



Avis n° 32/2016 du 29 juin 2016

Objet: Avis d'initiative concernant une demande de communication de données biométriques introduite par l'ambassade américaine auprès du SPF Affaires étrangères (CO-A-2016-008)

La Commission de la protection de la vie privée (ci-après « CPVP »);

Vu la loi du 8 décembre 1992 *relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel* (ci-après « LVP »), en particulier l'article 29 ;

Vu la question adressée à la CPVP par le SPF Affaires étrangères le 20 octobre 2015 ;

Vu le rapport de Monsieur Gert Vermeulen, Commissaire ;

Émet, le 29/06/2016, l'avis suivant :

REMARQUE PRELIMINAIRE

La Commission attire l'attention sur le fait qu'une nouvelle réglementation européenne relative à la protection des données à caractère personnel a été promulguée récemment : le Règlement 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 la Directive Police et Justice. Ces textes ont été publiés au journal officiel de l'Union européenne le 4 mai 2016^[1].

Le Règlement, couramment appelé GDPR (General Data Protection Regulation), est entré en vigueur vingt jours après sa publication, soit le 24 mai 2016, et sera automatiquement d'application deux ans plus tard, soit le 25 mai 2018. La Directive Police et Justice doit être transposée dans la législation nationale au plus tard le 6 mai 2018.

Pour le Règlement, cela signifie qu'à partir du 24 mai 2016 et pendant le délai de deux ans de mise en application, les États membres ont d'une part une obligation positive de prendre toutes les dispositions d'exécution nécessaires, et d'autre part une obligation négative, appelée "devoir d'abstention". Cette dernière obligation implique l'interdiction de promulguer une législation nationale qui compromettrait gravement le résultat visé par le Règlement. Des principes similaires s'appliquent également pour la Directive.

Il est dès lors recommandé d'anticiper éventuellement dès à présent ces textes. Et c'est en premier lieu au(x) demandeur(s) d'avis qu'il incombe d'en tenir compte dans ses (leurs) propositions ou projets. Dans le présent avis, la Commission a d'ores et déjà veillé, dans la mesure du possible et sous réserve d'éventuels points de vue complémentaires ultérieurs, au respect de l'obligation négative précitée.

I. OBJET DE L'AVIS

1. Le SPF Affaires étrangères a contacté la CPVP au sujet d'une demande de communication de données biométriques lui étant adressée par les services de l'ambassade américaine à Bruxelles. Il s'agit des données biométriques de quatre ressortissants burundais faisant l'objet de sanctions européennes (interdiction d'accès au territoire et gel des avoirs) suite à des actes

^[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)

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

<http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=OJ%3AL%3A2016%3A119%3ATOC>

<http://eur-lex.europa.eu/legal-content/NL/TXT/?uri=OJ:L:2016:119:TOC>

de violence, de répression ou d'incitation à la violence qu'ils sont réputés avoir commis (décision PESC 2015/1763 du Conseil du 1^{er} octobre 2015).

2. Selon les informations fournies par le SPF Affaires étrangères à la CPVP, le but déclaré de cette démarche de l'ambassade américaine est d'organiser des sanctions similaires à l'égard de ces individus aux USA.
3. Les données biométriques reçues par le SPF Affaires étrangères proviennent d'une demande de visa formulée par les quatre burundais concernés à l'ambassade belge de Bujumbura, selon les dernières informations communiquées à la CPVP par le SPF Affaires étrangères¹.
4. La CPVP a estimé opportun d'émettre un avis d'initiative à ce sujet.

II. ANALYSE

5. L'article 5 de la loi du 8 décembre 1992 sur la protection de la vie privée (ou « *LVP* ») dispose que les données à caractère personnel ne peuvent être traitées que dans un nombre limité de cas, comme par exemple, sur base du consentement indubitable de la personne concernée, ou lorsque le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable de traitement est soumis, ou encore, lorsque le traitement est nécessaire à l'exécution d'une mission d'intérêt public dont est investi le responsable de traitement. Il convient d'examiner si une de ces bases légales potentielles peut être invoquée par le SPF Affaires étrangères en ce qui concerne le traitement et la communication de données biométriques récoltées dans le cadre de l'octroi de visas.
6. Les données biométriques visées dans la demande de l'ambassade américaine ont été collectées par le SPF Affaires étrangères dans le cadre de la délivrance d'un visa sollicité auprès de l'ambassade belge à Bujumbura.
7. Le SPF Affaires étrangères n'a précisé à la CPVP le type de visa dont question. Il peut donc s'agir d'une demande de visa de court séjour de type « *Schengen* », ou d'une demande de visa national pour un séjour de plus de 90 jour². Comme explicité ci-dessous, la récolte de

¹ Précisons que l'origine de ces données biométriques a fait l'objet d'une rectification de la part du SPF Affaires étrangères. Tout d'abord, le SPF a écrit à la CPVP que les données biométriques concernées lui ont été transmises par les Services Généraux du Renseignement et de la Sécurité (SGRS) ; ultérieurement, le SPF a rectifié cette information et a déclaré que ces données lui avaient été transmises dans le cadre d'une demande de visa formulée par les quatre burundais auprès de l'ambassade belge à Bujumbura.

² Pour une description des type de visa disponibles pour la Belgique (visa national de séjour de plus de 90 jours ; visa pour un séjour de maximum 9 jours, visa de transit), voir le site des Affaires étrangères à la page suivante : http://diplomatie.belgium.be/fr/Services/venir_en_belgique/visa_pour_la_belgique/veelgestelde_vragen/types_de_visa ou le

données biométriques dans ces deux hypothèses, est réalisée pour des finalités bien délimitées par la législation applicable, et le SPF Affaires Intérieures est responsable du traitement des données collectées dans le cadre des demandes de visa formées à partir d'une ambassade ou d'un consulat étranger, même si les données y ont été collectées et traitées par le SPF Affaires Etrangères (ambassade).

(a) Responsable du traitement des données visa

8. Le SPF Intérieur est l'autorité compétente en matière d'accès au territoire, de séjour, d'établissement et d'éloignement des étrangers en Belgique (la loi du 15 décembre 1980 sur l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers, ci-après « *Loi Etrangers* », article 1 2°)³.
9. A ce titre, le SPF Intérieur (Office des Etrangers) est l'autorité compétente pour la délivrance de visas d'entrée dans l'espace Schengen, que ce soit pour un court séjour, un transit, ou long séjour.
10. En matière de court séjours (moins de 90 jours) et de transit, le Règlement CE n° 810/2009 du Parlement européen et du Conseil du 13 juillet 2009 établissant un code communautaire des visas (ci-après « *Code des visas* ») fixe les procédures et les conditions de délivrance des visa dans l'Espace Schengen. L'article 4 du Code des visas prévoit que les demandes de visas sont examinées par les consulats. Un Etat membre peut demander qu'un autre de ses services participe à l'examen des demandes de visas et des décisions à leur sujet. En l'occurrence, la Belgique a désigné l'Office des Etrangers du SPF Intérieur comme autorité centrale chargée de la délivrance des visas Schengen⁴.
11. C'est également le SPF Intérieur qui est l'autorité responsable de la délivrance des visas pour un long séjour (plus de trois mois) en Belgique (par exemple, pour travailler en Belgique)⁵.

site de l'Office des étrangers à la page suivante : https://dofi.ibz.be/sites/dvzoe/FR/Guidedesprocedures/Pages/Suis_je_soumis_a_l_obligation_de_visa.aspx.

³ Pour une description des compétences de l'Office des étrangers en matière d'accès au territoire, voir le site Internet <https://dofi.ibz.be/sites/dvzoe/FR/Apropos/Pages/Competences.aspx>.

⁴ Voir la Décision de la Commission 2014/C 106/04 « Liste des autorités compétentes dont le personnel dûment autorisé sera habilité à saisir, à modifier, à effacer ou à consulter des données dans le système d'information sur les visas (VIS) » [http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:52014XC0409\(01\)&from=FR](http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:52014XC0409(01)&from=FR).

⁵ Article 61/27 de la Loi Etrangers.

12. Le SPF Intérieur (son administration « *Office des étrangers* ») est d'ailleurs désigné comme responsable de traitement dans les demandes de visas de type « *Schengen* » ou « *long séjour* » disponibles sur son site⁶.
13. Lorsque les demandes de visas sont formées auprès d'un poste consulaire ou diplomatique belge à l'étranger, le SPF Intérieur collabore étroitement avec le SPF Affaire étrangère pour la récolte et le traitement des données nécessaires au traitement de la demande⁷.
14. Lorsqu'une prise d'empreinte biométrique est réalisée dans le cadre d'une demande de visa formée dans un pays tiers, cette collecte de données est effectuée par le représentant consulaire ou diplomatique local auprès duquel la demande est introduite (article 30bis § 3 de la Loi Etrangers)⁸.
15. Il incombe toutefois à l'Office des étrangers, en tant que responsable du traitement de ces données, de se prononcer sur la demande de transfert de données introduite par l'ambassade américaine auprès du SPF Affaires Etrangères dans le cadre d'une demande de visa⁹.

(b) Finalités de traitement

16. La Loi Etrangers spécifie expressément que les données biométriques prises à une telle occasion ne peuvent être utilisées que « *dans la mesure où elles sont nécessaires pour : 1° établir et/ou vérifier l'identité de l'étranger ; 2° examiner si l'étranger concerné constitue un danger pour l'ordre public ou la sécurité nationale ; 3° respecter les obligations prévues par les règlements et directives européens adoptés par le Conseil de l'Union européenne* » (article 30bis § 4 de la Loi Etrangers).

⁶ Exemples demandes de visa court « Schengen » (https://dofi.ibz.be/sites/dvzoe/FR/Guidedesprocedures/Pages/Formulaire_de_demande_visa_SCHENGEN.aspx), ou long séjour pour la Belgique (https://dofi.ibz.be/sites/dvzoe/FR/Guidedesprocedures/Pages/Formulaire_de_demande_de_visa_long_sejour_pour_la_Belgique.aspx).

⁷ Sur le rôle du SPF Affaires étrangères dans les demandes de visa, voir la page Internet suivante : http://diplomatie.belgium.be/fr/Services/venir_en_belgique/visa_pour_la_belgique.

⁸ Un étranger, à savoir, quiconque ne fournit pas la preuve qu'il possède la nationalité belge, peut être soumis à une prise de données biométriques (prise d'empreintes digitales et de photographies) lorsqu'il demande un visa, auprès d'un représentant diplomatique ou consulaire belge (article 1 *juncto* article 30bis § 2 1° de la Loi Etrangers). Les données biométriques sont alors prises à l'initiative du représentant diplomatique ou consulaire belge (article 30bis § 3 de la Loi Etrangers).

⁹ Précisons que si dans les faits, il devait s'avérer que le SPF Affaires étrangères se prononce sur les demandes de transfert des données VIS à sa disposition, ce SPF prendrait alors de facto une responsabilité de co-responsable du traitement, et l'information aux demandeurs de VISA devrait être mise à jour sur ce point (pour autant que la législation permette au SPF Affaires étrangères de prendre cette responsabilité, ce qui n'est pas établi et ne fait pas l'objet du présent avis). Sur les notions de « responsable de traitement » et de « sous-traitant », voir l'avis du Groupe 29 du 16 février 2010, « *Opinion 1/2010 (the "Opinion") on the concepts of "controller" and "processor"* ».

17. Il s'agit de finalités bien déterminées et strictement limitées. Les deux premières finalités mentionnées ci-dessus ne semblent pas recouvrir la transmission de ces données à une autorité étrangère, telle que l'ambassade des Etats-Unis, aux fins de contrôler l'accès à son propre territoire. Il reste à déterminer si la troisième finalité peut offrir une base juridique au transfert envisagé, autrement dit, il convient de déterminer si un tel transfert peut être permis par les règlements et directives adoptées au niveau européen par le Conseil en matière de récolte de données biométriques dans le cadre des demandes de visas, et applicables au cas d'espèce.

(c) Règles européennes en matière de traitement de données biométriques dans le cadre de demandes de visas

c.1 Principes généraux applicables au VIS

18. Dans l'hypothèse où le visa sollicité entre dans le cadre d'un *court séjour ou un transit* par le Belgique, l'enregistrement d'éléments d'identification biométriques est imposé par le système d'information sur les visas (VIS). L'enregistrement de données biométriques dans le VIS est également effectué pour des demandes de visa pour *long séjour*¹⁰.
19. Le système d'information sur les visas (VIS) permet aux pays Schengen d'échanger des données relatives aux visas. Il s'agit d'un système informatique central relié aux systèmes informatiques nationaux tant des autorités compétentes pour l'émission de visas dans les pays Schengen que des consulats dans des pays ne faisant pas partie de l'Union européenne¹¹.

¹⁰ Voir le formulaire de demande de visa long séjour disponible sur le site de l'office des étrangers, lequel indique que les données seront reprises dans le système VIS: https://dofi.ibz.be/sites/dvzoe/FR/Guidedesprocedures/Pages/Formulaire_de_demande_de_visa_long_sejour_pour_la_Belgique.aspx. En effet, pour l'introduction d'une demande de visa long séjour, auprès d'un poste consulaire ou diplomatique belge, le visa apposé dans le document de voyage du candidat au séjour est un visa national de long séjour (visa D). Le visa D a les mêmes effets qu'une carte de séjour en ce qui concerne la libre circulation sur le territoire SCHENGEN. L'étranger est par conséquent autorisé à se rendre dans un autre Etat SCHENGEN que la Belgique pour une durée totale n'excédant pas 3 mois sur une période de 6 mois, à compter de la date de sa première entrée sur le territoire SCHENGEN, à condition toutefois de remplir les conditions d'entrée et de ne pas avoir fait l'objet d'un signalement par l'Etat SCHENGEN (https://dofi.ibz.be/sites/dvzoe/FR/Guidedesprocedures/Pages/Le_travailleur_independant.aspx#les_documents_justificatifs_a_deposer_lo).

¹¹ Pour une description générale du système Schengen, voir la page Internet suivante de la CPVP : <https://www.privacycommission.be/de/node/15719>.

20. Le VIS a été institué par le Règlement CE n° 767/2008 du Parlement européen et du Conseil du 9 juillet 2008 concernant le système d'information sur les visas et l'échange de données entre Etats membres sur les visas de court séjour (ci-après « *Règlement VIS* »). Ce règlement a fait l'objet de précisions dans le Code des visas, où sont fixées les procédures et les conditions de délivrance des visas pour les transits ou les courts séjours (moins de 90 jours) dans l'Espace Schengen.
21. Lorsqu'une demande est jugée recevable, conformément au Code des Visas, l'autorité nationale en charge des visas crée le dossier de demande en saisissant dans le VIS l'ensemble des données imposées par le Règlement VIS, telles que les empreintes digitales (Article 8 du Règlement).

c.2 Règles relatives au traitement d'identifiants biométriques

22. Le Code des visas prévoit que les Etats membres doivent recueillir les *identifiants biométriques* du demandeur, comprenant sa photographie et ses dix empreintes digitales, dans le respect des garanties prévues par la Convention de sauvegarde des droits de l'homme et des libertés fondamentales du Conseil de l'Europe, par la charte des droits fondamentaux de l'Union européenne et par la convention des Nations unies relatives aux droits de l'enfant. Le recueil des identifiants biométriques est effectué par les membres du personnel qualifiés et dûment autorisés des autorités compétentes (Article 13 du Code des Visas).
23. Le Règlement VIS définit l'objet et les fonctionnalités du système d'information sur les visas (VIS) et établit la liste des finalités pour lesquelles le VIS peut être consulté par les Etats membres de l'Union européenne et les pays associés qui appliquent la politique commune des visas. Tout traitement des données VIS doit être proportionné aux objectifs poursuivis et « *nécessaire* » à l'exécution des tâches des autorités compétentes (Considérant 12 du Règlement VIS).
24. Ainsi notamment, les autorités nationales compétentes peuvent consulter le VIS aux fins de l'examen de demandes de visa ou de demandes d'asile (Articles 15 et 22 du Règlement VIS), ou encore à des fins de coopération judiciaire ou policière (Article 3 du Règlement VIS).
25. Les autorités nationales de contrôle, dont fait partie la Commission vie privée, contrôlent la légitimité des traitements de données personnelles du VIS au niveau national, conformément à leur pouvoirs tels que décrits à l'article 28 de la Directive 95/46/CE (article 41 et considérant 19 du Règlement VIS).

c.3 Transfert de données « visa », y compris biométriques, vers des pays tiers

26. Le Règlement VIS ne prévoit *pas de possibilité de transfert de données « visa »* vers des autorités de pays tiers à l'Union Européenne qui n'appliquent pas une politique commune de visas, tel les Etats-Unis. En ce qui concerne spécifiquement les données biométriques du VIS, les autorités européennes de protection des données, rassemblées au sein du Groupe 29 ont estimé que l'accès à de telles données par des autorités non européennes serait problématique, du point de vue des principes relatifs à la finalité du traitement des données, ainsi que du point de vue des restrictions de transfert vers des pays n'offrant pas une protection adéquate en matière de données personnelles au sens de l'article 25 (1) de la Directive 95/46/UE (Opinion du Groupe 29 n° 7/2004 sur l'insertion d'éléments biométriques dans les visas et titres de séjour en tenant compte de la création du système d'information Visa (VIS), 11 août 2004, p. 9¹² ; voir également nos commentaires au point (e) ci-dessous concernant les transferts de données personnelles vers des pays non adéquats).
27. Le transfert de données biométriques VIS vers les Etats-Unis n'est donc en principe pas permis, excepté toutefois dans des *cas exceptionnels, dans le cadre de la coopération policière et judiciaire internationale*.
28. En ce qui concerne les règles applicables à la coopération policière et judiciaire en matière de visas, le Règlement VIS, en effet, détaille les conditions de consultation du VIS par les autorités désignées des Etats membres aux fins de la prévention, de la détection et de l'investigation des infractions terroristes et autres infractions pénales graves telles que visées dans la décision-cadre du Conseil du 13 juin 2002 relative au mandat d'arrêt européen et aux procédures de remise entre Etats membres, ainsi qu'aux fins d'enquête en la matière (Article 3 § 1 et 2 du Règlement VIS *juncto* article 2 § 2 de la Décision-cadre 2002/584/JAI du Conseil relative au mandat d'arrêt européen).
29. Parmi les infractions pénales graves susceptibles de faire l'objet d'un mandat européen et donc, susceptibles de justifier une consultation du VIS par les autorités désignées des Etats membres dans le cadre de la coopération policière et judiciaire internationale, on relève les crimes relevant de la juridiction de la Cour pénale internationale (Article 2 de la Décision 2008/633/JAI).

¹² Opinion du Groupe 29 n° 7/2004 sur l'insertion d'éléments biométriques dans les visas et titres de séjour en tenant compte de la création du système d'information Visa (VIS), 11 août 2004, p. 9 : « *Il semblerait que certains États membres estiment que des autorités de pays tiers devraient pouvoir accéder aux informations de la base de données VIS. Le Groupe estime qu'une telle approche poserait des difficultés majeures au regard des règles de la directive 95/46/CE, notamment quant au principe de finalité et quant aux exigences posées par l'article 25 paragraphe 1 de la directive, relatives à l'existence d'un niveau de protection adéquat dans le pays d'établissement des destinataires des données.* »

30. La prévention et lutte contre de telles infractions graves justifie selon le Conseil une entorse au principe selon lesquelles « *les données à caractère personnel obtenues du VIS* » dans le cadre de la coopération policière et judiciaire « *ne sont pas transférées à des pays tiers ou à des organisations internationales ou mises à leur disposition* » (article 8.4, Décision 2008/633/JAI du Conseil du 23 juin 2008 concernant l'accès en consultation au VIS par les autorités désignées des Etats membres et par l'Office européen de police (Europol) aux fins de la prévention et de la détection des infractions terroristes et autres infractions pénales graves, ainsi qu'aux fins des enquêtes en la matière, ci-après « *Décision 2008/633/ JAI* »¹³).
31. Une exception à l'interdiction de transfert vers des pays tiers est en effet prévue « *en cas d'urgence exceptionnelle* ». Le cas échéant, « *ces données peuvent être transférées à des pays tiers ou à des organisations internationales ou mises à leur disposition exclusivement aux fins de la prévention et de la détection des infractions terroristes et des autres infractions pénales graves* », et ce, sous réserve de plusieurs conditions (Article 8.4 de la Décision 2008/633/ JAI).
32. Trois conditions doivent être respectées en vue d'un tel transfert sous couvert de circonstances exceptionnelles. Premièrement, les organes compétents (Autorités de protection des données locale) doivent contrôler la licéité du traitement. Deuxièmement, l'accord de l'Etat membre qui a introduit les données dans le VIS est requis. Et troisièmement, le transfert doit être conforme au droit national de l'Etat membre qui transfère les données ou les met à disposition. Au sujet de cette troisième condition, il est spécifié que « *le transfert de données par l'Etat membre qui a saisi les données dans le VIS conformément au règlement (CE) n° 767/2008 (Règlement VIS) est soumis au droit national de cet Etat membre* » (Article 8.4 dernier alinéa de la Décision 2008/633/ JAI).
33. Une telle exception pourrait-elle justifier le transfert des données biométriques de quatre burundais vers l'ambassade des Etats-Unis par le SPF Affaires étrangères ? Sous réserve d'informations complémentaires concernant les circonstances du cas d'espèce, la CPVP doit répondre par la négative à cette interrogation car la demande est formulée en dehors d'un cadre de coopération judiciaire ou policière internationale sous couvert d'une urgence. La CPVP est d'avis qu'en dehors d'un tel cadre, le droit belge ne permet pas le transfert de données biométriques issues du système VIS vers des pays tiers, et ce, faute de base légale autorisant le SPF Intérieur (ou son sous-traitant le SPF Affaires étrangères) à traiter les

¹³ La décision (UE) 2015/1956 du Conseil a fixé au 1er septembre 2013 la date d'entrée en vigueur de la décision 2008/633/JAI.

données biométriques recueillies dans le cadre de demandes de visa aux fins de les communiquer à des pays tiers. Ainsi par exemple, une base légale a été jugée nécessaire pour permettre l'échange de données personnelles relatives à des comptes financiers par les institutions financières belges et le SPF Finances, dans le cadre d'un échange automatique de renseignements au niveau international à des fins fiscales (cf. Avis n° 61/2014 du 17 décembre 2014 concernant un projet de loi réglant la communication des renseignements relatifs aux comptes financiers, par les institutions financières belges et le SPF Finances, dans le cadre d'un échange automatique de renseignements au niveau international et à des fins fiscales, points 13 et 14).

34. Surabondamment, l'examen des règles nationales relatives à la collecte de données biométriques dans le cadre de la confection de passeports belges démontre et illustre « *mutatis mutandis* » qu'il n'est pas permis aux autorités chargées du traitement de telles données de les transférer à d'autres autorités en dehors d'une obligation légale spécifique.

C.4 Exemple : les données biométriques des passeports belges

35. La procédure applicable pour le traitement de données biométriques dans le cadre de la délivrance d'un passeport et titre de voyage est décrite dans le Code consulaire et la loi du 10 février 2015 relative aux traitements automatisés de données à caractère personnel nécessaires aux passeports et titres de voyage belges (ci-après « *loi Passeports* »)¹⁴.
36. La loi Passeports impose la reprise d'éléments d'identification biométriques dans le passeport tels qu'une photo numérique et des empreintes digitales (article 4 de la loi Passeports)¹⁵. Le SPF Affaires Etrangères est tenu d'appliquer la loi Passeports (articles 51 et 57 du Code Consulaire) et est par conséquent obligé de collecter et traiter des données biométriques en vue de la production des passeports et des titres de voyage belges (cf. Avis 60/2013 de la CPVP demande d'avis concernant l'avant-projet de loi relative aux traitements automatisés de données à caractère personnel nécessaires aux passeports et titres de voyage belges).
37. La loi Passeports identifie de manière limitative les différents traitements automatisés qui découlent de la mission légale du SPF Affaires étrangères relativement à la délivrance des

¹⁴ Pour une description des types de visa disponibles pour la Belgique (visa national de séjour de plus de 90 jours ; visa pour un séjour de maximum 9 jours, visa de transit), voir le site des Affaires étrangères à la page suivante : http://diplomatie.belgium.be/fr/Services/venir_en_belgique/visa_pour_la_belgique/veelgestelde_vragen/types_de_visa ou le site de l'Office des étrangers à la page suivante : https://dofi.ibz.be/sites/dvzoe/FR/Guidedesprocedures/Pages/Suis_je_soumis_a_lobligation_de_visa.aspx.

¹⁵ La Loi Passeports met en œuvre le Règlement (CE) 2252/2004 du Conseil du 13 décembre 2004 établissant des normes pour les éléments de sécurité et les éléments biométriques intégrés dans les passeports et les documents de voyage délivrés par les Etats membres.

passports et titres de voyage. Pour chaque traitement, en effet, la loi Passeport définit la finalité, énumère les données qui seront traitées, délimite le délai de conservation de ces données et détermine de manière limitative qui y aura accès. Il est notamment spécifié dans l'exposé des motifs de la loi Passports que les données ne sont pas accessibles à d'autres personnes et/ou organisations que celles listées dans la Loi Passeport, à savoir, le personnel du SPF Affaires étrangères affecté dans le service qui met en œuvre le traitement automatisé de ces données, et le personnel chargé des demandes de passports et de titres de voyage énuméré de façon exhaustive à l'article 6 de la loi¹⁶.

38. A cet égard, la CPVP a relevé qu'il n'était pas envisageable d'étendre la communication de données des passports belges à d'autres personnes ou organisations via une autorisation du Comité sectoriel pour l'Autorité Fédérale¹⁷.
39. La communication à d'autres autorités des données biométriques intégrées dans les passports est en outre strictement encadrée par le Code consulaire. Il y est prévu que les modalités selon lesquelles les informations concernant les passports et titres de voyages belges délivrés ainsi que les données biométriques y figurant, sont enregistrées, conservées et peuvent être transmises à d'autres autorités sont « *déterminées par la loi* » (article 56 du Code consulaire).
40. Il ressort des dispositions précitées du Code consulaire et de la loi Passeport que les données biométriques recueillies par le SPF Affaires étrangères dans le cadre de la confection de passports ne peuvent être traitées et communiquées à d'autres autorités belges (ou *a fortiori* étrangères) que sur base d'une législation spécifique, et non sur pied d'autres bases légales offertes par l'article 5 de la LPV telles le consentement ou l'intérêt légitime du responsable du traitement¹⁸. Les données biométriques conservées dans les passport et documents de voyage peuvent bien entendu servir dans le cadre d'enquêtes diligentées par les services de

¹⁶ DOC 54 0731/001, p. 14 ; cette précision a d'ailleurs été ajoutée à la demande de la CPVP (voir également l'avis 60/2013 de la CPVP précité : « *L'utilisation du terme "exclusivement" semble indiquer que l'intention n'est pas de rendre ces données accessibles, via une autorisation du Comité sectoriel pour l'Autorité Fédérale, à d'autres personnes et/ou organisations que celles mentionnées à l'article 6 de l'avant-projet, ce qui, du point de vue de la LVP, ne soulève aucune objection de la part de la Commission. Afin d'exclure toute ambiguïté, il est préférable de clarifier ce point (au moins dans l'Exposé des motifs)* » (p. 6-7).

¹⁷ Ibid.

¹⁸ Le Règlement 2252/2004, dont la loi Passports fait application, ne s'oppose certes pas à ce que les données biométriques soient utilisées pour d'autres finalités que la vérification de l'authenticité du passport ou document de voyage pour autant que ces finalités de traitement soient compatibles avec les droits fondamentaux (Cour de Justice de l'UE, 16 avril 2015, C-446/12 et C-449/12, n°20). Ainsi par exemple, lors des débats parlementaires relatifs à la loi Passports, le ministre a envisagé d'étendre les possibilités de consultation des données des passports et documents de voyage « *dans le cadre de certaines enquêtes criminelles, notamment en cas d'attentat* » (cf. discussion parlementaire relative au projet de Loi Passports, DOC 54, 0731/002). Une telle législation visant à étendre les possibilités de traitement des données de passport et documents de voyage, y compris au travers de collaboration avec des Etats tiers n'est toutefois pas disponible à l'heure de la rédaction/finalisation du présent avis.

police, judiciaires ou de renseignement, conformément au dispositif législatif en vigueur (cf. discussion parlementaire relative au projet de Loi Passeports, DOC 54, 0731/002).

41. La CPVP est d'avis que ces conclusions s'appliquent également en ce qui concerne le transfert de données biométriques collectées dans le cadre de demandes de visa par le SPF Affaires étrangères (agissant alors en tant que sous-traitant du SPF Intérieur, responsable de traitement, comme expliqué ci-dessus).

c.5 Conclusion sur la nécessité d'une base légale

42. Ainsi donc, pour conclure sur ce point relatif à la base légale du traitement envisagé, compte tenu du fait que, selon les dernières informations fournies par le SPF Affaires étrangères, la source des données biométriques concernées est le système d'information « VIS », la CPVP estime que le droit national ne permet pas au SPF Intérieur, responsable de traitement ou au SPF Affaires étrangères, sous-traitant du SPF Intérieur, de transmettre les données à l'ambassade américaine, faute de base légale permettant le traitement de données biométrique dans le système VIS à une telle fin en droit belge, et ce, en dehors d'un cadre de coopération judiciaire ou policière.

(e) Transfert vers un pays « non adéquat »

43. Au-delà de la question de l'absence d'une base légale autorisant le SPF Affaires Etrangères et/ou le SPF Intérieur à traiter les données biométriques recueillies dans le cadre de demandes de visa à des fins de communication à des autorités de pays tiers au système VIS, il faut relever que ces SPF ne peuvent *a fortiori* pas transférer les données biométriques concernées vers un pays tiers « *non adéquat* » tel que les Etats-Unis, qui ne figure pas dans la liste de pays offrant un niveau de protection adéquat en matières de données personnelles, établie par la Commission européenne. Le transfert de données personnelles vers un tel pays à partir d'un Etat membre doit être couvert par une des bases légales spécifiques prévues à l'article 22 de la LVP relatif au transfert de données vers des pays tiers ou par un accord/traité bi- ou multilatéral visant un tel transfert de données et ratifié par le Parlement belge, comme tel est le cas par exemple pour bien nombre d'accords ou traités dans le domaine de la coopération judiciaire et policière en matière pénale.
44. Ainsi par exemple, sous couvert de l'article 22 de la LVP, le transfert vers un pays tiers « *non adéquat* » sera en principe permis s'il est nécessaire ou rendu juridiquement obligatoire par la sauvegarde d'un intérêt public important, tel qu'une obligation légale de transfert, ou un intérêt public important (article 22 § 1 4°). Il importe à cet égard de relever que l'invocation

de la nécessité d'un transfert en raison d'un intérêt public important doit être interprétée de manière restrictive dans le sens où un tel intérêt doit exister, le cas échéant, dans le chef de la Belgique ou de l'Union européenne (Groupe 29, Avis 114, Document de travail relatif à une interprétation commune des dispositions de l'article 26, paragraphe 1, de la Directive 94/46/CE du 24 octobre 1995, 25 novembre 2005 ; Groupe 29, avis 143, n° 10/2007 relatif à la huitième directive sur les contrôle légaux de comptes, 23 novembre 2007 ; CPVP, avis 61/2014 du 17 décembre 2014 sur un projet de loi réglant la communication des renseignements relatifs aux comptes financiers, par les institutions financières belges et le SPF Finances, dans le cadre d'un échange automatique de renseignements au niveau international et à des fins fiscales, p. 8).

45. Certes, la décision PESC 2015/1763 du Conseil du 1^{er} octobre 2015, par laquelle des mesures restrictives ont été promulguées contre les quatre ressortissants burundais concernés, encourage les Etats tiers à « *adopter des mesures restrictives analogues* » et ce, « *afin que les mesures prévues par la présente décision aient le plus grand impact possible* » (article 5 de la décision PESC 2015/1763). Il se peut donc que l'Union Européenne ait intérêt à ce que des pays tiers, adoptent des sanctions analogues, et qu'il soit nécessaire et proportionné qu'un pays tiers tel que les Etats-Unis traite à cet effet les données biométriques des individus frappés par de telles sanctions internationales.
46. Toutefois, même dans l'hypothèse où le SPF Affaires étrangères et/ou le SPF Intérieur pourrait démontrer l'existence dans le chef de la Belgique ou de l'Union européenne d'un intérêt public important à ce que les données biométriques concernées soient transférées vers l'ambassade des Etats-Unis, la CPVP est d'avis qu'un tel transfert ne serait pas permis par la LVP à défaut d'une législation spécifique autorisant le SPF Affaires étrangères/les Etats membres à effectuer le traitement sous-jacent préalable au transfert, à savoir, collecter et traiter les données biométriques des passeports et documents de voyage et/ou du système VIS aux fins de les communiquer à la demande à des pays tiers en dehors d'un cadre de coopération internationale judiciaire ou policière. En outre, si une telle base légale était disponible, le transfert de données envisagé, s'il a lieu par voie électronique, devrait faire l'objet d'une autorisation préalable du Comité sectoriel pour Autorité Fédérale de la Commission Vie Privée, lequel est compétent pour autoriser a priori toute communication électronique de données personnelles par un service public fédéral (article 36 bis de la LVP).

III. CONCLUSION

47. Le SPF Affaires étrangères ne dispose pas de base légale autorisant la communication à l'ambassade des Etats-Unis des données biométriques de quatre ressortissants burundais

visés par les sanctions internationales PESC précitée, aux fins de permettre à cet autorité de restreindre l'accès à ses frontières pour les individus concernés.

48. Premièrement, le SPF Affaires étrangères n'est pas le responsable du traitement de ces données, et doit s'en référer au SPF Intérieur pour toute décision à cet égard.
49. Deuxièmement, la législation applicable ne fournit aucune base légale au SPF Intérieur pour traiter des données biométriques aux fins de les transmettre à des pays tiers, en dehors de la coopération policière et judiciaire internationale. A défaut d'une telle base légale justifiant le traitement de base des données biométriques à de telles fins, il serait non pertinent de justifier le transfert de ces données en invoquant un quelconque intérêt public impérieux dans le chef de la Belgique ou des Etats membres européens à ce que de telles mesures soient prises par les Etats-Unis.

L'Administrateur f.f.,

Le Président,

(sé) An Machtens

(sé) Willem Debeuckelaere