ORGANE DE CONTRÔLE DE L'INFORMATION POLICIÈRE

Votre référence	Notre référence	Annexe(s)	Date
/	DA220021		14.7.2022

Objet : Avis relatif à un avant-projet de loi relatif aux traitements de données à caractère personnel par la Direction générale Office des étrangers du Service public fédéral Intérieur

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 VII, 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').

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 adressée le 9 juin 2022 par le Secrétaire d'État à l'Asile et à la Migration à l'Autorité de protection des données (ci-après : 'APD') en vue d'émettre un avis sur l'avant-projet de loi relatif aux traitements de données à caractère personnel par la Direction générale Office des étrangers du Service public fédéral Intérieur (ci-après 'l'avant-projet') ;

Vu la transmission de la demande susmentionnée, en date du 9 juin 2022, par l'APD à l'Organe de contrôle dans le cadre de la fonction de guichet unique de l'APD (article 54/1 de la LAPD) et conformément aux dispositions du protocole de coopération entre les autorités de contrôle fédérales belges en matière de protection des données (cf. www.organedecontrole.be).

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

Émet, le 14 juillet 2022, 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 ou *LED*). 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

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

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'), telle que visée dans la loi du 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. Enfin, 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.

II. Objet de la demande

5. La demande d'avis a trait à un avant-projet de loi relatif aux traitements de données à caractère personnel par la Direction générale Office des étrangers du Service public fédéral Intérieur.

6. Les autorités et les traitements de données à caractère personnel et d'informations pour lesquels le COC est exclusivement compétent sont strictement définis par la loi. En conséquence, l'Organe de contrôle limite ses avis aux traitements relevant de sa compétence, en l'occurrence dans le cas présent ceux qui sont effectués par les services de police ou qui ont un impact sur le fonctionnement des services de police. En l'occurrence, le Secrétaire d'État qui a formulé la demande a également coché les services de police en réponse à la

[5] Articles 59 §1er, 2e alinéa et 236 §2 de la LPD.
[6] Article 71 §1er, troisième alinéa juncto article 236 §3 de la LPD.

question de savoir si *« le projet a trait à ou implique un (des) traitement(s) de données à caractère personnel par une ou plusieurs des autorités suivantes »*.

Quoi qu'il en soit, les avis du COC ne se limitent pas nécessairement à l'éventuel article ou aux éventuels articles mentionnés dans une demande d'avis. Le COC tient en effet toujours compte de tous les éléments et dispositions relevant de sa compétence en vertu de la réglementation susmentionnée. De plus, l'Organe de contrôle n'est pas seulement une autorité de protection des données, mais est aussi chargé du contrôle et de la surveillance des banques de données policières[7] et de tous les traitements policiers, également en termes de légalité, d'efficacité et d'effectivité. Ces éléments (par exemple la faisabilité opérationnelle et la capacité) sont toujours pris en compte lors de la formulation d'un avis.

III. Analyse de la demande

7. Le COC se limite dans le présent avis aux articles qui ont un impact sur le fonctionnement des services de la police intégrée (ci-après 'la GPI') ou sur le fonctionnement de l'Organe de contrôle.

1. Les traitements dans la Banque de données Nationale Générale et dans le Système d'Information Schengen

8. Le projet d'article 10 prévoit les finalités pour lesquelles les données à caractère personnel peuvent être traitées par l'Office des étrangers (ci-après 'l'OE'). Les catégories de données à caractère personnel visées à l'article 6 peuvent être traitées notamment pour la finalité prévue au point 11°, à savoir pour *« assurer le suivi des interdictions d'entrée, en ce compris leur levée ou leur suspension ainsi que la gestion de leur enregistrement dans le Système d'Information Schengen et dans la Banque de données Nationale Générale ou dans toute autre banque de données nationale »*. L'exposé des motifs stipule pour le projet d'article 9 que *« … l'Office des étrangers doit pouvoir traiter les données à caractère personnel de cette catégorie de personnes concernées afin de pouvoir assurer le suivi des décisions d'interdiction d'entrée, la gestion de l'enregistrement de ces interdictions d'entrée dans le SIS et/ou dans la BNG* (soulignement propre) *ainsi que traiter les demandes de suspension ou de levée de*

[7] Voir aussi le rapport d'activité 2020 du COC, https://www.organedecontrole.be/files/Rapport-dactivit%C3%A9_COC_2020_F.pdf, points 7 et 8.

ces décisions ». Un alinéa similaire est mentionné dans le commentaire relatif à l'article 10 (*« assurer le suivi des interdictions d'entrée »*).

L'avant-projet fait donc en sorte que **pour la première fois, ne serait-ce qu'implicitement**, une disposition légale prévoit qu'un 'service non policier', à savoir l'OE, puisse traiter des données dans une banque de données **policière** nationale et dans une banque de données **policière** internationale. On entend donc en l'occurrence par « traitement » la saisie effective de données et tous les actes apparentés, comme la modification, la rectification, l'effacement, etc., et donc pas uniquement la 'consultation'. Les membres du personnel de l'OE seraient donc autorisés à effectuer plusieurs fois des traitements dans la BNG concernant une même personne (par exemple en fonction de son statut de séjour).

À ce jour, aucune disposition légale ne prévoit pour l'OE (ni d'ailleurs pour quelque autre administration, organe ou institution tierce) la possibilité d'effectuer ces traitements dans la BNG ou dans une autre banque de données policière. Jusqu'ici, l'OE pouvait uniquement obtenir communication d'informations et données à caractère personnel de la BNG (cf. articles 44/11/4 et suivants et plus précisément l'article 44/11/9 §1er, 2° et l'article 44/11/12 §1er, 2° de la LFP). Ces traitements au bénéfice de l'OE ne sont d'ailleurs actuellement pas effectués par l'OE lui-même, mais toujours par la GPI (à la demande de l'OE, voir aussi le point 15). Modifier cette situation en permettant à une administration, un organe ou une institution tierce d'effectuer soi-même les traitements intrusifs visés ici sous toutes leurs facettes constitue dès lors un précédent important dont l'objectif ne saurait être qu'il ouvre la voie à d'autres modifications similaires, à moins qu'une motivation spécifique ne le justifie.

Il est en outre encore plus important de créer une base légale claire – en en motivant suffisamment la nécessité – pour permettre à l'OE d'effectuer de manière autonome ces traitements dans des banques de données policières comme la BNG. Cela signifie en tout cas que la loi sur la fonction de police doit être amendée en ce sens, et plus particulièrement la section 12 (*« De la gestion des informations »*) du Chapitre IV (*« De la forme et des conditions générales d'exercice des missions »*) en y créant, de préférence dans un article distinct, la base légale permettant à l'OE d'effectuer les traitements visés dans le projet d'article 10, 11° de l'avant-projet de loi (*« … le suivi des interdictions d'entrée, en ce compris leur levée ou leur suspension ainsi que* ***la gestion de leur enregistrement*** *dans le Système d'Information Schengen et dans la Banque de données nationale générale ou dans toute autre banque de données nationale »*). De plus, cette modification indispensable de la LFP

devra au préalable être soumise pour avis à l'Organe de contrôle en vertu de l'article 59 §1er, 2e alinéa de la LPD.

9. En ce qui concerne la BNG, les responsables du traitement sont les ministres de l'Intérieur et de la Justice et les responsables opérationnels sont les services de police. L'Organe de contrôle n'a pas été en mesure d'établir si le ministre de la Justice, en sa qualité de coresponsable du traitement, est au courant de la possibilité qui est ici créée de permettre à l'OE d'effectuer directement les traitements les plus intrusifs dans la BNG ; en marge de l'évidente nécessité d'impliquer le ministre de la Justice en sa qualité de coresponsable du traitement, il semble que d'un point de vue formel, le ministre de la Justice doive également cosigner l'avant-projet étant donné qu'il touche directement à une législation relevant de ses attributions.

10. Il n'est évidemment pas sans danger ni sans risque d'autoriser une administration comme l'OE à effectuer directement dans la BNG des traitements qui vont beaucoup plus loin que la seule consultation. L'avant-projet n'approfondit nullement cet aspect essentiel et ne motive pas non plus la nécessité pour l'OE d'obtenir cette compétence et ces possibilités, peut-être aussi pour que l'ancrage légal ne soit qu'implicite et indirect, et donc insuffisant. Comment ces possibilités seront-elles organisées dans la pratique ? Quels mécanismes de contrôle sont prévus ? Qui au sein de l'OE aura accès à la BNG ? À quelles applications de la BNG l'OE pourra-t-il accéder ? Quelle formation sera prévue pour le personnel de l'OE ? Etc.

Autrement dit, les modalités concrètes devront être reprises dans une réglementation. Une possibilité serait de mettre ce système en œuvre dans l'arrêté royal existant du 28 avril 2016 relatif à l'interrogation directe de la Banque de données Nationale Générale visée à l'article 44/7 de la loi sur la fonction de police par les membres du personnel désignés de l'Office des étrangers (M.B. 12 mai 2016), qui aurait d'ailleurs de toute façon dû depuis longtemps ou devrait être adapté en fonction du nouveau cadre juridique de la protection des données[8] qui est d'application depuis 2018. En vertu de cet arrêté royal, certains membres du personnel de l'OE disposent actuellement uniquement d'une possibilité 'd'interrogation directe' de la BNG, ce qui va donc beaucoup moins loin que la possibilité d'effectuer effectivement des saisies de données, d'établir et de saisir des signalements, d'apporter des corrections et des modifications, etc. L'arrêté royal devra donc être remanié en profondeur à la lumière de cet avant-projet de loi et du fondement juridique qui devra nécessairement être créé dans la LFP

[8] L'arrêté royal fait notamment encore référence à l'ancienne Commission de la protection de la vie privée (art. 1, 8°, art. 5) et à un *« conseiller en sécurité et en protection de la vie privée »* (art. 5), le COC n'était à l'époque pas encore une autorité de protection des données, ce qu'il est dans l'intervalle évidemment devenu à l'égard de la GPI, etc.

(voir le point 8). De plus, cette modification de l'arrêté royal devra elle aussi être soumise pour avis à l'Organe de contrôle en vertu de l'article 59 §1er, 2e alinéa de la LPD.

Par ailleurs, l'Organe de contrôle ne voit pas clairement ce que le projet d'article 10, 11° entend par *« ou dans toute autre banque de données nationale »* (la version néerlandaise ne dit d'ailleurs pas tout à fait la même chose puisque l'on y trouve la formulation *« of in* ***een*** *andere nationale gegevensbank »*). L'exposé des motifs ne fournit lui non plus aucune précision à ce sujet. Le COC ne voit pas de quelle autre banque de données nationale il pourrait potentiellement s'agir, de sorte qu'il n'y a aucune raison de maintenir cette partie de la phrase vu qu'il ne peut s'agir que de la BNG qui est déjà citée.

11. En outre, l'arrêté royal fait également mention d'un protocole entre l'OE et *« la direction qui gère les accès à la B.N.G. »* (dans les faits, il s'agit de la DRI, la Direction de l'information policière et des moyens ICT de la police fédérale (une direction faisant partie du Commissariat général). Ce protocole du 29 septembre 2016 devra lui aussi être remanié pour la même raison que celle que nous évoquions plus haut, à savoir la nécessité de l'adapter en fonction du nouveau cadre de la protection des données, et compte tenu des possibilités de traitement étendues que l'avant-projet a l'intention d'offrir à l'OE. Cette modification du protocole devra elle aussi être soumise au préalable non seulement à l'Autorité de protection des données, mais aussi à l'Organe de contrôle (cf. article 6 de l'arrêté royal du 28 avril 2016). Les questions qu'il faudra dans ce contexte se poser porteront notamment, mais sans s'y limiter, sur les aspects suivants :

- la portée de l'enquête de milieu et des antécédents (voir aussi le point 2 du protocole d'accord entre l'OE et la DRI) dont les membres du personnel de l'OE doivent actuellement faire l'objet avant d'être autorisés à interroger directement la BNG ; à l'heure actuelle, seul un avis de sécurité au sens de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité (art. 22quinquies) est requis. Un avis de sécurité positif ponctuel suffira-t-il encore à l'avenir ?

- le profil exact du collaborateur de l'OE. Ces profils ne doivent-ils pas être réexaminés à présent que le collaborateur de l'OE se verra attribuer des compétences qui vont beaucoup plus loin qu'aujourd'hui, où il peut seulement obtenir communication d'informations et de données à caractère personnel à travers l'interrogation directe (système *hit/no hit*) et n'a par exemple pas accès aux informations douces (voir aussi l'article 4, b) : uniquement les informations consignées dans des procès-verbaux) ? Comment peut-on éviter que le

collaborateur de l'OE prenne connaissance de toutes les informations douces disponibles à partir du moment où il obtient un profil lui permettant de saisir des données ?

- *quid* du télétravail prévu pour les membres du personnel de l'OE (voir le point 4.1 du protocole d'accord) ?

- un audit de fonctionnement tous les deux ans est-il suffisant (voir le point 5 du protocole d'accord) ?

- quelle formation concrète va-t-on devoir prévoir pour le collaborateur de l'OE ? Il va de soi que cette formation devra être beaucoup plus poussée et plus intensive que celle qui est prévue actuellement (voir le point 6 du protocole d'accord) pour l'interrogation directe.

- etc.

12. Le protocole parle encore aussi d'un *« document ad hoc distinct »* reprenant les aspects techniques de l'interrogation directe. Le COC n'a pas encore connaissance de ce document mais le demandera en tout état de cause à la DRI lorsque cet avant-projet sera en passe de devenir une loi. Le protocole d'accord prévoit d'ailleurs lui-même sa révision en son point 10, *« à tout le moins, dans les cas suivants :*

- *modification du cadre légal ou réglementaire :*
- *… ;*
- *émergence de besoins supplémentaire ;*
- *… »*

Ce protocole d'accord aurait donc en réalité déjà dû être revu à la lumière de la modification du cadre juridique de la protection des données en 2018, et ce sera encore davantage le cas si cet avant-projet devient une loi.

13. D'un autre côté, le responsable du traitement de la partie nationale de la banque de données SIS II n'a jamais été identifié dans une loi ou dans un arrêté d'exécution, ce qui pose d'ailleurs toujours un problème juridique à ce jour. À cet égard, il convient de faire référence à une enquête de contrôle que le COC a menée en 2019 en collaboration avec l'APD et qui a conduit à l'établissement le 2 février 2020 d'un rapport intitulé *« Rapport final de la visite de contrôle du bureau SIRENE (Système d'Information Schengen) par l'Organe de contrôle de l'information policière et par l'Autorité de protection des données »*. Ce rapport transmis au commissaire général de la police fédérale et au directeur de CGI contient notamment les constatations suivantes :

6.1.1.1. Première observation générale : Les instances responsables pour le bureau SIRENE et l'Office N.SIS II n'ont pas été désignées dans le droit belge

56. En 2019, aucune réglementation n'a encore transposé la Décision SIS II en droit belge.
De même, aucun texte légal belge ne complète les règles Schengen (*ci-après la remarque de CGI suite à la remise du rapport intermédiaire de visite : « Point 56 de la page 16/60 : (idem constatation A1 à la page 50) à nuancer ; la Décision SIS II produit ses effets directement sur l'ordre juridique interne, de sorte qu'une transposition en tant que telle de l'intégralité de la décision en droit belge n'est pas nécessaire (voir aussi l'analyse du SPF Intérieur lors de l'entrée en vigueur de la Décision SIS II). Les principes opérationnels ont toutefois été transposés dans la fiche C22 de la directive ministérielle MFO-3. Si une modification légale s'impose dans le sillage de la directive européenne 680/2016 qui a été transposée par la loi nationale du 30/07/2018, les adaptations requises auraient dû être apportées par la loi du 22/07/2019, ce qui n'est pas le cas. Dans l'intervalle, il a été constaté que l'article 26, 8° de la loi 30/07/2018 doit être modifié pour permettre de désigner les ministres compétents en tant que responsables du traitement et de l'exécution de la directive européenne. Les autorités politiques en ont été informées au préalable. »*) qui laissent aux législateurs nationaux le soin de régler certaines questions. C'est le cas par exemple dans la Décision SIS II et dans le Règlement SIS II pour les délais de conservation concernant les signalements et les informations traitées par le bureau SIRENE : rien n'est explicitement prévu sur ces questions au niveau belge.
Les autorités de contrôle ont constaté que la Décision SIS II et le Règlement SIS II, malgré qu'ils soient d'application directe en droit belge et ne demandent par conséquent pas de transposition en tant que telle, renvoient pour certains points au droit national. Ces renvois doivent trouver une réponse en droit belge, ce qui n'est pas le cas au jour de la rédaction du présent rapport puisque certaines questions, comme les délais de conservation à appliquer à certains types de signalements ou encore la désignation du bureau SIRENE et de l'Office N.SIS II, ne sont pas réglées en droit belge. Cette remarque de CGI ne modifie donc pas la constatation des autorités de contrôle.
57. Ce constat est le même pour la désignation des instances responsables pour le bureau SIRENE et l'Office N.SIS II (Décision SIS II et Règlement SIS II, articles 6 et 7 communs). En effet, la Belgique doit désigner un Office N.SIS II qui assume la responsabilité centrale du N.SIS II. Cette instance est responsable du bon fonctionnement et de la sécurité du N.SIS II, elle doit faire en sorte que les autorités compétentes aient accès au SIS II mais aussi prendre les mesures nécessaires pour assurer le respect des dispositions de la Décision SIS II et du Règlement SIS II.
58. La Belgique doit également désigner une instance – le bureau SIRENE – chargée de l'échange de toutes les informations supplémentaires et de vérifier la qualité des informations introduites dans le SIS II. Pour cela, le bureau SIRENE doit avoir accès aux données traitées dans le SIS II.
59. Ces instances ne sont pas identifiées dans le droit belge. En effet, l'arrêté royal du 14 novembre 2006 (*Arrêté royal du 14 novembre 2006 relatif à l'organisation et aux compétences de la police fédérale, articles 2, 1°, e) et 6, 3°*) qui attribue la détermination des normes et d'une approche standardisée en matière de sécurité de l'information et de protection de la vie privée au Commissariat général, et qui confie entre autres la préparation de la politique et des règles relatives au traitement de l'information policière à la Direction générale de la gestion des ressources de l'information (« DGR ») de la police fédérale, le tout en concertation avec la Commission permanente de la police locale, ne constitue pas une base suffisamment claire et précise d'identification des instances responsables pour le bureau SIRENE et l'Office N.SIS II.
60. Cela oblige les autorités de contrôle à constater que dès lors l'exercice concret, correct et efficace des missions qui incombent à ces instances responsables peut difficilement être mis en œuvre.
61. *De facto*, le bureau SIRENE est installé sous CGI et s'occupe de la gestion des signalements ainsi que de l'échange des informations supplémentaires. DRI met pour sa part à disposition du bureau SIRENE les outils nécessaires au traitement des signalements Schengen : DRI gère le fonctionnement et la sécurité de la copie nationale du N.SIS II dont a besoin le bureau SIRENE pour travailler avec le SIS II.
62. La note de politique générale de sécurité de l'information SIS II approuvée par les Ministres de l'Intérieur et de la Justice le 18 octobre 2016 a pour objectif de *« définir un cadre pour la mise en œuvre d'un ensemble approprié de mesures pour assurer la sécurité de la copie nationale du N.SIS II et des systèmes d'information des services de police nécessaires au fonctionnement du SIS II »*. L'objectif de cette note est de garantir la confidentialité, l'intégrité et la disponibilité des informations traitées dans ces systèmes d'information.
En matière de sécurité, la note partage les responsabilités fonctionnelles et techniques : CGI détermine les objectifs du plan de sécurité pour le SIS II et est donc responsable pour le N.SIS II et le bureau SIRENE, quant à DRI, elle détermine les objectifs de sécurité et met en place les mesures techniques de sécurité pour les différents systèmes d'information.
63. De leurs rencontres avec les *DPO* de CGI et de DRI, les autorités de contrôle ont constaté que si les deux Directions de la police fédérale s'accordent pour considérer que les Ministres de la Justice et de l'Intérieur sont responsables du traitement pour la copie nationale du N.SIS II, le *DPO* de DRI indique que DRI n'est pas responsable pour l'Office N.SIS II tandis que le *DPO* de CGI estime que CGI est l'instance responsable pour le bureau SIRENE et qu'elle partage une responsabilité avec DRI (selon CGI, DRI s'occuperait des aspects techniques et logistiques tandis que CGI assumerait les tâches opérationnelles) en ce qui concerne le N.SIS II.
64. La vision du *DPO* de CGI va dans le même sens que ce qui est indiqué dans la note de politique générale de sécurité de l'information SIS II approuvée le 18 octobre 2016.

> **65**. Cependant, la Belgique doit communiquer chaque année (*ces Directions sont ainsi désignées depuis 2015 au Journal Officiel de l'Union européenne. Avant cela, les anciennes Direction de la télématique pour le SIS II et Direction de l'information policière opérationnelle pour le bureau SIRENE étaient désignées*) au gestionnaire fonctionnel du SIS II, conformément à la Décision SIS II et au Règlement SIS II *(Règlement SIS II et Décision SIS II, article 7 §3 commun)*, les coordonnées de son Office N.SIS II ainsi que de son bureau SIRENE. Elle s'y est dernièrement conformée en indiquant que pour le N.SIS II, l'autorité responsable est « le Bureau N.SIS II de la police fédérale – DRI » et que pour le bureau SIRENE, il s'agit de la « Commission SIRENE de la police fédérale – CGI (*Liste des offices N.SIS II et des bureaux SIRENE nationaux » consolidée au 15 mars 2019, J.L.O., C222, 2 juillet 2019, p. 173.*) ».
> **66**. Ainsi, tandis que la Décision SIS II et le Règlement SIS II nécessitent, pour la bonne alimentation du SIS II, une coopération soutenue et une communication fluide entre deux instances désignées responsables au niveau national, cela est difficilement possible au niveau belge sans désignation claire puisque cette coopération et cette communication se jouent *de facto* entre deux Directions différentes qui ne se situent pas au même niveau hiérarchique (*ci-après la remarque de CGI suite à la remise du rapport intermédiaire de visite : « Point 66. CGI ne fait pas partie du commissariat général mais est une direction spécifique (voir l'arrêté royal du 14 novembre 2006). » L'Organe de contrôle se réfère à l'article 3, 1° de l'arrêté royal du 14 novembre 2006 relatif à l'organisation et aux compétences de la police fédérale qui indique que le Commissariat général se compose de la Direction de la coopération policière internationale. Cette remarque de CGI ne modifie donc pas la constatation des autorités de contrôle)* de la police intégrée et structurée à deux niveaux telle qu'elle est instituée en Belgique. En effet, d'une part le bureau SIRENE est installé au sein du Single Point of Operational Contact de CGI qui fait partie du Commissariat général de la police fédérale et d'autre part, DRI fait partie de la DGR.
> **67**. Vu l'absence de désignation claire des deux instances responsables dans le droit belge et eu égard aux positions contradictoires de CGI et DRI, les autorités de contrôle considèrent que la communication officielle de la Belgique au gestionnaire fonctionnel du SIS II, telle qu'elle a encore été récemment inscrite au Journal Officiel de l'Union européenne du 2 juillet 2019, constitue une désignation de CGI et de DRI comme autorités responsables, respectivement pour le bureau SIRENE et pour le N.SIS II.
> **68**. D'emblée, les autorités de contrôle insistent sur le fait que la répartition des tâches de mise à jour, de gestion des signalements et des responsabilités telle qu'elle est prévue dans le Règlement SIS II et la Décision SIS II invite l'Office N.SIS II – DRI et le bureau SIRENE – CGI à travailler étroitement ensemble pour que l'alimentation du SIS II fonctionne plus efficacement.

14. Il va de soi que le problème se fait encore plus cuisant à partir du moment où l'OE est à présent investi d'une responsabilité (partagée) à l'égard des aspects visés par le projet d'article 10, 11° de l'avant-projet, à savoir *« le suivi des interdictions d'entrée, en ce compris leur levée ou leur suspension ainsi que la gestion de leur enregistrement dans le Système d'Information Schengen et dans la Banque de données nationale générale ou dans toute autre banque de données nationale ».*

Il semble donc indispensable de remédier à ce problème posé par l'absence, dans la LFP, d'un fondement juridique clair et d'une désignation des responsables du traitement et des responsables opérationnels du Système d'Information Schengen, et de faire la clarté sur ce point.

15. La problématique des signalements reposant sur l'article 24 du Règlement SIS II a également été abordée dans le cadre de l'enquête susmentionnée de l'APD et du COC. La constatation suivante a été formulée à ce sujet :

> **138**. Certains autres partenaires externes comme l'ODE, le Ministère des affaires étrangères et la Direction de l'Immatriculation des véhicules (*« Liste des autorités compétentes autorisées à consulter directement les données introduites dans le système d'information Schengen de deuxième génération », J.O.L. C222, 2 juillet 2019, p. 1.*) ont également accès via l'application Portal ou un webservice. Le service des Douanes n'a pour l'instant aucun accès.

> **139**. Les protocoles avec l'ODE sont en cours d'élaboration. Il existe cependant une procédure tacite applicable depuis un certain nombre d'années : les signalements visés à l'article 24 du Règlement SIS II sont introduits dans le SIS II sur base d'un formulaire standard communiqué par l'ODE et sans pièces justificatives c'est-à-dire que la décision ayant motivé le signalement n'est pas jointe. De même, les signalements sont automatiquement renouvelés jusqu'à l'échéance de la décision de l'ODE. Par ailleurs, le *Legal Office* déclare que la révision de la Directive « retour » (Directive 2008/115/CE du Parlement européen et du Conseil du 16 décembre 2008 relative aux normes et procédures communes applicables dans les États membres au retour des ressortissants de pays tiers en séjour irrégulier) devrait accroître exponentiellement le nombre de signalements. Dès lors, le protocole en projet vise à fournir à l'ODE une possibilité d'alimentation directe du N.SIS II (ci-après la remarque de CGI suite à la remise du rapport intermédiaire de visite *(« Point 139 de la page 32/60 : il n'y a qu'un seul protocole en vigueur avec l'OE concernant la décision SIS II. La dernière phrase n'est pas correcte ; le protocole actuellement en vigueur vise à officialiser la collaboration actuelle entre la police et l'OE. Si l'alimentation directe du N.SIS II (par ex. en ce qui concerne les décisions de retour) est confirmée et déployée (ou en cas de modification de quelque autre méthode de travail), ce protocole devra être adapté en conséquence. » Dans la mesure où cet accès est envisagé, les autorités de contrôle invitent les autorités concernées à d'ores et déjà prévoir toutes les modalités dans le protocole et à procéder à une analyse complète du respect des règles en matière de protection des données. Cette remarque de CGI ne modifie donc pas la constatation des autorités de contrôle*).

Cette procédure qui s'est manifestement imposée tacitement dans la pratique et qui consiste à ce que la police (et plus précisément le bureau SIRENE de CGI/SPOC de la police fédérale) introduise les signalements pour l'OE (art. 24 du Règlement SIS II) devra donc être réexaminée à la lumière de l'avant-projet et du présent avis de l'Organe de contrôle. Déjà à l'époque, on envisageait manifestement déjà la possibilité de laisser l'OE introduire lui-même ses signalements dans le Système d'Information Schengen et il était question d'un projet de protocole. Le COC n'a pas connaissance d'un protocole définitif en la matière et il serait d'ailleurs difficile d'en conclure un sans une modification légale préalable, comme l'a à juste titre indiqué CGI dans sa réplique au projet de rapport du COC et de l'APD.

2. <u>Les destinataires des données communiquées par l'OE</u>

16. Le projet d'article 11 énumère en son paragraphe 1er les différents destinataires ou catégories de destinataires auxquels l'OE peut communiquer les données à caractère personnel qu'il collecte. Ce paragraphe prévoit d'une part un point 6° – à savoir les *« autorités chargées du contrôle aux frontières extérieures de la Belgique ou d'un autre État membre aux fins d'assurer »* les finalités visées aux points a) à d) – mais d'autre part aussi un point 14°, à savoir les services de police fédérale et de police locale *« pour veiller au respect sur le territoire du Royaume des dispositions légales relatives à l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers et prendre les mesures requises en exécution de celles-ci »*. Parmi les autorités *« chargées du contrôle aux frontières extérieures de la Belgique ou d'un autre État membre »* figurent, selon l'exposé des motifs, la police aéronautique, la police de la navigation et la police des chemins de fer de la police fédérale, alors que ce même exposé des motifs mentionne encore une fois parmi les services de police

fédérale et de police locale ces trois unités spécialisées de la police fédérale. Ces deux dispositions semblent donc (du moins pour une part) faire double emploi.

17. Parmi les destinataires potentiels figurent également, au point 22°, les médiateurs fédéraux. L'exposé des motifs stipule à ce sujet que ceux-ci ont notamment *« pour missions d'examiner les réclamations des citoyens relatives aux actes et au fonctionnement des autorités administratives fédérales ainsi que de mener, à la demande de la Chambre des représentants, toute investigation sur le fonctionnement des services administratifs fédéraux. L'Office des étrangers fait partie de ces « services administratifs fédéraux » [Loi du 22 mars 1995 instaurant des médiateurs fédéraux]. »*.

L'Organe de contrôle constate par contre qu'il ne figure pour sa part pas parmi les institutions qui peuvent recevoir des données à caractère personnel de l'OE ou, mieux, auxquelles l'OE peut communiquer des données à caractère personnel. En sa qualité d'autorité de contrôle indépendante, l'Organe de contrôle ne peut pas non plus être considéré comme une *« autorité policière ou judiciaire belge »* au sens du point 36° du projet d'article 11, §1er. Dans la pratique, cependant, la communication de données à caractère personnel entre l'Organe de contrôle et l'OE est fréquente dans le cadre des demandes d'accès direct (auprès de l'OE) ou indirect (auprès de l'Organe de contrôle). Lorsque l'objet d'une demande est un article 24 du Règlement SIS II[9] (voir plus haut), de telles demandes sont aussi très régulièrement introduites auprès du COC, qui les transmet alors à l'OE ; à l'inverse, il arrive aussi que le COC reçoive une demande qui a initialement été introduite auprès de l'OE, mais qui s'avère après examen avoir trait à un signalement pour un autre motif qu'une interdiction d'entrée. La collaboration mutuelle entre l'OE, l'APD et le COC a d'ailleurs également été convenue et mise au point lors d'une concertation entre l'OE, le COC et l'APD organisée dans le cadre d'une réunion qui a eu lieu le 27 juin 2019 auprès de l'Organe de contrôle. Si l'objet

[9] Règlement (CE) n° 1987/2006 du Parlement européen et du Conseil du 20 décembre 2006 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen de deuxième génération (SIS II). Ce Règlement et la Décision 2007/533/JAI du Conseil du 12 juin 2007 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen de deuxième génération (SIS II) seront remplacés par le Règlement (UE) 2018/1860 du Parlement européen et du Conseil du 28 novembre 2018 relatif à l'utilisation du système d'information Schengen aux fins du retour des ressortissants de pays tiers en séjour irrégulier, le Règlement (UE) 2018/1861 du Parlement européen et du Conseil du 28 novembre 2018 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen (SIS) dans le domaine des vérifications aux frontières, modifiant la convention d'application de l'accord de Schengen et modifiant et abrogeant le règlement (CE) n° 1987/2006 et le Règlement (EU) 2018/1862 du Parlement européen et du Conseil du 28 novembre 2018 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen (SIS) dans le domaine de la coopération policière et de la coopération judiciaire en matière pénale, modifiant et abrogeant la décision 2007/533/JAI du Conseil, et abrogeant le règlement (CE) n° 1986/2006 du Parlement européen et du Conseil et la décision 2010/261/UE de la Commission.

d'une demande est un *« article 24 Entry ban »*, le COC transmet cette demande pour traitement à l'OE conformément aux conventions susmentionnées.

18. Cette communication doit évidemment rester possible, de sorte qu'il est indiqué de reprendre également l'Organe de contrôle de l'information policière parmi les destinataires légitimes des données à caractère personnel collectées par l'OE vu qu'il est, tout comme les médiateurs fédéraux, une institution ayant droit à une dotation du Parlement fédéral et l'autorité de protection des données et de contrôle notamment de la GPI. Même si l'on argumentait que le COC relèverait de l'application des articles 28 et suivants de l'avant-projet, cela ne semble pas apporter de solution étant donné qu'il semble s'agir là d'un accès effectif (après autorisation du ministre compétent) aux banques de données de l'OE, ce qui n'est pas à l'ordre du jour pour le COC et n'est d'ailleurs pas demandé.
Pour terminer, on peut se demander s'il ne faut pas formuler la même remarque pour le Comité permanent de contrôle des services de renseigenements (Comité R) et l'Autorité de protection des données (APD).

3. L'accès aux fichiers de journalisation

19. Le projet d'article 36 prévoit un accès limité aux fichiers de journalisation visés aux articles 32 et 33 (ou enregistrements d'un certain nombre de métadonnées). L'intention ne semble pas être de rendre l'accès aux fichiers de journalisation impossible pour les services de police et les autorités judiciaires, et l'exposé des motifs le confirme en précisant que *« selon les recommandations de l'Agence nationale de la sécurité des systèmes d'information, le personnel habilité doit, d'une part, être soumis à des obligations de confidentialité particulières et ne peut divulguer ces informations que dans des cas limités liés au fonctionnement technique ou à la sécurité des systèmes et, d'autre part, ne doit subir aucune contrainte quant au dévoilement des informations sauf si la loi en dispose autrement (par exemple, dans le cadre d'une procédure judiciaire[10]) »*.

Il va en effet de soi que les fichiers de journalisation doivent être accessibles pour la police et la justice dans le cadre de leurs missions légales. Il est donc indiqué de faire commencer l'article 36 par la formulation *« Sous réserve des exceptions légales, en vue des finalités … »*. De cette manière, il sera clair que ce projet d'article 36 ne porte pas préjudice aux dispositions

[10] Soulignement propre.

légales notamment du Code d'instruction criminelle ou des lois pénales spéciales, ni aux compétences d'investigation de la police.

Quoi qu'il en soit, l'objectif doit être de conserver tant au niveau de l'OE qu'au niveau du N.SIS II des fichiers de journalisation accessibles pour la police et la justice. Sans cela, la police pourrait savoir que l'OE a procédé à une consultation ou à un traitement dans le N.SIS II, mais sans pouvoir déterminer par qui au sein de l'OE ce traitement a été effectué, ce qui est bien sûr à éviter.

PAR CES MOTIFS,

l'Organe de contrôle de l'information policière

prie le demandeur de donner suite aux remarques et recommandations qui précèdent.

Avis approuvé par l'Organe de contrôle de l'information policière le 14 juillet 2022

Pour l'Organe de contrôle,
Le Président,
(s) Philippe ARNOULD