier des interdictions de stade*.

qui constitue quand même un problème majeur que l'Organe de contrôle a déjà mis en évidence de manière répétée. Ce n'est que le 20 novembre 2018 que les données à caractère personnel de police administrative ont été ventilées de manière systématique, comme le prévoit l'article 44/9 de la LFP. Il s'agissait, pour autant que l'Organe de contrôle ait pu le constater, d'une opération "one shot". Les données à caractère personnel de police judiciaire ne sont toujours pas ventilées, et encore moins de manière systématique. Son application automatisée ne serait prête qu'à la mi 2019, à titre ou non de mesure "one shot". Il est évident que tout cela est de plus en plus problématique, d'autant plus depuis l'entrée en vigueur du nouveau cadre de protection des données. L'Organe de contrôle acceptera encore une période de tolérance jusqu'à la mi 2019 mais recourra ensuite au besoin à ses possibilités de sanction administrative et à ses compétences correctrices. Il doit en effet être clair que la non-application des règles de ventilation est tout à fait contraire notamment avec les articles 28, 1°, 2°, 3° et 4°, 29, § 5 et 30, 1e alinéa de la LPD (et les articles 4 et 5 correspondants de la Directive Police et Justice). Ce n'est pas le lieu pour aborder cette problématique en profondeur, ce que l'Organe de contrôle fera dans le cadre d'une enquête thématique spécifique sur l'application des règles de ventilation par les services de la police intégrée.

Toutefois, une des principales raisons pour lesquelles la police et ses autorités de tutelle sont restées en défaut, depuis 2014 à aujourd'hui, de respecter un principe fondamental du droit de protection des données touche principalement à la complexité des règles de ventilation dans la LFP. Le COC a déjà adressé un courrier à la police fédérale à ce sujet il y a une paire d'années pour demander d'envisager une simplification du système, courrier qui a toutefois reçu une réponse négative. Il est cependant clair que plus un règlement est complexe, plus son respect sera problématique et plus il sera néfaste pour la vie privée. Vu le caractère nécessairement automatisé de la ventilation des millions de données, il est important d'avoir un système de délai qui ne soit pas trop complexe. Le résultat de la situation actuelle prédit par l'Organe de contrôle, à savoir que les règles légales ne seront simplement pas appliquées, s'est aussi confirmé depuis 2014 à aujourd'hui. En l'espèce, le COC renouvelle son appel à simplifier les règles de ventilation légalement prévues. Cette simplification est en parfaite adéquation avec (l'ancien et le nouveau) cadre de protection des données et porte le moins atteinte à la vie privée, bien au contraire. Récemment, la Cour constitutionnelle a estimé ce qui suit dans son arrêt 29/2018, en ce qui concerne le délai de conservation de données de consommation d'eau, d'électricité et de gaz qui sont transmises aux autorités depuis les entreprises d'utilité publique ou les gestionnaires de réseaux de distribution dans le cadre de la lutte contre la fraude au domicile : "*Compte tenu du fait que le législateur ne peut prévoir des règles distinctes et précises pour tous les cas spécifiques, il pouvait régler de manière générale les conditions de conservation des données à caractère personnel, ainsi que la durée de cette conservation. Il découle de ce qui précède que le législateur a réglé les éléments essentiels de la durée de conservation des données.*" (considérant B.23).

Par ailleurs, l'Organe de contrôle se demande si l'ensemble du système d'archivage tel que prévu dans la LFP est encore compatible avec l'article 30 de la LPD qui affirme dans son 1e alinéa qu'à l'échéance de cette durée de conservation, les données sont effacées. Un archivage général et non ciblé de toutes les données semble contraire à cette disposition. Certes, le 2e alinéa de l'article 30 de la LPD prévoit la possibilité que la loi puisse prévoir qu'à l'échéance d'un premier délai de conservation, une analyse doive être effectuée sur la base de différents critères de nécessité et de proportionnalité afin de déterminer si la conservation des données doit être maintenue et, le cas échéant, le nouveau délai de conservation, mais le constat reste que dans la LFP, on ne trouve rien quant à de tels "critères différents de nécessité et de proportionnalité", et ils ne sont pas non plus appliqués en pratique, pour autant déjà qu'ils existent. En principe, **toutes** les données à caractère personnel et informations sont en effet archivées sans un quelconque contrôle de nécessité et de proportionnalité. La LPD est en l'espèce la transposition notamment des articles 4 et 5 de la Directive Police et Justice qui concernent à leur tour une **vérification régulière** de la conservation des données, un système d'archivage automatique de

toutes les données après une échéance déterminée étant également contraire à ce principe. Il incombe à l'auteur du projet de faire la clarté à cet égard.

**11.** Dans le projet d'article 44/11/2 (article 13 de l'avant-projet) au 2e paragraphe, l'actuel 1e alinéa est supprimé, lequel dispose que "*Les données à caractère personnel et les informations traitées dans les banques de données de base, à l'exception de celles relatives à la gestion des enquêtes, ne sont disponibles et directement consultables que par les services de police qui les ont enregistrées ou qui doivent, de par leurs missions légales, coordonner les données et informations.*" De cette manière, l'auteur du projet veut retirer de la zone d'ombre légale la pratique actuelle - problématique du point de vue légistique - de couplage entre les banques de données de base ISLP des différentes zones de police locales (cf. ci-avant, l'enquête INFOTHÈQUE du COC). Le COC a lui-même plaidé pour cela dans son enquête de contrôle dès lors que la plus-value opérationnelle de tels couplages est incontestable, mais engendre par ailleurs aussi des risques plus élevés au niveau de la vie privée et de la protection des données, l'application précitée étant un exemple type de cas dans lesquels la police travaillera avec des informations non validées et posera probablement aussi certains actes policiers avec exercice ou non de la contrainte ou de la violence. D'où la nécessité d'intégrer dans ces cas les limites et sécurités utiles dont question ci-avant (cf. point 8).

**12.** À l'article 44/11/3 de la LFP qui régit les banques de données particulières (article 14 de l'avant-projet), le premier paragraphe est remplacé et l'on indique surtout quelles catégories de données peuvent y être reprises. L'Organe de contrôle, depuis qu'il a rendu son avis le 31 mars 2017 sur environ 800 banques de données particulières, plaide pour la suppression des termes "*dans des circonstances exceptionnelles*" comme condition pour la création d'une banque de données particulière.

Tout d'abord, personne ne sait vraiment, et certainement pas la police, ce que l'on doit entendre par "*circonstances exceptionnelles*". Lors de la déclaration de dizaines de banques de données particulières, l'Organe de contrôle a déjà aussi été en conflit avec cette notion, d'autant plus que de nombreuses déclarations ne reflétaient rien d' "exceptionnel", mais faisaient simplement partie du fonctionnement régulier de la police. En d'autres termes, de très nombreuses banques de données particulières font partie de ce qu'on peut considérer comme des missions de routine et des compétences d'un service de police dans l'exercice normal des tâches de police administrative et judiciaire. Étant donné toutefois que le fichier de données déclaré ne peut être considéré comme faisant partie ni d'une banque de données de base, ni de la BNG, bon nombre d'entre eux ont quand même été considérés comme une banque de données particulière par l'Organe de contrôle parce qu'autrement, on aurait pu penser que le fichier n'aurait tout simplement aucune base juridique étant donné que l'énumération des banques de données policières existantes est une énumération limitative. On peut citer comme exemple les banques de données particulières reprenant des données de transmigrants ou de personnes pour lesquelles il y a des indices de radicalisation, ou une banque de données à caractère personnel liées à des bateaux et à leurs propriétaires, ou la banque de données "Mercure" pour la gestion des données d'une enquête sur la téléphonie, ou une banque de données de personnes qui habitent la zone et à l'égard desquelles des mesures de probation ont été prononcées, une banque de données pour le management RIR[13] (management d'informations douces), une banque de données des permis de conduire retirés immédiatement, une banque de données de personnes sous surveillance électronique, la banque de données "infocop" qui est plutôt un outil de briefing avec toutes sortes d'informations opérationnelles, une banque de données "attention particulière" dont le but est de diriger des équipes d'intervention et d'action et qui reprend un relevé

[13] Pour "Rapport d'Information-Informatierapporten".

des personnes, lieux et véhicules qui doivent faire l'objet de l'attention particulière des équipes, une banque de données des mineurs placés sous surveillance, etc. On pourrait donner ainsi des dizaines d'exemples. Toutes ces banques de données sont nécessaires pour l'exercice courant et régulier des missions de police et ne constituent dès lors pas véritablement des "*circonstances exceptionnelles*".

Pour ne pas dévaluer le concept de banque de données "*particulière*", l'Organe de contrôle a toutefois estimé à de très nombreuses reprises qu'il ne s'agissait pas de banques de données particulières mais que la police devait quand même pouvoir les maintenir, parce qu'elles sont nécessaires pour son fonctionnement (bien que, comme indiqué, on peut douter quant à l'existence d'une base juridique pour la police pour maintenir une banque de données opérationnelle, autre que les types énoncés dans la LFP). Il s'agissait par exemple d'une banque de données de personnes arrêtées administrativement (registre des personnes arrêtées), d'une banque de données de visiteurs d'un poste de police, d'un registre d'objets saisis, d'une banque de données d'infractions commises par des véhicules prioritaires, etc.

Il serait plus confortable pour tout le monde sur le terrain si la notion de "*circonstances exceptionnelles*" était abandonnée, ou du moins si elle était remplacée par une description plus proche de la réalité et mieux utilisable tant pour la police que pour le COC, comme par exemple la notion de "dans des circonstances spécifiques, ...". L'Exposé des motifs parle d'ailleurs à juste titre de la "*spécificité des banques de données particulières*", ce qui est plus correct que leur prétendu caractère exceptionnel. Pour le reste, les besoins particuliers prévus au § 2 restent d'application.

Dans le paragraphe 3 modifié, la déclaration préalable de la banque de données particulière au COC est abrogée, avec la justification sommaire que *"ceci ne correspond plus au système établi par la loi relative à la protection des données*". Cependant, ni la Directive Police et Justice, ni le titre 2 de la LPD n'interdisent d'instaurer un système d'avis préalable pour certaines banques de données. Le système de consultation préalable de l'autorité de contrôle tel que prévu à l'article 58 et à l'article 59 de la LPD (à savoir lorsqu'un traitement présente probablement un risque élevé pour les droits et libertés de personnes physiques, en combinaison avec les conditions telles que prévues à l'article 59 de la LPD) ne peut être comparé au système existant de déclaration préalable de la LFP et à l'avis consécutif du COC. Quoi qu'il en soit, le COC a l'intention de suivre cela de près via l'application de l'article 59, § 2[14]. Pour l'Organe de contrôle, **toutes** les banques de données particulières sont en principe des traitements pour lesquels une consultation préalable est nécessaire.

Néanmoins, dans le cadre de la simplification administrative en faveur des services de police et de l'Organe de contrôle (qui lui-même ne peut plus tenir de registre), le COC peut se retrouver dans un accès via le registre des traitements des services de police comme établi dans le nouveau projet d'article 145 de la LPI. Il doit alors être clair que ledit registre doit contenir toutes les données que la déclaration actuelle au COC contient, ce qui n'est pas le cas à première vue. L'Organe de contrôle a vu une première démonstration du registre par la police fédérale et il est apparu d'emblée que les informations qui s'y trouvent sont trop sommaires que pour permettre à l'Organe de contrôle de réaliser une (première) évaluation en connaissance de cause (autrement dit, sans devoir vérifier sur place dans la banque de données).

**13.** À l'article 44/11/3ter, § 1 de la LFP, qui comporte une description des services/organismes qui ont un accès direct aux banques de données communes, cet accès fait défaut à l'heure actuelle, tant pour le COC que pour le Comité permanent R. Chez le gestionnaire de la banque de données, à savoir la

---

[14] "*L'autorité de contrôle compétente peut établir une liste des opérations de traitement devant faire l'objet d'une consultation préalable conformément au paragraphe 1.*"

police fédérale, on débat sur la question de savoir s'il y a actuellement une base juridique pour les deux instances de contrôle pour disposer d'un accès direct. Il incombe en effet à la police fédérale de veiller au niveau technique à ce que cet accès soit donné.

Pour le COC, cette base juridique est limpide étant donné qu'au § 1, 1e alinéa, il est littéralement question d'un accès pour "*l'organe*", qui ne peut viser ici que le COC. Étonnamment toutefois, le Comité R n'y est pas repris, une erreur manifestement. Quoi qu'il en soit, l'occasion est idéale pour faire la clarté et pour prévoir expressément l'accès direct, tant pour le COC que pour le Comité permanent R. Cela peut se faire soit dans cet article, soit dans le projet d'article 44/11/3quinquies/2 de la LFP. Le fait que les deux organes de contrôle aient besoin d'un tel accès direct ne peut être mis en doute. Un contrôle sérieux n'est possible que si l'autorité de contrôle dispose du même accès que les services de base. Tant le RGPD que la Directive Police et Justice prévoient d'ailleurs que l'autorité de contrôle doit disposer de "*pouvoirs d'enquête effectifs*". Le COC a d'ailleurs déjà un accès direct à la BNG. Le COC préfère clairement une disposition spécifique expresse dans le projet d'article 44/11/3quinquies/2 de la LFP, où l'on pourrait insérer l'alinéa suivant entre le 1e et le 2e alinéa (qui deviendrait le 3e alinéa) : "*Sur la base du besoin d'en connaître, tout ou partie des données à caractère personnel et des informations des banques de données communes sont directement accessibles à tout moment à l'Organe de contrôle et au Comité permanent de contrôle des services de renseignements. Le gestionnaire assure la mise en place de l'accès direct précité.*"

À cet égard, le début dudit article et notamment les termes "*Dans le respect de l'exercice de leurs missions respectives*", manquent de clarté. Les deux autorités de contrôle peuvent exercer leurs compétences respectives (reprises dans la LPD pour le COC et dans la loi du 18 juillet 1991 pour le Comité R) lors du contrôle des banques de données communes. Il conviendrait de le formuler comme suit : "*le contrôle du traitement des informations et des données à caractère personnel contenues dans les banques de données visées à l'article 44/2, § 2 est assuré, conformément à leurs compétences prévues respectivement dans la loi relative à la protection des données et dans la loi du 18 juillet 1991 du contrôle des services de police et de renseignement et de l'Organe de coordination pour l'analyse de la menace, par l'Organe de contrôle et le Comité permanent de contrôle des services de renseignements tel que visé à l'article 28 de la loi précitée du 18 juillet 1991*".

Par souci d'exhaustivité, l'Organe de contrôle souhaite faire remarquer que les références à "L'Organe" à l'article 44/11/3ter, § 4 et à l'article 44/11/3quater reposent manifestement sur une erreur. La référence à l'Organe de contrôle doit être supprimée dans cette disposition. L'Organe de contrôle constate enfin que l'actuel article 44/11/3quinquies de la LFP n'est pas modifié par le projet bien que son 2e alinéa renvoie encore à la loi du 8 décembre 1992 *relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel* qui a entre-temps été abrogée. L'auteur du projet se devra d'adapter cette disposition au nouveau cadre législatif en vigueur.

**14.** Dans la version néerlandaise du projet d'article 44/11/8bis (article 21 de l'avant-projet), aussi bien à l'alinéa 1 qu'à l'alinéa 2, les termes "*veiligheidsdiensten*" doivent être remplacés par les termes "*inlichtingen- en veiligheidsdiensten*". Cette disposition doit quoi qu'il en soit être lue conjointement avec le projet modifié d'article 44/11/12 (article 23 de l'avant-projet).

De manière plus fondamentale, le COC constate avant tout un manque de réciprocité équivalente dans les accès que l'on veut octroyer réciproquement aux banques de données respectivement des services de police et des services de renseignement. Alors que les services de renseignement obtiendraient la forme la plus aboutie de communication d'informations policières via un accès direct, le mouvement inverse, à savoir un accès (direct) pour les services de police aux banques de données des services de renseignement resterait dans le flou et serait relégué à un "*protocole d'accord*" qui doit entrer en

vigueur simultanément avec celui de l'accès direct à la BNG au profit des services de renseignement. Le renvoi aux articles 19 et 20 de la loi organique des services de renseignement et de sécurité[15] du 30 novembre 1998 est également très peu explicite. Ainsi, le projet semble vouloir accorder davantage de protection/cloisonnement à l'information des services de renseignement qu'aux informations policières. Indépendamment du fait que l'on ne trouve aucune justification de ce choix dans l'Exposé des motifs, le COC s'interroge sérieusement à cet égard. L'échange d'informations plus performant propagé dans l'Exposé des motifs, qui a en effet été recommandé par la Commission d'enquête parlementaire attentats, n'est manifestement valable que dans un seul sens principalement (de la police vers les services de renseignement). Par ailleurs, le 1e alinéa fait double emploi avec l'article 14 de la LRS.

Laisser fixer les modalités de communication des données (à noter que le terme "*données*" est aussi bien plus vague que le mouvement inverse où "*des données à caractère personnel et des informations*" seraient directement accessibles pour les services de renseignement) dans un protocole d'accord est quoi qu'il en soit contraire au principe de légalité et à l'article 22 de la Constitution[16]. Étant donné que le COC n'a aucune idée de ces modalités (s'agit-il aussi d'un accès direct, uniquement d'une consultation ou d'une communication ponctuelle quelque peu structurée ?), il n'est pas en mesure d'évaluer correctement ledit flux de données vers la police. L'Exposé des motifs n'apporte pas plus de clarté sur ce point.

---

[15] Ci-après "LRS".

[16] De nombreux arrêts de la Cour constitutionnelle indiquent comment il convient de comprendre cela. À cet égard, on peut de nouveau se référer à l'arrêt 29/2018 (Considérants B 13.1 et B 13.2) et à toutes les références à la jurisprudence de la Cour européenne des droits de l'homme et de la Cour de justice qui y sont énumérées) : "*En réservant au législateur compétent le pouvoir de fixer dans quels cas et à quelles conditions il peut être porté atteinte au droit au respect de la vie privée, l'article 22 de la Constitution garantit à tout citoyen qu'aucune ingérence dans l'exercice de ce droit ne peut avoir lieu qu'en vertu de règles adoptées par une assemblée délibérante, démocratiquement élue.*
*Une délégation à un autre pouvoir n'est toutefois pas contraire au principe de légalité pour* ***autant que l'autorisation soit définie de manière suffisamment précise et porte sur l'exécution de mesures dont les éléments essentiels sont fixés préalablement par le législateur****.*

*Outre l'exigence de légalité formelle, l'article 22 de la Constitution impose également que l'ingérence dans l'exercice du droit au respect de la vie privée soit* ***définie en des termes clairs et suffisamment précis qui permettent d'appréhender de manière prévisible les hypothèses dans lesquelles le législateur autorise une pareille ingérence****.*

*De même, l'exigence de prévisibilité à laquelle la loi doit satisfaire pour être jugée conforme à l'article 8 de la Convention européenne des droits de l'homme implique que sa formulation soit assez précise pour que chacun puisse - en s'entourant au besoin de conseils éclairés - prévoir, à un degré raisonnable, dans les circonstances de la cause, les conséquences d'un acte déterminé (CEDH, grande chambre, 4 mai 2000, Rotaru c. Roumanie, § 55 ; grande chambre, 17 février 2004, Maestri c. Italie, § 30). La législation doit donner à chacun une* ***indication suffisante sur les circonstances dans lesquelles et à quelles conditions elle habilite la puissance publique à recourir à des mesures*** *affectant les droits protégés par la Convention (CEDH, grande chambre, 12 juin 2014, Fernández Martínez c. Espagne, § 117).*

*Plus particulièrement, lorsque l'intervention de l'autorité présente un caractère secret, la loi doit offrir des garanties suffisantes contre les ingérences arbitraires dans l'exercice du droit au respect de la vie privée,* ***en délimitant le pouvoir d'appréciation des autorités concernées avec une netteté suffisante****, d'une part, et en prévoyant des procédures qui permettent un contrôle juridictionnel effectif, d'autre part (CEDH, grande chambre, 4 mai 2000, Rotaru c. Roumanie, § 55 ; 6 juin 2006, Segerstedt-Wiberg c. Suède, § 76 ; 4 juillet 2006, Lupsa c. Roumanie, § 34).*

En ce moment, les services de renseignement disposent déjà d'une base juridique pour une interrogation directe de la BNG, et ce depuis avril 2014. Mais pour des raisons que le COC ignore, ce n'est pas appliqué en pratique. C'est ce que reconnaît l'Exposé des motifs, bien que de manière implicite, qui précise que l'échange d'informations est à présent réalisé "*par des mécanismes ad hoc au travers de relais formels ... ou de contacts ponctuels entre enquêteurs dans des dossiers concrets ... ou à l'occasion de plateformes de travail (comme entre autres, les LTF et les groupes de travail du Plan R) ou via les mécanismes d'assistance technique ou d'accords informels pris sur la transmission systématique de certains documents sous format mail ..., mais souvent aussi à la demande d'un enquêteur des services de renseignements ...*" (p. 31). On ne sait donc pas clairement si le système existant d'interrogation directe de la BNG via une fonction "*hit no hit*" pour les services de renseignement est insuffisant et dans l'affirmative, pourquoi ce le serait. Par souci de clarté, une interrogation directe de la BNG permet déjà énormément de choses. Elle permet aux services de renseignement, en vertu de l'article 44/11/4, § 3 de la LFP, de disposer d'un accès direct "*à tout ou partie des données suivantes :*
*a) l'existence de données sur une personne en application de l'article 44/5, § 1er, alinéa 1er, 2° à 6°, et § 3, 1° à 9° ;*
*b) la qualification retenue par la police concernant les faits pour lesquels la personne est enregistrée ;*
*c) les données nécessaires pour obtenir plus d'informations auprès de l'autorité compétente ; et*
*d) les données relatives aux mesures à prendre pour les personnes visées au point a)*", sur la base de quoi les services de renseignement peuvent prendre contact avec le service de police – ou le fonctionnaire - concerné pour obtenir des informations encore plus détaillées.

Avant même qu'il soit établi clairement ou du moins de manière acceptable que l'interrogation directe ne permettrait pas aux services de renseignement de réaliser leurs missions correctement, ni pour quelle raison ces possibilités ne sont manifestement pas exploitées en pratique, la BNG est **entièrement** "ouverte" aux services de renseignement par une consultation directe. Contrairement à ce que l'Exposé des motifs semble affirmer, cette extension est bel et bien très importante et place les services de renseignement en tant qu'organes exécutifs au même rang que les autorités administratives et judiciaires et les organes de contrôle indépendants. Pour l'OCAM, il semble y avoir moins d'objections parce que l'OCAM n'est pas un service de renseignement avec des compétences opérationnelles. Une consultation directe permet quoi qu'il en soit aux services de renseignement de prendre connaissance de tous les antécédents policiers et judicaires d'une personne concernée, même de ceux qui n'ont absolument rien à voir (par exemple des faits de mœurs purs, des faux de droit commun, des infractions routières, la fraude fiscale et sociale ordinaire, etc.) avec les compétences des services de renseignement, et ce sans appliquer le moindre filtre, ce qui n'est pas le cas lors de l'interrogation directe en vigueur actuellement. Le fait que l'accès soit "limité" à certains agents des services de renseignement qui sont titulaires d'une habilitation du degré très secret n'enlève rien à ce constat. La toute grande majorité des membres des services de renseignement disposent d'une telle habilitation et les possibilités d'accès direct à la BNG vaudront pour la toute grande majorité de ces membres du personnel (aussi bien les services extérieurs que les services d'analyse).

Pour l'Organe de contrôle, tout cela est contraire au principe de proportionnalité et de finalité, à l'article 22 de la Constitution (lu en combinaison ou non avec l'article 8 de la CEDH, l'article 17 du Pacte DCP et les articles 7 et 8 de la Charte européenne des droits fondamentaux) et est encore moins de nature à "*préserver la présomption d'innocence et le droit au respect de la vie privée*", dont question dans l'Exposé des motifs.

Par souci d'exhaustivité, le COC souligne que l'accès direct envisagé pour les services de renseignement est bien limité à la BNG. En ce sens, le passage de l'Exposé des motifs indiquant "***dont*** *celles figurant*

*dans la BNG*" prête à confusion. Pour une bonne compréhension, il incombe d'ailleurs à l'auteur du projet de clarifier les choses. S'agit-il de l'accès direct envisagé ou encore d'autres banques de données en dehors de la BNG et des banques de données techniques ?

**15.** Les modifications envisagées de l'article 44/11/9, § 1 de la LFP s'inscrivent dans le prolongement des modifications prévues à l'article 44/11/8 et au nouvel article 44/11/8bis de la LFP.

Au 2e paragraphe, le présent avant-projet est toutefois l'occasion de transposer l'arrêt 108/2016 du 14 juillet 2016 de la Cour constitutionnelle dans le texte légal en faisant suivre le terme "avis" du terme "***contraignant***" afin que le texte de ce paragraphe devienne : *"§ 2. Après avis **contraignant** de l'Organe de contrôle, elles peuvent également être communiquées aux autorités publiques belges, organes ou organismes publics ou d'intérêt public chargés par la loi de l'application de la loi pénale ou qui ont des missions légales de sécurité publique lorsque ceux-ci en ont besoin pour l'exécution de leurs missions légales.*" De la sorte, on donne suite à l'arrêt précité qui indiquait notamment ce qui suit au sujet de cette disposition en ce qui concerne la communication de données à caractère personnel des banques de données policières aux autorités publiques/organes/institutions belges :

*"Bien que l'article 44/11/9, § 2 de la loi sur la fonction de police prévoie qu'une telle communication n'est possible qu'après avis de l'Organe de contrôle de l'information policière, il ne ressort pas de cet article si l'avis est contraignant ou non. Dans la mesure où l'avis ne serait pas contraignant, la disposition attaquée pourrait donner lieu à des communications de données à caractère personnel provenant des banques de données policières qui, de l'avis de cet Organe de contrôle, ne sont pas conformes aux dispositions de la loi attaquée, par exemple parce que l'autorité qui demande la communication des données à caractère personnel n'a pas besoin de ces données pour l'exécution de sa mission légale et ne justifie ainsi pas du "besoin d'en connaître" (voy. les travaux préparatoires reproduits en B.98.4.4). Dans l'interprétation précitée, l'article 44/11/9, § 2 de la loi sur la fonction de police causerait une ingérence disproportionnée dans l'exercice du droit au respect de la vie privée."*

*"Ce n'est que dans la mesure où l'avis de l'Organe de contrôle est considéré comme contraignant pour les autorités qui sont compétentes pour communiquer des données à caractère personnel provenant des banques de données policières aux autorités, organes et organismes visés dans l'article 44/11/9, § 2, que cet article n'a pas d'effet disproportionné au regard des objectifs du législateur. Sous réserve de cette interprétation, cet article est compatible avec les dispositions constitutionnelles et conventionnelles mentionnées en B.7"* (considérants B. 99.3.3 en B.99.3.4). Le terme "avis" a donc le sens d' "autorisation" ou d' "avis contraignant". Le COC exhorte l'auteur du projet à donner suite à l'arrêt précité de la Cour constitutionnelle.

**16.** La modification technique de l'article 44/10/10 (article 22 de l'avant-projet) de la LFP est l'occasion pour le COC d'attirer l'attention sur la problématique actuellement très préoccupante de la communication de données à caractère personnel policières à des institutions pour la recherche scientifique ou à des chercheurs d'instituts scientifiques, une communication entourée d'une très grande insécurité juridique. À ce sujet, l'avis COC-CONTROLE-002-2018 du 23 octobre 2018 a été remis à l'auteur du projet. Ladite disposition prévoit qu'un arrêté royal, après avis (à l'avenir) de l'Organe de contrôle, précisera les institutions ou personnes auxquelles peuvent être communiquées les données à caractère personnel qui sont nécessaires pour accomplir les missions d'intérêt public liées à la recherche scientifique qui leur sont confiées par ou en vertu d'une loi, d'un décret ou d'une ordonnance. Cet arrêté devra également préciser les modalités de cette communication.

Cette disposition, qui est entrée en vigueur le 7 avril 2014, n'a jamais été exécutée jusqu'à présent, de sorte qu'au sens strict, on ne peut pas transmettre des données policières aux chercheurs d'universités ou de hautes écoles, ce qui pose bien entendu des problèmes majeurs pour la recherche scientifique

de même que pour les services de police. Actuellement, on peut se tirer d'affaire par le biais d'autorisations ponctuelles du ministère public compétent, pour autant que les données policières se trouvent sur le procès-verbal et fassent donc partie d'un dossier pénal. Si tel n'est toutefois pas le cas, par exemple s'il s'agit de données sur les patrouilles, les lieux d'interventions et les types d'interventions, etc., un véritable problème juridique se pose. Le COC a déjà été interrogé à ce sujet par exemple par l'Université de Gand, qui veut réaliser au sein de la zone de police d'Anvers – et à la demande de cette dernière – une recherche scientifique sur les possibilités et limitations du concept appelé "predictive policing", nécessitant une multitude de données policières, dont des données à caractère personnel. À défaut d'arrêté d'exécution, de telles recherches sont soumises à de grandes incertitudes ou la police refuse de fournir ces données du fait que l'existence d'un fondement juridique suffisant n'est pas garantie.

Cette absence d'arrêté d'exécution est d'autant plus singulière que, pour d'autres services de sécurité, comme par exemple les services de renseignement ou l'OCAM, la LPD a bel et bien prévu un règlement spécifique pour l'utilisation des données traitées par ces institutions à des fins scientifiques. Il convient en effet de se référer au chapitre X ("*Traitement de données à caractère personnel à des fins historiques, scientifiques ou statistiques*") du sous-titre 1 (les articles 99 à 104 inclus), du sous-titre 3 (les articles 132 à 137 inclus) et du sous-titre 4 (les articles 162 à 167 inclus) du titre III de la LPD qui ont prévu à cet égard un règlement propre pour une telle communication de données à caractère personnel. La responsabilité de cette communication repose ainsi sur les services respectifs en tant que responsable du traitement. De toute évidence, il n'est pas logique que le cadre juridique actuel ne prévoie pas ces possibilités pour les données policières qui sont généralement bien plus demandées dans le monde scientifique.

Une autre option éventuelle consiste à ce que le COC émette un avis contraignant dans lequel il lui appartiendrait d'évaluer la légalité (finalité, limitation de données, sécurité de l'information, etc.) et la proportionnalité de la communication de données policières au(x) chercheur(s). Cela s'inscrirait d'emblée dans le prolongement de la compétence du COC (et est similaire à celle-ci) prévue dans l'article 44/11/9, § 2 de la LFP abordé ci-avant. Dans ce cas, un arrêté royal n'est plus nécessaire.

### III.2. Modifications de la loi du 7 décembre 1998 relative à la police intégrée

**17.** L'Organe de contrôle est très positif à l'égard de la création du Comité d'avis en charge de la stratégie en matière d'information (Comité Information et ICT). Il doit être en mesure d'apporter aide et conseils au responsable du traitement et aux sous-traitants de la police intégrée en ce qui concerne les nombreux thèmes, questions ou points de discussion souvent difficiles qui se présentent pour les différentes entités policières et leurs responsables. Il doit être en mesure d'agir en tant que premier intervenant pour le compte de la police afin de trouver des solutions et apporter des réponses pour ce qui se passe sur le terrain au sujet des thèmes vie privée, protection des données, gestion de l'information, technologies de l'information et sécurité de l'information, sans préjudice évidemment de leur propre responsabilité et de celle des délégués à la protection des données respectifs. Le COC ne peut en effet que constater qu'il reçoit déjà actuellement de très nombreuses questions qui devraient être traitées dans une première phase par le responsable du traitement lui-même. À l'avenir, ils pourront s'adresser au préalable à ce nouveau Comité Information et ICT qui devra également tenter de dégager des solutions et visions uniformes pour l'ensemble de la police intégrée.

Le projet souhaite confier au Comité Information et ICT une compétence particulière : un rapport annuel sur la mise en œuvre des règles de ventilation. Le COC salue cette mission, qui rejoint aussi ses remarques formulées ci-dessus au point 10 et qui s'inscrit dans le prolongement de la préoccupation du Gouvernement quant à l'exécution des règles d'effacement et d'archivage, telle qu'elle ressort de la notification au Conseil des ministres.

Dans le deuxième paragraphe, l'Organe de contrôle part du principe que, bien que cela ne ressorte pas explicitement de l'Exposé des motifs, au point c) toute une série de questions juridiques – ou du moins les plus essentielles ou les plus fondamentales – peuvent aussi être saisies. Ici aussi, le COC doit souvent répondre que l'Organe de contrôle n'a pas pour but (le COC n'est pas le conseiller juridique de l'ensemble de la police intégrée), ni forcément la capacité de réagir à toutes sortes de questions ou remarques ou d'émettre un avis. Ce type de questions doivent être abordées selon un système de cascade : en premier lieu, le responsable du traitement doit développer une réponse (avec son DPO) ; ensuite, on pourrait s'adresser au nouveau Comité Information et ICT et seulement en dernier lieu, à l'Organe de contrôle qui peut alors s'exprimer en connaissance de cause (il peut alors prendre connaissance de la vision du responsable du traitement, du DPO et/ou du Comité Information et ICT).

L'Organe de contrôle souhaite enfin être informé de tous les avis émis par le Comité Information et ICT. Pour être en mesure d'exercer ses missions d'autorité de contrôle de manière qualitative, il est évidemment primordial d'être et de rester informé de la vision, des initiatives et des points de vue de la police intégrée et de ses autorités de tutelle.

**18.** Le titre V de la LPI, actuellement abrogé, est rétabli avec une série de dispositions portant sur certaines modalités des traitements de données. Le projet d'article 144 de la LPI (article 30 de l'avant-projet) introduit l'obligation, pour chaque zone de police, le commissariat général, toute direction générale et direction de la police fédérale, de désigner un délégué à la protection des données (DPO) et exécute ainsi l'article 37 de la LPD et l'article 63 du RGPD et il impose une obligation similaire aux sous-traitants qui travaillent avec les responsables du traitement de la police.

Le COC demande qu'au 4e paragraphe du projet d'article 144, l'avis du COC soit rendu obligatoire dans l'élaboration de l'arrêté d'exécution qui y est visé.

**19.** Le projet d'article 145, qui crée la base légale pour un registre électronique des traitements, ne précise pas s'il sera imposé obligatoirement à toutes les zones de police et entités de la police fédérale. Il semblerait que l'on puisse déduire implicitement de l'Exposé des motifs que le but est d'en faire une obligation. Pour le COC, il est préférable d'inscrire d'emblée l'obligation légale à l'article 145.

De nouveau, le COC demande que dans le projet d'article 145, l'avis de l'Organe de contrôle soit rendu obligatoire dans l'élaboration de l'arrêté d'exécution qui y est visé, lequel fixera la forme et les modalités du registre.

**20.** Le projet d'article 146 est une application de l'article 9.2 de la Directive Police et Justice. La disposition est toutefois très générale. L'Organe de contrôle propose de se référer à l'article 29 de la LPD : "*Conformément aux conditions de l'article 29 de la LPD, les responsables du traitement communiquent ...*"

**21.** Le projet d'article 147 (article 33 de l'avant-projet) prévoit aussi, pour les demandes d'accès dans les matières du RGPD où il est question d'un traitement de données qui avait été réalisé initialement par la police en application du titre 2 de la LPD, un accès indirect dans l'exercice des droits via l'Organe de contrôle. Cet article se situe dans le même esprit que l'article 14, § 6 de la LPD où le COC a tout autant une responsabilité dans les demandes d'exercice des droits de la personne concernée auprès

d'une autorité qui relève du titre 1 de la LPD/du RGPD et qui concernent des informations qui ont été traitées initialement par les services de police (dans le cadre de leurs missions opérationnelles). Le 2e alinéa du 1e paragraphe semble être superflu et faire double emploi avec l'article 14, § 2 de la LPD.

En l'espèce, il n'est pas précisé quelle information le COC peut/doit communiquer dans ce cas à la personne concernée. À l'article 14, § 6, 2e alinéa de la LPD évoqué ci-avant, on affirme que lorsque l'APD a été saisie par la personne concernée, après réception de la réponse de l'Organe de contrôle, l'APD informe la personne concernée "*selon les modalités légales prévues*". On ne précise pas quelles sont ces modalités. Quoi qu'il en soit, à défaut de description plus détaillée, le COC aura la responsabilité d'évaluer quelles informations peuvent être communiquées. C'est par ailleurs la solution que préfère l'Organe de contrôle. La seule mention du fait "*qu'il a été procédé aux vérifications nécessaires*", comme prévu par le titre 2 (article 42 de la LPD) génère très souvent une incompréhension totale chez la personne concernée.

De manière plus générale, il convient d'ailleurs de remarquer que l'article 41 de la LPD n'instaure pas d'emblée un système d'accès indirect, même si on en est parfois manifestement convaincu sur le terrain. Cet article dispose en effet que : "*la loi, le décret ou l'ordonnance, peut prévoir que les droits de la personne concernée sont exercés par l'intermédiaire de l'autorité de contrôle compétente*". Bien que cette disposition puisse être lue dans le sens où, par "loi", on viserait aussi la LPD elle-même, il ne semble pas que telle était l'intention du législateur. Dans l'Exposé des motifs de la LPD, l'intention de l'article 41 de la LPD est en effet motivée comme suit : "*Il s'agit de laisser le système de l'accès indirect* ***une option pour les autorités qui le souhaitent.*** *Il est également prévu que* ***lorsqu'il*** *est fait application de l'accès indirect, la demande se fait via l'autorité de contrôle compétente.*"[17] Le fait que cet article 42 dispose que la demande doit être adressée au COC est la simple mise en œuvre de l'article 17, 1e alinéa de la Directive Police et Justice. Il convient donc de mettre fin à cette imprécision dans la LFP.

**22.** Enfin, l'Organe de contrôle comprend parfaitement que les dispositions ambitieuses concernant la journalisation ne puissent pas toutes entrer en vigueur immédiatement. Il s'agit de la journalisation concernant les traitements dans la BNG, dans les archives de la BNG, dans les banques de données de base et dans les banques de données particulières. Le renvoi, à l'article 34 de l'avant-projet, à l'article 279 de la LPD est probablement une erreur ; on vise incontestablement l'article 284 de la LPD. En ce qui concerne toutefois les traitements dans la BNG, l'Organe de contrôle ne voit aucune bonne raison de ne pas faire entrer en vigueur immédiatement la conservation des fichiers de journalisation pendant 30 ans. Les fichiers de journalisation de la BNG sont d'ores et déjà conservés de sorte que l'on ne comprend pas pourquoi un report à 2023 serait encore nécessaire.

[17] Doc. Parl. Chambre 2017-2018, 54-3126/001, 84. Marquage propre.

**PAR CES MOTIFS,**

**l'Organe de contrôle de l'information policière**

**demande**

- **de donner suite aux remarques reprises aux points 3 à 6 inclus, 8, 9, 12 à 16 inclus et 18 à 21 inclus**
- **de tenir compte des remarques susmentionnées aux points 10, 11, 17 et 22**

Avis approuvé par l'Organe de contrôle de l'information policière le 12 décembre 2018.

Pour l'Organe de contrôle,

le Président,

(sé.) Philippe ARNOULD

p.o. Frank Schuermans

Membre-conseiller