ORGANE DE CONTRÔLE DE L'INFORMATION POLICIÈRE

Votre référence	Notre référence	Annexe(s)	Date
	DA200002		10 avril 2020

<u>Objet</u> : Demande d'avis concernant un protocole d'accord entre l'Office des étrangers et la police fédérale relatif à la mise en place et aux modalités en matière de transmission automatisée d'empreintes digitales

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, en particulier l'article 4, § 2, troisième alinéa.

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 d'avis du Ministre de l'intérieur ('le demandeur') du 16 mars 2020, en vertu de la LPD susmentionnée.

Vu le rapport de Monsieur Koen Gorissen, membre-conseiller de l'Organe de contrôle.

Émet, le 10 avril 2020, 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 profondément modifié les tâches et les missions de l'Organe de contrôle. L'article 4, § 2, quatrième alinéa de la loi organique du 3 décembre 2017 portant création de l'Autorité de protection des données (ci-après la 'LCA') 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, les compétences, missions et pouvoirs d'autorité de contrôle tels que prévus par le Règlement 2016/679 sont exercés par l'Organe de contrôle.

2. 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 loi sur la protection des données[3], l'article 36.4 du RGPD et l'article 28.2 de la Directive Police-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)[4] et 2 (pour les traitements opérationnels) de la LPD[5]. En outre, le COC a également une mission d'avis d'initiative, prévue à l'article 236, § 2 de la LPD, et une mission d'information générale du grand public, des personnes concernées, des responsables du traitement et des sous-traitants dans la matière du droit à la protection de la vie privée et des données, prévue à l'article 240 de la LPD.

3. 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[6].

---

[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 (ci-après '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' ou '*LED'* (*Law Enforcement Directive*)).

[3] Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel (ci-après la 'LPD').

[4] Article 4, § 2, quatrième alinéa de la LCA.

[5] Article 71, § 1er, troisième alinéa de la LPD.

[6] Article 236, § 2 de la LPD.

4. Enfin, l'Organe de contrôle est également chargé du contrôle de l'application du Titre 2 de la LPD et/ou du traitement de données à caractère personnel telles que visées 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 vis-à-vis des services de police, de l'Inspection générale de la police fédérale et de la police locale (ci-après l' '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 'BELPIU'), telle que visée dans le Chapitre 7 de la loi du 25 décembre 2016[7].

II. Objet de la demande

5. La demande d'avis porte sur un projet de protocole (ci-après 'le projet de protocole') entre l'Office des étrangers (ci-après 'l'ODE') et la police fédérale relatif à la mise en place et aux modalités en matière d'échange automatisé d'empreintes digitales.

6. D'une part, il est question de l'échange mutuel de données, dont principalement des empreintes digitales, entre l'ODE et les services de police, afin que l'ODE puisse exercer ses missions légales.
En effet, le projet de protocole indique que, via ses *livescans*, l'ODE relève des empreintes digitales dans le cadre de ses missions[8] et les enregistre sous forme de fiches dactyloscopiques. Celles-ci sont conservées dans son AFIS (*Automated Fingerprint Identification System* – ci-après 'l'AFIS de l'ODE').
La police fédérale quant à elle dispose d'une banque de données AFIS – BIS (*Automated Fingerprint Identification System of the Biometric Identification Service* – ci-après 'l'AFIS-BIS') dans laquelle sont conservées toutes les prises d'empreintes effectuées par les services de police dans le cadre de leurs missions[9].

7. Il ressort du projet que le fichier NIST[10] reprenant les images des empreintes digitales relevées par l'ODE est envoyé automatiquement de l'AFIS de l'ODE à l'AFIS-BIS afin que les empreintes digitales soient comparées. Dans un premier temps, les empreintes sont comparées de manière automatisée aux données de l'AFIS-BIS. Dans un deuxième temps, celles-ci font l'objet d'un contrôle et d'une vérification manuels avec des traces non encore identifiées.

Cet échange mutuel constitue un *workflow* automatisé entre l'ODE et les services de police.

8. Le point 3.1.1. du projet de protocole précise que si des empreintes transmises par l'ODE correspondent à des traces dactylaires[11] encore non identifiées dans l'AFIS-BIS liées à des enquêtes

[7] Article 71, § 1er, troisième alinéa *juncto* article 236, § 3 de la LPD.
[8] Loi du 15 décembre 1980 sur l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers, *M.B.*, 31 décembre 1980 (ci-après 'loi du 15 décembre 1980').
[9] Articles 44/1, §2, alinéa 2, 1° et 44/11/2 de la LFP.
[10] Fichier qui obéit à un format de données standard pour l'échange de données biométriques, qui permet à différents systèmes de communiquer entre eux.
[11] Point 3.1.1. du projet de protocole.

judiciaires, celles-ci et les éventuelles autres données d'identification fournies seront enregistrées dans l'AFIS-BIS et traitées, uniquement au niveau policier, en tant qu'élément d'enquête.

9. Dans le même sens, le point 3.2. indique que seule la réponse issue de la comparaison automatique sera communiquée à l'ODE de manière automatisée et comprendra l'historique des prises d'empreintes de la personne concernée. Il est spécifié au point 3.3. que l'ODE peut, après la réception de ces informations, procéder à une interrogation directe de la Banque de données nationale générale (ci-après la 'BNG') selon les règles et les conditions établies dans l'arrêté royal du 28 avril 2016[12] (ci-après 'l'AR interrogation directe') et le protocole d'accord[13] qui y est lié (ci-après 'le protocole d'interrogation directe').

10. Le projet de protocole indique que la réponse automatique de l'AFIS-BIS vers l'ODE peut être accompagnée, sur demande de l'ODE, du set d'empreintes relevées par les services de police.

11. D'autre part, il est question dans le projet de protocole d'un échange de données entre les services de police et l'ODE lorsque les services de police cherchent à identifier une personne dans le cadre d'une enquête ou cherchent à l'identifier et que cela n'est pas possible sur base de ses documents. Dans ces cas, les services de police transmettent leur demande à l'ODE, qui leur répondra suivant le modèle *HIT/NO HIT* accompagné le cas échéant d'un *webreport*, via le BIS ou sur la station *FIT livescan* du service de police demandeur.

Cet échange mutuel résulte de questions des services de police à l'ODE.

12. Les échanges mutuels d'empreintes digitales dont il est question concernent deux autorités qui se trouvent dans le champ de compétence de deux autorités de contrôle différentes à savoir l'Organe de contrôle de l'information policière (le COC) d'une part, et l'Autorité de protection des données d'autre part.
Le COC est compétent pour tous les traitements de données à caractère personnel effectués par les services de police, et il est chargé notamment de contrôler le traitement des informations et des données à caractère personnel visées aux articles 44/1 à 44/11/13 de la LFP, y compris celles enregistrées dans les banques de données visées à l'article 44/2 de la même loi[14].

13. Dès lors, l'examen réalisé dans le présent avis se concentrera sur les communications d'empreintes digitales qui tombent dans le champ de compétence de l'Organe de contrôle de l'information policière,

[12] Arrêté royal 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 (ci-après 'AR interrogation directe') et article 44/11/12 de la LFP.
[13] Protocole d'accord entre l'Office des étrangers et la police fédérale relatif à la mise en place et aux modalités de l'interrogation directe de la banque de données nationale générale par l'Office des étrangers en application de l'article 44/11/12, §1er, 2° de la loi sur la fonction de police, 29 septembre 2016 (ci-après 'protocole d'interrogation directe').
[14] Article 71 de la LPD.

c'est-à-dire les flux des données policières opérationnelles vers l'ODE ainsi que l'utilisation par les services de police des données transmises par l'ODE.

En revanche, il revient à l'Autorité de protection des données de s'exprimer quant à la légalité des flux de données de l'ODE vers les services de police.

III. Examen du projet de protocole

III.1. Bases légales applicables - Remarques générales

14. Les empreintes digitales constituent des données dites 'sensibles' dont le traitement est encadré de manière particulière.

Avant tout, il y a lieu de rappeler que les services de police peuvent traiter des données à caractère personnel en vue d'exercer leurs missions de police administrative et de police judiciaire[15].
Le traitement de données sensibles par ces services est également autorisé, en complément ou en soutien d'autres catégories de données visées à l'article 44/5 de la LFP, toujours afin d'exercer leurs missions[16]. Pour ce qui est des empreintes digitales, les services de police ne peuvent les traiter que dans le but d'assurer l'identification certaine de la personne concernée visée à l'article 44/5, § 1er, 2° à 7° et § 3 1° à 6° de la LFP[17]. En outre, la circulaire ministérielle OOP 44[18] permet aux services de police de recevoir de l'ODE les données nécessaires à l'identification des individus qu'ils contrôlent dans le cadre de l'article 34 de la LFP. Ces données comprennent notamment des empreintes digitales.

Quant à l'ODE, celui-ci peut, dans le cadre de ses missions, relever et traiter des données biométriques telles que des empreintes digitales[19].

15. Tel que l'Organe de contrôle le comprend, le projet de protocole a vocation à régler plusieurs échanges de données à caractère personnel.

Un échange automatisé (le premier échange) concerne la transmission automatique des empreintes relevées par l'ODE à l'AFIS-BIS et la réponse automatique de l'AFIS-BIS à l'ODE suite à une comparaison automatique des empreintes. Ces flux réciproques doivent permettre à l'ODE, en cas de *HIT*, d'identifier de manière certaine la personne concernée.
Un autre échange (le deuxième échange) concerne la transmission d'empreintes des services de police à l'ODE à des fins d'identification en cas de *HIT* dans l'AFIS de l'ODE.

[15] Articles 33 de la LPD et 44/1 de la LFP.
[16] Articles 34 de la LPD et 44/1, §2 de la LFP.
[17] Articles 34 et 44/1, §2, alinéa 2, 1° de la LFP.
[18] Circulaire ministérielle OOP 44 relative au contrôle renforcé sur la base de l'article 34 de la loi sur la fonction de police, *M.B.*, 30 novembre 2015.
[19] Articles 30bis, 51/3 et 57/31 de la loi du 15 décembre 1980.

16. En ce qui concerne le premier échange, tel que l'Organe de contrôle le comprend, le projet de protocole a vocation à régler un échange de données préalable à l'interrogation directe de la BNG par les membres du personnel de l'ODE spécialement autorisés.

En effet, l'accès ou l'interrogation directs de la BNG peuvent être octroyés à certaines autorités autres que les services de police, selon les modalités déterminées par arrêté royal[20].

L'AR interrogation directe concrétise cette possibilité pour l'ODE et est accompagné d'un protocole d'accord qui règle les modalités de l'interrogation directe pour l'ODE ainsi que les modalités concrètes de sécurisation[21] (le protocole d'interrogation directe).

Ainsi, les membres autorisés de l'ODE peuvent procéder à une interrogation directe de la BNG. Quant à la portée de cette interrogation, elle est circonscrite à l'article 4 de l'AR interrogation directe. L'ODE est aussi dans ce cadre mis au courant des mesures à prendre qu'il aurait lui-même demandées dont il doit logiquement déjà être au courant[22], cela afin de lui assurer une vue complète des données dont les services de police disposent[23].

Les données et les informations issues de l'interrogation directe de la BNG ne peuvent être utilisées par l'ODE que pour la prise de décision en application de la loi sur l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers (ci-après 'la loi du 15 décembre 1980'), c'est-à-dire que l'ODE ne peut les utiliser qu'afin de vérifier que la personne concernée ne représente pas un danger pour l'ordre public, la sécurité nationale et la tranquillité publique[24].

Afin d'obtenir les informations souhaitées, l'ODE doit disposer des données d'identification de la personne concernée[25]. L'interrogation directe a lieu sur la base des noms et prénoms des personnes concernées, avec éventuellement une date de naissance (complète ou non), ou sur la base du numéro de registre national[26].

17. Ainsi, vu le projet de protocole faisant l'objet du présent avis et selon les éléments exposés ci-dessus, l'Organe de contrôle voit dans le projet de protocole la volonté de fournir à l'ODE une possibilité supplémentaire de disposer des données d'identification nécessaires à l'interrogation directe de la BNG : par cet échange automatique, c'est l'AFIS-BIS qui est questionné et non la BNG qui sera interrogée par la suite et à d'autres fins. En effet, en cas de *HIT* dans l'AFIS-BIS, la réponse automatique

[20] Article 44/11/12 de la LFP.
[21] Article 6 de l'AR interrogation directe ; Arrêté royal du 28 avril 2016, Rapport au Roi, *M.B.*, 12 mai 2016, p. 31191 et 31195.
[22] Arrêté royal du 28 avril 2016, Rapport au Roi, *M.B.*, 12 mai 2016, p. 31193.
[23] *Ibidem*, p. 31193.
[24] Article 4 de l'AR interrogation directe et point 8. du Protocole d'interrogation directe.
[25] Arrêté royal du 28 avril 2016, Rapport au Roi, *M.B.*, 12 mai 2016, p. 31192.
[26] Point 3.1.a) du Protocole d'interrogation directe.

doit permettre à l'ODE d'identifier de manière certaine la personne concernée. Celui-ci pourra ensuite procéder à l'interrogation directe dans la BNG en vue de prendre sa décision.

Ce premier échange ne peut suffire à l'ODE pour ses vérifications en matière d'ordre public, de sécurité nationale et de tranquillité publique. En effet, le *HIT* dans l'AFIS-BIS et les éventuelles liaisons aux empreintes relevées par les services de police ne reflètent pas tous les éléments pertinents[27] nécessaires pour la prise de décision de l'ODE dans la cadre de la loi du 15 décembre 1980.

Ces précisions faites, l'Organe de contrôle demande que les objectifs du premier échange soient clairement identifiés dans le projet de protocole.

18. Le projet de protocole renvoie, pour base légale, à l'article 44/11/9, §1er et §4 de la LFP.
L'Organe de contrôle profite de ce renvoi afin de souligner que, au moment de la rédaction du présent avis, les directives des ministres de l'Intérieur et de la Justice auxquelles renvoie le paragraphe 1er de l'article 44/11/9 n'existent pas. Ces directives doivent comprendre les modalités des communications inclues dans l'article 44/11/9, §1er de la LFP.
Ni la LFP, ni les travaux préparatoires qui se rapportent à cet article ne permettent d'identifier précisément ce que qu'il y a lieu d'entendre par *« les modalités »* que ces directives doivent déterminer. La nature et le contenu des communications qui pourraient être réalisées dans le cadre de l'article 44/11/9, §1er sont variés, ce qui fait présumer à l'Organe de contrôle que les modalités que les directives des ministres doivent déterminer comprendraient au moins le type de données qui peuvent être communiquées, par qui[28], à qui et pour quelles finalités. Cependant, la manière de procéder à ces communications, c'est-à-dire les canaux utilisés, selon quelles mesures de sécurité, avec quelle durée de conservation, le système de login, etc. pourraient, d'initiative et dans une optique de transparence et aux fins d'objectifs de sécurité, être inscrits dans des protocoles permettant aux parties de se référer à des consignes écrites et à des procédures communes établies au préalable.

L'Organe de contrôle invite à nouveau les ministres concernés à mettre en place les directives adéquates visées à l'article 44/11/9, §1er de la LFP – il s'agit d'une obligation qui existe depuis le 7 avril 2014 - afin que les protocoles d'accord conclus dans le cadre de l'article 44/11/9 les suivent et les complètent et non l'inverse.

19. Quant au paragraphe 4 de l'article 44/11/9, celui-ci concerne les communications venant des autorités/organes/organismes publics visés notamment au paragraphe 1er, c'est-à-dire aussi l'ODE, aux services de police. Les modalités de ces communications doivent cette fois-ci être précisées dans un protocole d'accord approuvé par les ministres concernés[29].

[27] Arrêté royal du 28 avril 2016, Rapport au Roi, *M.B.*, 12 mai 2016, p. 31192 31193.
[28] A titre d'exemple, le personnel de l'ODE habilité à recevoir et traiter les réponses automatiques de l'AFIS-BIS pourrait y être identifié selon des critères clairs.
[29] Article 44/11/9, §4, alinéa 2 de la LFP.

20. Par conséquent, à titre subsidiaire et sous réserve des remarques mentionnées au paragraphe 19, eu égard à l'absence de directives ministérielles fixant les modalités de communication des services de police à l'ODE et vu l'objet du projet de protocole, l'Organe de contrôle demande que celui-ci prévoie au moins les données pouvant être communiquées, par qui et à qui, les finalités de ces communications, les canaux utilisés, qui peut les utiliser, ce qui a été prévu au niveau des mesures techniques et organisationnelles appropriées et des mesures de sécurité nécessaires qui entourent ces communications, la durée et les modalités de conservation des données et informations échangées, la politique en matière d'accès à ces données, l'utilisation qui peut en être faite et la gestion des incidents, le tout au regard de l'avis des Délégués à la protection des données (ci-après les '*DPO*') désignés et de l'/des analyse(s) d'impact réalisée(s).

Par exemple, le projet de protocole fait référence à l'utilisation future de *web services* sans indiquer pour quelles raisons, ni les mesures de sécurité qui seront prévues et n'indique pas le canal de communication qui sera utilisé avant le recours à ce système, ni les garanties qui l'entourent.

21. Le degré de précision de ces modalités dans le protocole doit varier en fonction des impératifs de proportionnalité et de sécurité. Cela nécessite qu'une analyse d'impact et que l'avis des *DPO* concernés soient demandés et pris en compte pour la rédaction du protocole.

En effet, le projet de protocole indique que les parties s'engagent à réaliser ensemble une *DPIA* (analyse d'impact et des risques) conformément à l'article 35 du RGPD. En premier lieu, afin que les obligations de toutes les parties au protocole soient mentionnées, l'Organe de contrôle invite également à faire référence à l'article 58 de la LPD. En deuxième lieu, il est indispensable que cette analyse – de même que les avis des *DPO* concernés – soit réalisée **avant** l'élaboration du protocole et surtout avant la concrétisation des échanges mutuels dont question.

En effet, cette analyse – et ces avis – permettront d'identifier les mesures nécessaires et adéquates ainsi que les questions pertinentes auxquelles le protocole doit répondre. De plus, les articles 35 du RGPD et 58 de la LPD demandent que la *DPIA* soit réalisée **préalablement** au traitement. Pour le surplus et le contenu minimum de cette analyse, l'Organe de contrôle renvoie aux indications des articles cités.

22. Le projet de protocole indique également tenir compte du RGPD et de la LPD. Celui-ci renvoie particulièrement à l'article 32 du RGPD qui concerne les mesures techniques et organisationnelles appropriées[30]. D'une part, afin que les obligations de toutes les parties au protocole soient mentionnées, il y a lieu de faire référence aussi aux articles 50, 51 et 60 de la LPD. D'autre part, les points 5.2. et 5.3. du projet indiquent certaines mesures de sécurité qui seront prises par les parties et le point 5.6. est

[30] Point 5.1. du projet de protocole.

fort flou quant à la confidentialité des données. A ce stade, l'Organe de contrôle ne peut dès lors se faire une idée des mesures éventuellement prises ou de celles encore à prendre.

Le lancement des échanges mutuels en question ne peut être réalisé dans ces conditions.

L'Organe de contrôle demande dès lors que des mesures concrètes et adéquates soient prises en matière de sécurité, de confidentialité, d'accès aux données, de gestion des incidents et de durée de conservation notamment, et ce avant la signature d'un protocole entre les parties. Le COC souhaite en être mis au courant avant la mise en œuvre des échanges mutuels.

23. L'Organe de contrôle souhaite également rappeler les missions et le statut du *DPO* qui est notamment chargé de contrôler le respect de la réglementation et des règles internes du responsable du traitement en matière de protection des données à caractère personnel, et qui doit pouvoir exercer ses missions en toute indépendance[31]. Dès lors, l'autorisation préalable que devraient recevoir les *DPO* de l'ODE et de la police fédérale afin de réaliser un audit opérationnel n'assure pas cette indépendance[32].

D'ailleurs, le projet de protocole mentionne « *le DPO de la police fédérale*[33] ». L'Organe de Contrôle suppose que le DPO compétent dont question est celui de la Direction de la police technique et scientifique (DJT).

De plus, le projet de protocole fait référence à la publication d'un rapport annuel relatif aux comparaisons d'empreintes digitales effectuées sans mentionner où ce rapport sera publié. L'Organe de contrôle demande que le projet de protocole précise les modalités ainsi que les destinataires de cette publication et souhaite faire partie de ces destinataires.

24. En ce qui concerne le point 5.7. du projet de protocole, relatif au droit d'accès des citoyens aux données transmises dans le cadre du protocole, l'Organe de contrôle recommande d'ajouter qu'en ce qui concerne les données envoyées par l'ODE aux services de police, le droit d'accès s'exerce conformément à l'article 15 du RGPD. En effet, l'ODE reste responsable des données et des informations qu'il traite et qu'il transmet à des tiers, ce qui a pour conséquence que les demandes d'accès à ces données des personnes concernées doivent être adressées à l'ODE.

Le droit d'accès devra en revanche être exercé selon les modalités des articles 41 et 42 de la LPD uniquement en ce qui concerne les données et informations traitées par les services de police, en ce compris les empreintes digitales enregistrées dans l'AFIS-BIS suite à la transmission de l'ODE et utilisées par les services de police pour leurs missions légales.

[31] Articles 63 à 65 de la LPD.
[32] Point 6. du projet de protocole.
[33] *Ibidem.*

25. Vu ce qui précède, l'Organe de contrôle invite les ministres concernés à déterminer les modalités de communication dans des directives conformément au prescrit de l'article 44/11/9, §1er de la LFP.

A titre subsidiaire et étant donné les remarques formulées ci-dessus, il est requis du demandeur de faire procéder, en premier lieu, à une analyse d'impact et de demander un avis aux *DPO* désignés des deux autorités. En deuxième lieu, l'Organe de contrôle demande que les mesures adéquates de sécurité soient établies et mises en œuvre, de même que l'identification dans le protocole au minimum des données et des destinataires concernés, des canaux utilisés, de leurs utilisateurs autorisés, de la durée et des modalités de conservation des données échangées, de la politique en matière d'accès aux données et leur utilisation ainsi que de la gestion des incidents, et ce **avant** le lancement de l'échange mutuel de données.

L'Organe de contrôle demande également que l'indépendance totale des *DPO* concernés soit garantie et que les modalités de publication et les destinataires du rapport annuel relatif aux comparaisons d'empreintes digitales soient précisées. L'Organe de contrôle rappelle qu'il souhaite recevoir ce rapport annuel. Mais encore, le COC demande que l'autorité auprès de qui le droit d'accès aux données peut être exercé soit clairement définie pour chaque cas de figure.

III.2. Remarques spécifiques quant au flux des données policières opérationnelles vers l'ODE (dans le cadre du premier échange)

26. Avant toute chose, eu égard au caractère sensible des données concernées et aux règles spécifiques qui s'y attachent, l'Organe de contrôle invite les parties à rappeler dans le projet de protocole les garanties supplémentaires prévues dans la LPD[34] (et dans le RGPD).

27. Les réponses automatiques de l'AFIS-BIS en cause au présent constituent des communications de données et d'informations des services de police à l'ODE pour permettre à celui-ci de disposer des données d'identification nécessaires à l'interrogation directe de la BNG par ses services, afin d'exercer ses missions légales inscrites dans la loi du 15 décembre 1980. Dès lors, l'Organe de contrôle recommande d'inscrire clairement aux points 4.1.2. et 8.1. les finalités de ces communications plutôt que de faire référence « *aux recherches ultérieures* » et « *aux fins de traitement ultérieur par le service concerné de l'ODE* ».

28. L'Organe de contrôle remarque aussi que le projet de protocole décrit un processus de « *workflow automatisé*[35] », qui pourrait être interprété comme une transmission automatique mais aussi systématique des empreintes relevées par l'ODE à l'AFIS-BIS.

[34] Article 29, §3 et §5 de la LPD.
[35] Point 3.1. du projet de protocole.

L'Organe de contrôle demande qu'il soit précisé dans le projet de protocole si la transmission des empreintes de l'ODE vers l'AFIS-BIS est automatique et systématique, et que les modifications des bases légales applicables soient réalisées le cas échéant.

29. Le projet de protocole indique qu'en cas de *HIT*, la réponse automatique de l'AFIS-BIS à l'ODE comprendra l'historique des prises d'empreintes et précise que, à la demande de l'ODE, le set d'empreintes complet lui sera envoyé. L'échange dont question ne devant permettre à l'ODE que de disposer des données nécessaires à l'identification précise de la personne concernée, dès lors, l'Organe de contrôle ne trouve pas dans le projet de protocole de justification quant à la communication sur demande du set d'empreintes. En effet, les services de police peuvent communiquer à l'ODE les données et informations « *pour lui permettre d'exercer ses missions légales*[36] », mais ces communications sont toujours soumises au principe de proportionnalité et aux principes du traitement repris à l'article 28 de la LPD. Ainsi, l'Organe de contrôle demande que la réponse automatique de l'AFIS-BIS ne contienne que les données nécessaires à l'identification précise de la personne concernée. Si ces données correspondent aux données reprises à l'annexe 1 du projet de protocole, l'Organe de contrôle demande qu'un descriptif complet de ces données soit inséré dans le protocole et non dans une annexe de celui-ci.

30. Le projet de protocole indique que les empreintes transmises par l'ODE « *ne pourront pas non plus ultérieurement être accessibles aux fins de recherche pour la police fédérale*[37]*.* » Le projet indique également que, sauf concordance avec des traces dactylaires non identifiées dans le cadre d'une enquête judiciaire, les empreintes envoyées par l'ODE ne seront pas conservées dans l'AFIS-BIS[38]. Le projet indique aussi que les réponses automatiques envoyées à l'ODE seront également transmises à la Direction des opérations de police administrative (DAO) « *pour suite du traitement policier*[39]*.* »

L'Organe de contrôle souhaite rappeler que les informations communiquées aux services de police deviennent, une fois transmises, la propriété de ces services. Cela signifie que les finalités pour lesquelles ces données et informations transmises peuvent être traitées par les services de police ne peuvent être circonscrites ou limitées, sauf exception légale spécifique, à certains services ou à certaines finalités. Ces informations et données policières peuvent être traitées pour les finalités spécifiques de l'article 27 de la LPD, toujours dans le respect des règles en matière de protection des données et de gestion de l'information policière, en ce compris les articles 34 et 44/1, §2, 1° de la LFP ainsi que les principes du traitement inscrits dans la LPD et le principe de proportionnalité.

31. L'Organe de contrôle demande également que dans le cas où le projet se concrétise, la déclaration dans le registre de traitements REGPOL de la police intégrée soit complétée afin de refléter les nouvelles

[36] Article 44/11/9, §1er de la LFP.
[37] Point 3.1.1. du projet de protocole.
[38] *Ibidem.*
[39] Point 3.1.4. du projet de protocole.

communications de données qui auront lieu[40]. Le COC invite également le responsable du traitement à veiller à ce que les demandes de consultation de l'AFIS-BIS résultant d'une demande de l'ODE puissent être identifiées au moyen des fichiers de journalisation[41].

32. Vu ce qui précède, l'Organe de contrôle demande des précisions sur les finalités de l'échange mutuel dont il est question et demande qu'un descriptif complet des données qui sont envoyées à titre de réponse automatique de l'AFIS-BIS à l'ODE dans le protocole soit apporté. L'Organe de contrôle demande également que les points du projet de protocole concernant les possibilités de réutilisation des données et informations par les services de police soient revus et adaptés selon ses remarques du paragraphe 30.

III.3. Remarques particulières quant à l'utilisation par les services de police des données transmises par l'ODE (dans le cadre du deuxième échange)

33. L'Organe de contrôle recommande, afin d'éviter des confusions, que les modalités du deuxième échange ne soient pas réglées dans un projet de protocole qui concerne, de manière principale, un autre échange de données. Il y a lieu de séparer les deux échanges et de leur garantir à chacun une assise claire et complète. A tout le moins, les deux échanges devraient être traités dans des chapitres différents.
L'Organe de contrôle ne peut identifier clairement si ce sont des questions ponctuelles que les services de police adressent à l'ODE ou si les échanges envisagés sont en réalité plus récurrents. Il revient au demandeur d'éclaircir ce point.
Ainsi, l'Organe de contrôle demande que la nature, les objectifs et les bases légales du deuxième échange soient précisément identifiés.

34. De plus, le projet de protocole indique avoir pour objet de déterminer, entre l'ODE et la police fédérale, les modalités de transmission mutuelle de données d'empreintes digitales des étrangers, **dont celles** des demandeurs de protection internationale se présentant à l'ODE[42]. L'Organe de contrôle demande d'éclaircir cette transmission, et de définir de quelles données d'empreintes digitales il s'agit : est-il question uniquement des empreintes digitales des demandeurs de protection internationale ou d'autres personnes sont-elles concernées ?

Il est fait référence dans le projet aux missions légales de chacune de ces autorités, à savoir la loi du 15 décembre 1980 pour l'ODE, et l'article 30*bis* de la même loi ainsi que la Circulaire ministérielle OOP 44 pour la police fédérale.

[40] Article 55 de la LPD et article 145 de la loi du 7 décembre 1998 sur la police intégrée, structurée à deux niveaux, *M.B.,* 5 janvier 1999.
[41] Article 56 de la LPD et article 44/11/12, §8 de la LFP.
[42] Point 1.3. du projet de protocole.

Néanmoins, le point 3.4. du projet de protocole semble envisager de manière plus large ces échanges mutuels de données, puisqu'il fait référence « *aux services de police* ». Le point 8.2. du projet de protocole quant à lui fait référence à « *la police* » qui n'utilisera les données « *que dans le cadre de ses missions légales, dont celles découlant des articles 14 et 15 de la LFP* ». Le paragraphe 2 du même point fait référence à la « *police fédérale* ».

Afin d'identifier précisément les parties concernées et de déterminer clairement le champ d'application de l'échange envisagé, l'Organe de contrôle demande que les modifications et précisions nécessaires soient apportées, c'est-à-dire de déterminer les données de qui sont concernées, qui sont les parties au protocole et qui peut utiliser ces données, et dans le cadre de quelle(s) mission(s). Suivant ces réponses, l'Organe de contrôle demande que toutes les parties soient associées pour l'élaboration du protocole.

35. L'Organe de contrôle souhaite rappeler que les informations communiquées aux services de police deviennent, une fois transmises, la propriété de ces services. Cela signifie que ces informations et données policières peuvent être traitées pour les finalités spécifiques de l'article 27 de la LPD, toujours dans le respect des règles en matière de protection des données et de gestion de l'information policière, en ce compris les articles 34 et 44/1, §2, 1° de la LFP ainsi que les principes du traitement inscrits dans la LPD et le principe de proportionnalité. Les finalités pour lesquelles ces données et informations transmises peuvent être traitées par les services de police ne peuvent donc être circonscrites ou limitées à certains services ou à certaines finalités, sauf en cas d'exception légale spécifique.

PAR CES MOTIFS,

l'Organe de contrôle de l'information policière,

invite le demandeur à tenir compte des remarques susmentionnées,

demande qu'il soit donné suite aux considérations et questions formulées aux paragraphes 25 et 32 à 35,

invite le demandeur, eu égard au caractère sensible des données concernées, à lui fournir des réponses aux questions, considérations et remarques faites dans le présent avis.

Avis approuvé par l'Organe de contrôle de l'information policière le 10 avril 2020.

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