**ORGANE DE CONTRÔLE DE L'INFORMATION POLICIÈRE**

| Votre référence | Notre référence | Annexe(s) | Date |
|---|---|---|---|
| | DA240032 | | 23.10.2024 |

**<u>Objet :</u> Avis relatif à un projet de directive commune et contraignante des Ministres de la Justice et de l'Intérieur relative à l'interconnexion des banques de données de base dénommées ISLP via l'outil PoliceSearch@GPI (GPI 105).**

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 59 §1er, 2e alinéa, l'article 71 et le Titre 7, en particulier l'article 236.

Vu la loi du 3 décembre 2017 portant création de l'Autorité de protection des données (ci-après 'la LAPD'), et en particulier l'article 4 §2, 4e alinéa.

Vu la loi du 5 août 1992 sur la fonction de police (ci-après 'la LFP').

Vu la *Law Enforcement Directive* 2016/680 du 27 avril 2016 (ci-après 'la *LED*').

Vu la demande des Ministres de la Justice et de l'Intérieur, reçue par l'Organe de contrôle le 27 août 2024, en vue d'émettre un avis sur un projet de directive commune et contraignante des Ministres de la Justice et de l'Intérieur relative à l'interconnexion des banques de données de base dénommées ISLP via l'outil PoliceSearch@GPI (GPI 105).

Vu l'avis du 12 décembre 2022 de l'Organe de contrôle de l'information policière relatif à l'analyse d'impact relative à la protection des données de PoliceSearch@GPI, non publié.

Vu le rapport de Monsieur Ronny Saelens, Membre-conseiller *a.i.* de l'Organe de contrôle.

Émet, le 23 octobre 2024, l'avis suivant.

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

**1.** 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 remanié en profondeur les tâches et missions de l'Organe de contrôle. L'article 4 §2, quatrième alinéa de la loi du 3 décembre 2017 portant création de l'Autorité de protection des données (ci-après 'la LAPD') dispose qu'à l'égard des 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 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 compétent également 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 socioéconomiques ou de traitements relevant de la gestion des ressources humaines. L'Organe de contrôle doit être consulté lors de la préparation de la législation ou d'une mesure réglementaire ayant trait au traitement de données à caractère personnel par les services de police de la police intégrée (voir les articles 59 §1er, 2e alinéa et 236 §2 de la LPD, l'article 36.4 du RGPD et l'article 28.2 de la directive Police-Justice). L'Organe de contrôle a dans ce contexte pour mission d'examiner si l'activité de traitement projetée par les services de police est conforme aux dispositions du Titre 1er (pour les traitements non opérationnels)[3] et du Titre 2 (pour les traitements opérationnels) de la LPD[4]. De plus, le COC est aussi chargé d'émettre des avis d'initiative, comme prévu à l'article 236 §2 de la LPD, et est investi conformément à l'article 240 de la LPD d'une mission générale d'information à l'égard du grand public, des personnes concernées, des responsables du traitement et des sous-traitants dans le domaine du droit à la protection des données et à la protection de la vie privée.

**2.** En ce qui concerne en particulier les activités de traitement dans le cadre des missions de police administrative et/ou judiciaire, l'Organe de contrôle émet dès lors des 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 matière ayant trait à la gestion de l'information policière telle que régie par la Section 12 du Chapitre 4 de la loi sur la fonction de police[5].

**3.** Par ailleurs, l'Organe de contrôle est également chargé, à l'égard des services de police, de l'inspection générale de la police fédérale et de la police locale (en abrégé 'AIG') visée dans la loi du

---

[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 dénommée « directive Police-Justice » ou *Law Enforcement Directive* (*LED*)).

[3] Article 4 §2, 4e alinéa de la LAPD.

[4] Article 71 §1er, 3e alinéa de la LPD.

[5] Articles 59 §1er, 2e alinéa et 236 §2 de la LPD.

15 mai 2007 sur l'Inspection générale et de l'Unité d'information des passagers (ci-après dénommée en abrégé 'BELPIU') visée au Chapitre 7 de la loi du 25 décembre 2016, de la surveillance de l'application du Titre 2 de la LPD et/ou 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, et/ou de toute autre mission qui lui est confiée en vertu ou par d'autres lois[6].

**4.** L'Organe de contrôle est compétent à l'égard du Service Contentieux de l'Administration générale des Douanes et Accises en ce qui concerne les réquisitions adressées par ce service à la BELPIU dans des matières fiscales, et ce en vertu de l'article 281 §4 de la loi générale *« sur les douanes et accises »* du 18 juillet 1977, telle que modifiée par la loi du 2 mai 2019 *« modifiant diverses dispositions relatives au traitement des données des passagers »*.

**5.** Enfin, l'Organe de contrôle est également chargé, dans le cadre de la législation sur la rétention des données et en vertu de l'article 126/3 §1er, 8e alinéa de la loi du 13 juin 2005 relative aux communications électroniques (ci-après 'la LCE'), telle que modifiée par la loi du 20 juillet 2022 relative à la collecte et à la conservation des données d'identification et des métadonnées dans le secteur des communications électroniques et à la fourniture de ces données aux autorités (*M.B.* du 8 août 2022), de la validation des statistiques relatives au nombre de faits punissables et au délai de conservation pour chaque arrondissement judiciaire et chaque zone de police, une matière dans le cadre de laquelle il exerce toutes les compétences qui lui ont été attribuées par le Titre 7 de la loi du 30 juillet 2018. Il est par ailleurs également chargé, en application de l'article 42 §3, 2e et 3e alinéas de la LFP, du contrôle des requêtes de la Cellule Personnes disparues de la police fédérale en vue de la consultation des données relatives aux communications électroniques impliquant la personne disparue.

**6.** L'Organe de contrôle est compétent pour rendre des avis sur les aspects ayant trait au traitement des informations et des données à caractère personnel et à la protection de la vie privée par le traitement de données à caractère personnel pour autant qu'il existe un rapport avec le fonctionnement opérationnel et non opérationnel des services de police et/ou avec le personnel de la police intégrée (ci-après 'la GPI[7]') et/ou pour autant que le projet de texte soumis pour avis ait un impact sur la gestion de l'information policière en général.

**7.** Par ailleurs, l'Organe de contrôle n'est pas seulement une autorité de protection des données, mais est aussi une autorité de contrôle qui est légalement chargée de contrôler la légalité, l'efficacité, l'efficience et l'économie de la gestion de l'information policière[8].

---

[6] Article 71 §1er, troisième alinéa *juncto* article 236 §3 de la LPD.
[7] Geïntegreerde politie – Police Intégrée.
[8] Rapport d'activité 2021, www.organedecontrole.be, voir les points 3 et 52 et plus spécifiquement le point 71 : *« Il serait cependant faux de s'imaginer que le COC se préoccupe seulement de la protection des données ; il porte aussi énormément d'attention à tous les autres aspects opérationnels de la gestion de l'information policière et des informations des autres services qu'il contrôle, s'agissant là de matières relevant également de sa compétence. »* ; article 71 §1er de la LPD.

## II. Objet de la demande et antécédents

**8.** Le projet de directive commune et contraignante des Ministres de la Justice et de l'Intérieur (ci-après 'le projet de directive') a pour but de remédier à la situation actuelle où les banques de données de base des services de police sont séparées les unes des autres sans qu'il y ait de ponts technologiques entre elles. Comme le soulève le projet de directive, les zones de police et les entités de la Direction générale de la police administrative disposent chacune de leurs propres banques de données de base (locales), dénommées ISLP (*Integrated System for the Local Police*), qui ne sont pas reliées entre elles, de sorte que les données policières (informations et données à caractère personnel) ne sont pas directement accessibles pour les autres unités de police[9]. L'« outil »/application PoliceSearch@GPI a été développé(e) afin de rendre les données policières des différents ISLP directement accessibles pour la police intégrée (GPI[10]).

**9.** Comme on peut le lire dans le projet de directive[11], une analyse d'impact relative à la protection des données a été réalisée et l'Organe de contrôle a été consulté en application de l'art. 59 §1 LPD. L'Organe de contrôle a à cette occasion formulé un certain nombre de recommandations dans son avis du 12 décembre 2022[12], et constate que le projet de directive en tient compte[13].

## III. Remarques

**10.** Selon les auteurs du projet de directive, l'outil 'PoliceSearch@GPI' représente un pas important dans le sens de la mise en œuvre d'une recommandation de la commission d'enquête parlementaire sur les attentats terroristes du 22 mars 2016 visant à *« remédier au cloisonnement de l'information et donc à l'absence de partage des informations »*[14]. Selon les auteurs, *« la commission d'enquête parlementaire plaide clairement pour un changement de culture »*, notamment en ce sens que nous devons *« remplacer le principe du « besoin de savoir » par celui du « besoin de partager » (…) »*[15] (soulignement du COC).

**11.1.** L'idée que la commission d'enquête susmentionnée aurait préconisé de *« **remplacer** »* ce principe (*« vervangen »*) doit toutefois être fortement nuancée et mise en perspective. Le premier principe évoqué ne fait en effet pas obstacle au deuxième, comme en atteste d'ailleurs aussi le point 3.3 du projet de directive. C'est pour cette raison que la commission d'enquête pose 'clairement' qu'un

[9] Projet de directive, p. 2.
[10] Geïntegreerde politie – Police Intégrée.
[11] Projet de directive, p. 7.
[12] Avis DI220014 du 12.12.2022 sur l'analyse d'impact relative à la protection des données concernant *Police Search* GPI, non publié. (traduction libre)
[13] Comme en atteste le projet de directive, p. 7-8.
[14] Projet de directive, p. 2.
[15] Projet de directive, p. 3, faisant référence au rapport parlementaire de cette commission d'enquête : Doc. Parl. *Chambre* 2016-2017, n° 54-1752/008, 258.

équilibre doit être recherché entre les deux principes[16]. L'interprétation des auteurs du projet est par ailleurs d'autant plus étrange que contrairement à leur interprétation de la vision de la commission d'enquête parlementaire de **2016**, le législateur (européen) a en **2018** et **2019** solidement ancré le principe du « besoin de savoir » d'une part dans la législation européenne, et d'autre part (après transposition) dans la LPD et la LFP (articles 56 de la LPD et 44/2 §2 de la LFP). En ce sens, il convient de réaliser que les recommandations formulées en 2016 par la commission d'enquête de l'époque, en plus de n'être en effet que des 'recommandations', ne tenaient évidemment pas compte de la législation et de la réglementation contraignantes européennes et belges adoptées par la suite, qui naturellement prévalent à l'heure actuelle.

**11.2.** Le principe du *need to share* est l'un des aspects essentiels d'un traitement efficace de l'information par les services de police, tandis que le principe du *need to know* a trait à la licéité et à la légalité du traitement (compétence de traitement) compte tenu du rôle et de la fonction du membre de la police intégrée (du point de vue du droit à la protection des données). Ces deux principes ne s'excluent donc pas mutuellement. Ils sont au contraire complémentaires, bien que dans la hiérarchie des normes, la légalité et la licéité (telles que stipulées dans les normes européennes et nationales) prévalent évidemment sur l'efficacité opérationnelle. Si efficace qu'il soit ou semble être, un traitement policier souhaité doit toujours, préalablement et avant tout, être légal et licite.

**12.** Selon les auteurs du projet de directive, *« l'outil vient remédier à la situation actuelle où ces banques de données de base sont des « îlots d'information » séparés les uns des autres, sans qu'il y ait de ponts technologiques entre eux »*[17].

Pour les trois raisons exposées ci-après, l'Organe de contrôle trouve cet argument singulier.

Premièrement, c'est le législateur belge lui-même qui a en 2014 choisi délibérément et explicitement (1) d'imposer la conservation des données policières (informations et données à caractère personnel) dans des banques de données opérationnelles spécifiquement créées à cette fin et (2) de considérer ces banques de données de base comme des 'îlots'[18], ce qui ne traduit pas d'emblée le principe de police « intégrée », qui suppose nécessairement aussi une 'gestion intégrée de l'information'.

Deuxièmement, l' 'interconnexion' des banques de données de base au moyen d'un 'outil' ne change rien à cette situation, si ce n'est purement sur le plan opérationnel. Comme le font remarquer les auteurs du projet de directive, l'interconnexion de ces banques de données entre elles ou avec d'autres banques de données auxquelles les services de police ont légalement accès est depuis 2021 encadrée par la directive contraignante commune des Ministres de la Justice et de l'Intérieur du 4 août 2021.

[16] Ibidem.
[17] Projet de directive, p. 2.
[18] Pour reprendre la formulation utilisée par les auteurs du projet de directive pour décrire le cadre légal des banques de données opérationnelles (p. 2 du projet de directive).

Le fondement juridique de cette directive est ancré à l'article 44/4 §4 de la LFP[19]. Même si les banques de données de base n'étaient pas des îlots d'information, une directive contraignante commune des deux ministres compétents pour la police n'en serait pas pour autant superflue, bien au contraire. Si nous partons du principe, sur la base de la même hypothèse, que les services de police devraient en principe (pouvoir), sous conditions, avoir accès aux données policières qui sont traitées par la police intégrée dans des systèmes de police (intégrés), la définition des modalités opérationnelles plus détaillées dans une directive contraignante des ministres compétents pour la police pourrait sans aucun doute contribuer à une politique de traitement intégré de l'information policière.

Troisièmement, il existe déjà depuis 2014, dans le cadre des fonctionnalités de la directive MFO-6[20], un outil destiné aux CIA du SICAD[21] qui transmet chaque jour un flux statique des données de l'ISLP des zones de police et des entités de la DGA[22] au CIA compétent pour l'arrondissement (le 'flux 24h'), outil qui a été intégré à l'application 'Infosuite'. De plus, la plupart des CIA du SICAD disposaient déjà de droits d'accès sur les banques de données de base ISLP des zones de police de leur arrondissement avant même l'introduction du flux 24h et d'Infosuite. Cet accès découlait de l'article 23 de la loi du 18 mars 2014[23], qui a inséré dans la LFP l'article 44/11/2 relatif aux banques de données de base. En d'autres termes, la notion d' 'îlots d'information' doit être interprétée avec la nuance qui s'impose.

### A) Qu'est-ce que l' 'outil' PoliceSearch@GPI ?

**13.** Les auteurs du projet de directive présentent PoliceSearch@GPI comme un outil qui permet d'effectuer des recherches parmi les données, structurées ou non, des banques de données de base ISLP sur la base d'une indexation nationale et locale des données policières se trouvant dans ces banques de données de base, de sorte que celles-ci peuvent être consultées en temps (quasi) réel[24]. L'indexation nationale permet une recherche plus restreinte de données dans toutes les banques de données de base ISLP sur la base d'un filtre déterminé au préalable, tandis que l'indexation locale permet une recherche certes plus approfondie, mais exclusivement parmi les données de la banque de données de base ISLP choisie sur laquelle l'utilisateur a des droits, et uniquement en fonction des droits dont il dispose sur la banque de données de base ISLP en question.

---

[19] Directive contraignante commune des Ministres de la Justice et de l'Intérieur relative aux modalités relatives à l'interconnexion des banques de données visées à l'article 44/2 entre elles ou avec d'autres banques de données auxquelles les services de police ont accès par ou en vertu de la loi ou de traités internationaux liant la Belgique.
[20] Directive commune et contraignante MFO-6 des ministres de la Justice et de l'Intérieur du 9 janvier 2003 relative au fonctionnement et à l'organisation des carrefours d'informations de l'arrondissement.
[21] Les carrefours d'information d'arrondissement, faisant partie du service d'information et de communication de l'arrondissement (SICAD), pour le traitement de l'information en deuxième ligne après le traitement en temps réel.
[22] Direction générale de la police administrative.
[23] 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.
[24] Projet de directive, p. 4-5.

L' 'outil' permet donc aussi de consulter des informations et données à caractère personnel policières avant que celles-ci n'aient été enregistrées dans la Banque de données nationale générale (BNG). Pour pouvoir être intégrées dans la BNG, les données policières doivent en effet avoir fait l'objet d'un processus de validation. Pour cette raison, il s'écoule entre la collecte des données policières et leur enregistrement dans la BNG une certaine période durant laquelle les données policières ne sont pas accessibles dans la BNG alors qu'elles se trouvent bel et bien dans les banques de données de base. PoliceSearch@GPI rend donc également les données policières **non validées** accessibles à tous les services de police. Cet 'outil' permet de consulter en une seule recherche des données policières qui sont traitées dans d'autres banques de données de base (que celles dans lesquelles elles ont été saisies initialement). Cela dit, la définition des 'données validées' demeure précaire aux yeux du COC. Alors que dans l'avis non publié du 12 décembre 2022 relatif à l'AIPD de PoliceSearch@GPI (DI220014), l'Organe de contrôle constatait qu'il n'existe pas de définition claire de ce qu'il y a lieu d'entendre par 'données validées', le projet de directive en fournit à présent bel et bien une définition claire. Cependant, cette définition réduit les données validées aux seules données des procès-verbaux enregistrés dans la BNG et aux mesures à prendre. Le COC en déduit que les auteurs du projet de directive considèrent par définition les informations contenues dans des rapports d'information (RIR) ou dans des signalements d'enquête (DOS) comme 'non validées', qu'elles soient ou non reprises dans la BNG. Là aussi, le COC est d'avis que ce point mérite d'être nuancé.

**14.** PoliceSearch@GPI n'est donc pas une alternative à la BNG, mais un outil qui accélère l'accès aux données policières ('non validées') et qui fournit en même temps – excepté pour certaines catégories de données à caractère personnel (voir plus loin) – un aperçu (d'une quantité importante) de(s) données policières disponibles (à caractère personnel) concernant une personne donnée ou d'autres entités (par ex. des véhicules, des organisations ou des objets).

### B) Qui est le responsable du traitement ?

**15.** PoliceSearch@GPI est présenté comme un système d'indexation géré par la police fédérale, plus précisément par la DRI. L'Organe de contrôle constate que contrairement à l'analyse d'impact relative à la protection des données (AIPD[25]), le projet de directive ne désigne **pas** de responsable du traitement. L'AIPD, elle, désigne pourtant les Ministres de la Justice et de l'Intérieur, chacun dans le cadre de ses compétences, en tant que responsables du traitement dès lors que les auteurs de l'AIPD – tout comme d'ailleurs l'Organe de contrôle – considèrent l'outil PoliceSearch@GPI comme une banque de données de base telle que définie à l'article 44/4 §1er, 1er et 2e alinéas de la LFP. Les auteurs du projet sont priés de clarifier ce point et de désigner un ou plusieurs responsable(s) du traitement formel(s). Le responsable du traitement est en effet investi d'une obligation de reddition des comptes à l'égard du respect du Titre 2 de la LPD et de la LFP, et doit notamment dans ce contexte faciliter et

[25] En anglais *DPIA* pour *Data Protection Impact Assessment*.

permettre l'exercice des droits des personnes concernées (citoyens), comme le prévoient les articles 36 à 40 inclus de la LPD et l'article 42 de la LPD. La personne concernée dispose en outre en la matière d'une possibilité de recours en justice contre le responsable du traitement, de sorte qu'il est logique qu'elle doive savoir qui est le responsable du traitement auquel elle peut s'adresser ou contre lequel elle peut introduire un recours.

### C) La méthode de travail de PoliceSearch@GPI

**16.** L'Organe de contrôle constate avec plaisir que la recommandation n° 1 qu'il formulait dans son avis DI220014 au sujet du système de cascade a été intégrée dans le projet de directive. Le projet a également tenu compte de la recommandation n° 3 relative à l'application contextuelle, aux fichiers de journalisation et à la nécessité de mentionner un motif de consultation explicite, ainsi que des recommandations n° 4 et 5 portant respectivement sur le contrôle de la qualité et sur les délais de conservation, même s'il reste matière à évolution.

**17.1**. L'Organe de contrôle a cependant quelques remarques au sujet de la méthode de travail de l^outil' et des profils qui en résultent. À la lumière de la protection de la vie privée, l'Organe de contrôle comprend que l'utilisation de l'outil exclut l'indexation – ou du moins l'indexation directe – de certaines catégories de données à caractère personnel. Apparemment, c'est ainsi que les auteurs du projet de directive entendaient répondre à la recommandation n° 2 de l'avis DI220014 du COC relative à la proportionnalité des accès. Cette exclusion conduit cependant à une situation contradictoire, en ce sens que l'exemple concret des avantages du fonctionnement de PoliceSearch@GPI évoqué au point 1.5 du projet de directive – à savoir que des informations sur des faits de mœurs impliquant un pédophile présumé dans la ZP Westkust devraient être disponibles cinq minutes plus tard pour la ZP Mons-Quévy – est rendu techniquement impossible par les règles de *privacy by design* énoncées au point 2.3.1 du projet de directive, qui semblent exclure a priori les faits de mœurs, ainsi que par d'autres exclusions portant sur les rapports d'information et sur les rapports pour la coordination des enquêtes.

**17.2.** Cette contradiction illustre bien l'écart qui existe entre les extrêmes du spectre dans lequel se trouve la culture policière en matière de gestion de l'information. D'une part, il règne une 'crainte' par moments irrationnelle des traitements de données effectués par la police, qui tend à exclure un maximum de choses à la base en partant du principe que 'plus rien n'est possible ni permis'. Mais d'autre part, on retrouve aussi l'attitude pure et dure dictée par l'approche opérationnelle et la recherche d'efficacité, qui tend à mettre le plus possible de données à la disposition d'un maximum de collaborateurs en considérant que la fin justifie les moyens, dans l'optique qu' 'il vaut mieux trop que trop peu' ». Ces deux extrêmes font totalement abstraction des nuances indispensables qui transparaissent dans le droit à la protection des données appliqué au sein de la police, et qui sont

résumées dans la trinité 'légalité, nécessité et proportionnalité' des traitements policiers qui, combinée au caractère intégré de la GPI, constitue ou devrait constituer l'ADN d'une stratégie intégrée de partage de l'information.

**17.3.** Le dilemme entre ces deux extrêmes se traduit par le choix (contreproductif ou à tout le moins peu réfléchi) d'exclure certaines catégories de données à caractère personnel et de faits, et ce en dépit du nombre (non exhaustif) de cas pratiques dans lesquels tant la nécessité que la proportionnalité de ces données exclues sont abondamment prouvées.

1. L'exclusion des victimes

Les victimes d'un fait pénal font partie d'une catégorie de données à caractère personnel dont le traitement policier dans la BNG trouve sa base légale à l'article 44/5 §3, 9° de la LFP. Les trois exemples de cas pratiques qui suivent démontrent la nécessité et la proportionnalité de la consultation de telles données :

- le suivi de faits et événements récents, le suivi intégré de phénomènes et l'identification de relations entre des faits, mais en particulier le suivi de groupes d'auteurs et de victimes, par les CIA du SICAD dans le cadre des fonctionnalités de base de leur fonctionnement telles que décrites notamment dans la directive MFO-6 ;
- le suivi d'une personne qui effectue de (trop) nombreuses déclarations de perte ou de vol de sa carte d'identité sur une (trop) courte période, soit par une zone de police locale, soit par un CIA du SICAD, soit par une direction déconcentrée de la police judiciaire fédérale (PJF), soit par une direction centrale de la police judiciaire fédérale (DGJ) ;
- les services de police doivent et peuvent dans certaines circonstances traiter des noms et des identités de personnes physiques en cas d'abus de leur nom en tant qu'alias, abus ayant très souvent des conséquences très préjudiciables pour la personne concernée. La vérification en deuxième ligne d'une victime d'une usurpation d'identité à la suite d'un *hit* donné par la BNG Contrôle lors d'un contrôle à la frontière parce que le nom de cette personne est utilisé en tant qu'alias pourrait en effet être optimalisée grâce à l'utilisation de PoliceSearch@GPI en faisant une recherche sur la personne concernée en qualité de victime. Que la personne concernée dispose ou non d'une attestation de dépôt de plainte (ce qui s'avère souvent ne pas être le cas dans la pratique, pour diverses raisons), une recherche au moyen de l'outil PoliceSearch@GPI permettrait de vérifier si la personne concernée a ou non porté plainte pour usurpation d'identité, et donc de retenir cette personne le moins longtemps possible.

2. L'exclusion des mineurs d'âge

La seule restriction légale imposée aux catégories des mineurs d'âge en ce qui concerne les traitements dans la BNG est celle qui est prévue à l'article 44/7, 2e alinéa de la LFP : *« Pour ce qui concerne l'enregistrement dans la BNG des données visées à l'article 44/5, §3, 1°, relatives à un mineur qui n'a*

*pas 14 ans accomplis, l'autorisation du magistrat compétent est requise. »*. Autrement dit, la seule restriction imposée ici par le législateur concerne les mineurs de moins de 14 ans, et ce uniquement pour la catégorie des suspects et personnes condamnées. Les deux exemples de cas pratiques qui suivent démontrent la nécessité et la proportionnalité de (pouvoir) consulter les données de mineurs d'âge :

- le suivi de faits et événements récents impliquant des auteurs mineurs, le suivi intégré de phénomènes et l'identification de relations entre des faits impliquant des mineurs et le suivi de groupes d'auteurs utilisant des mineurs d'âge, par les CIA du SICAD dans le cadre des fonctionnalités de base de leur fonctionnement telles que décrites notamment dans la directive MFO-6 (par exemple des vols (organisés) commis par des groupes d'auteurs itinérants) ;
- les cas de disparition inquiétante récurrente de mineurs d'âge (art. 44/5 §3, 4°), dans lesquels la Cellule Personnes disparues doit par exemple être rapidement et efficacement informée des antécédents pour pouvoir se faire une idée du comportement d'un mineur disparu.

3. L'exclusion des faits de mœurs

À la lumière des mécanismes susmentionnés, et en particulier du fonctionnement des CIA du SICAD et du fonctionnement des directions centrales de la police judiciaire fédérale – sur lesquels nous revenons également plus loin –, le COC ne voit pas clairement pourquoi les faits de mœurs sont exclus *ab initio*. La seule motivation avancée est que cette exclusion est prévue *« dans l'optique de protéger l'intimité des victimes »* (p. 10 *in fine*, point 2.3.1, 4e § du projet de directive). Cette motivation vague et peu significative d'une exclusion qui protège d'emblée aussi (peut-être involontairement) l'intimité des suspects de faits de mœurs n'est pas convaincante ; le COC ne voit pas non plus pourquoi les victimes de tous les autres types d'infractions visées dans le Code pénal et dans les lois pénales spéciales ne devraient pas pouvoir se prévaloir de cette soi-disant protection de l'intimité. De plus, le COC ne voit pas non plus clairement pourquoi le projet reprend ici comme faits les codes de prévention '37 A à S'[26] mais ne fait *pas* mention du code de prévention '37 T', alors que cette catégorie de faits concerne la traite d'êtres humains et plus précisément l'exploitation sexuelle de mineurs d'âge. De plus, comme nous le disions plus haut, le point 1.5 du projet de directive cite justement comme exemple du fonctionnement intégré un fait de pédophilie, qui semble relever des exclusions puisqu'il s'agit d'un code de prévention '37 K'…

4. L'exclusion des données 'sensibles'

Le terme 'données sensibles' semble désigner les données sous embargo, les données d'enquêtes et les données relevant de codes d'utilisateurs restrictifs (les codes 00 et 01) tant des RIR que des DOS, ainsi que certaines données de nature administrative.

[26] Il s'agit du code attribué à de tels faits par le Ministère public.

À la lecture conjointe des dispositions des fiches B31[27], B42[28] et C13[29] de la directive MFO-3 et à la lumière des mécanismes mentionnés ci-avant et ci-après, en particulier (mais pas exclusivement) pour le fonctionnement des CIA du SICAD et le fonctionnement des directions centrales de la DGJ, sur lesquels nous reviendrons plus loin, le COC ne comprend pas pourquoi le projet n'établit pas de distinction entre trois finalités distinctes en termes de sensibilité qui sont décrites dans le projet de directive :

- l'embargo, qui repose sur l'article 44/8 de la LFP et sur une décision prise au niveau du parquet fédéral et qui engendre un report de l'alimentation de la BNG ;
- l'utilisation de codes d'utilisateurs restrictifs, ayant pour fondement réglementaire la directive MFO-3, qui permet encore dans des circonstances bien définies une accessibilité explicite pour les CIA du SICAD ainsi que pour les directions centrales de la DGJ ;

La troisième finalité consiste en des motifs de nature administrative qui sortent du cadre des traitements policiers opérationnels, et dont il faut se demander s'ils ont même leur place dans une banque de données de base. Le COC ne voit absolument pas pourquoi des données concernant des absences ou une maladie devraient faire l'objet d'une saisie dans le module 'Signalements' d'ISLP. Au moins en ce qui concerne les maladies, il s'agit de données relatives à la santé qui en vertu du RGPD doivent faire l'objet d'une attention particulière et de possibilités de traitement (plus) limitées, et qui sortent évidemment entièrement du cadre des traitements policiers opérationnels.

**17.4.** À la lumière de ce qui précède, les CIA du SICAD et les directions centrales de la DGJ ont sur le plan des codes d'utilisateurs restrictifs, vu les tâches qui leur sont attribuées, au moins un rôle à jouer pour ce type de données.

La fiche B42 de la directive MFO-3 énonce les règles pour la transmission (et l'utilisation) de copies de procès-verbaux et de rapports d'information à des fins documentaires aux directions centrales de la DGJ (DJSOC[30]). La transmission de ces documents est limitée à un certain nombre de cas, à savoir pour le contrôle de la qualité et pour informer des services de police spécialisés dans le cadre d'un suivi de phénomènes nécessitant leur soutien et leur coordination.

La directive MFO-6 susmentionnée définit les huit fonctionnalités de base du fonctionnement des CIA du SICAD. À travers ces huit fonctionnalités de base, les CIA du SICAD assurent l'exploitation des informations pour les autorités de police et les services de police, pour autant que cette exploitation, compte tenu des possibilités propres dont disposent les services de police, représente une valeur ajoutée tant sur le plan opérationnel que sur le plan du déploiement d'une politique de sécurité dans les domaines de la police administrative et judiciaire. Autrement dit, pour les données pour lesquelles c'est proportionnel et nécessaire, l'outil PoliceSearch@GPI peut grandement contribuer à un

[27] L'établissement de rapports d'information judiciaires, non publiée.
[28] La transmission et l'utilisation de procès-verbaux et de rapports d'information à des fins documentaires, non publiée.
[29] La coordination des enquêtes, non publiée.
[30] « Serious and Organised Crime », la Direction centrale de la lutte contre la criminalité grave et organisée.

fonctionnement plus rapide et intégré des CIA du SICAD ainsi que des directions centrales de la DGJ en complétant – mais sans les remplacer – les outils existants.

**17.5.** L'exercice (in)direct des droits

Indépendamment de la problématique de l'exercice direct ou non des droits de la personne concernée, tant l'autorité de contrôle que le(s) délégué(s) à la protection concerné(s) (*DPO*) ont besoin d'un aperçu clair des traitements dont une personne concernée fait l'objet. Dans l'état actuel de la gestion de l'information, les données à caractère personnel sont traitées dans les banques de données visées à l'article 44/2 de la LFP. Une possibilité de recherche transversale parmi toutes les catégories de données à caractère personnel traitées dans les banques de données de base ISLP facilite considérablement ce travail, même si PoliceSearch@GPI ne fournit pas toutes les informations traitées par la police dans des banques de données (de base), ni ne résout a fortiori le problème des banques de données particulières. PoliceSearch@GPI ne permet en effet pas de recherches transversales dans d'autres banques de données de base comme FEEDIS[31] ou CAD[32], même s'il existe un flux (partiel) vers ISLP à partir de CAD. Pour toute clarté, le COC tient à préciser que les banques de données de base pour les enquêtes[33] ne sont pas prises en considération dans cet exemple ni dans le présent avis. L'interconnexion de telles banques de données nécessite en effet des conditions plus strictes en termes de nécessité et de proportionnalité des accès et des traitements, ainsi que des mesures techniques et organisationnelles plus poussées. Quoi qu'il en soit, il est certain que l'outil PoliceSearch@GPI a également une valeur ajoutée considérable pour la finalité de l'exercice (in)direct des droits des personnes concernées.

**18.** Bien que l'Organe de contrôle puisse *sensu lato* adhérer à cette méthode de travail dès lors qu'il a dûment été tenu compte des recommandations qu'il formulait dans son avis DI220014, on peut s'interroger sur la cohérence et l'opportunité de l'exclusion de la prise en connaissance directe des catégories susmentionnées, ou même se demander si la mise en place de PoliceSearch@GPI n'impose pas (volontairement ou non) une restriction (non nécessaire) sur le terrain. En tout état de cause, l'Organe de contrôle invite les auteurs du projet de directive :

- à réexaminer et reconsidérer les exclusions *ab initio* identifiées ;
- à les replacer dans le contexte d'un fonctionnement intégré en les associant à des **profils additionnels** qui tiendraient compte :
    - des finalités des CIA du SICAD et des directions centrales de la DGJ ;
    - des finalités du délégué à la protection des données (*DPO*) et des services du Contrôle Interne ;
    - des finalités de l'autorité de contrôle.

[31] Feeding Information System, une banque de données de base utilisée par la PJF.
[32] Computer Aided Dispatching, une banque de données de base utilisée par les CIC du SICAD.
[33] Dont GES (Gestion d'Enquêtes) et les outils qui en font partie, comme le traitement des données de téléphonie.

**PAR CES MOTIFS,**

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

**prie le demandeur de donner suite aux remarques susmentionnées.**

Avis approuvé par l'Organe de contrôle de l'information policière le 23octobre 2024.

Pour l'Organe de contrôle,

Le président a.i.,
Frank SCHUERMANS (Sé)