Avis n° 03/2017 du 11 janvier 2017

Objet : Projet de Memorandum of Understanding (mémorandum d'entente) entre les États-Unis d'Amérique et la Belgique afin d'organiser un accès direct aux systèmes nationaux de données relatives aux empreintes digitales, et ce dans le cadre de la prévention du terrorisme et de la lutte contre l'immigration illégale (CO-A-2016-071)

La Commission de la protection de la vie privée (ci-après "la Commission") ;

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 "la LVP"), en particulier l'article 29 ;

Vu la demande d'avis du Ministre de l'Intérieur, reçue le 16/11/2016 ;

Vu le rapport de Monsieur G. Vermeulen ;

Émet, 11 janvier 2017, l'avis suivant :

REMARQUE PRÉALABLE

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 général 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 ou RGPD pour Règlement général sur la protection des données), est entré en vigueur vingt jours après sa publication, soit le 24 mai 2016, et est automatiquement applicable 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 que depuis le 24 mai 2016, pendant le délai d'exécution de deux ans, les États membres ont d'une part une obligation positive de prendre toutes les dispositions d'exécution nécessaires, et d'autre part aussi 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) de l'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.

---

[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) 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.)

I. Objet et contexte de la demande d'avis

1. Le 16 novembre 2016, Monsieur Jan Jambon, Ministre de l'Intérieur (ci-après "le demandeur"), a demandé à la Commission d'émettre un avis sur un projet de *Memorandum of Understanding between the Government of the United States of America and the Governement of Belgium on enhancing cooperation to prevent terrorist travel and to Combat Illegal Immigration* (ci-après "le MOU"). Le demandeur sollicite non seulement un avis sur le MOU et les échanges de données opérationnels qui interviendraient en vertu de cet instrument, mais aussi sur une phase de test préalable qui serait réalisée sur la base de données relatives aux empreintes digitales relevées au cours des trois derniers mois en Belgique.

2. Le MOU a pour but de permettre entre les USA et notre pays un accès réciproque et direct aux systèmes nationaux de données d'empreintes digitales, et ce pour plusieurs finalités, dont l'application de la législation en matière de d'immigration et la lutte contre le terrorisme. La demande d'avis mentionne concrètement un accès à :

a. la banque de données AFIS de la Police fédérale[1] ;
b. la banque de données du Service Printrak[2] ;
c. la banque de données Visanet[3].

3. Le MOU s'inspire manifestement de l'Accord entre le Royaume de Belgique et les États-Unis d'Amérique *sur le renforcement de la coopération dans la prévention et la lutte contre la criminalité grave* (ci-après le Traité "Prüm-like"), au sujet duquel la Commission a rendu son avis n° 27/2010 le 24 novembre 2010 et que le Parlement belge a approuvé par la loi du 8 mai 2014[4]. Sur plusieurs points, le MOU irait toutefois bien plus loin que le Traité "Prüm-like", en particulier

---

[1] La Direction centrale de la police technique et scientifique de la Police fédérale regroupe six services, dont le Service d'identification judiciaire. Ce service gère la banque de données nationale des empreintes digitales judiciaires. Il se charge de la collecte, du traitement et de l'exploitation des fiches dactyloscopiques, via un système automatique d'identification des empreintes digitales (AFIS), et il traite et compare les traces de doigts recueillies sur les lieux des crimes et délits.

(http://www.police.be/fed/fr/a-propos/directions-centrales/direction-centrale-de-la-police-technique-et-scientifique).

[2] Le Service Printrak a été créé en 1993 au sein de l'Office des étrangers et avait pour mission d'éviter les demandes d'asile multiples en prenant les empreintes digitales et en les comparant. Petit à petit, ses tâches ont pris de l'ampleur et il a également commencé à prendre des empreintes digitales pour les services de police, dans le cadre de l'identification. Les centres pour illégaux sont rapidement devenus, eux aussi, une source importante d'empreintes digitales. Eurodac a été lancé en janvier 2003. Cette banque de données européenne d'empreintes digitales de demandeurs d'asile sert de support technique pour exécuter les accords de Dublin. Le Service Printrak est le seul service en Belgique qui a accès à cette banque de données. En 2007, les premières démarches ont été entreprises pour ajouter une banque de données supplémentaire dans le système d'empreintes digitales : la banque de données des « Illégaux ». Celle-ci a été mise en service le 1er janvier 2008.

(https://dofi.ibz.be/sites/dvzoe/FR/Documents/2013_FR.pdf).

[3] Le SPF Intérieur, à savoir l'Office des Étrangers, est l'autorité compétente pour la délivrance d'un visa d'accès à l'Espace Schengen, qu'il s'agisse d'un court séjour, d'un voyage de transit ou d'un long séjour. Cet Office est d'ailleurs mentionné en tant que responsable du traitement sur les demandes de visa disponibles sur son site Internet du "*Type Schengen*" ou pour "*long séjour*" (voir les points 9 à 16 inclus de l'avis n° 32/2016).

[4] Loi du 8 mai 2014 *portant assentiment à l'Accord entre le Royaume de Belgique et les États-Unis d'Amérique sur le renforcement de la coopération dans la prévention et la lutte contre la criminalité grave, établi à Bruxelles le 20 septembre 2011*.

parce que le nouveau règlement aurait des finalités bien plus larges et aussi parce que beaucoup plus de données seraient échangées de manière automatisée.

4. Le MOU est également lié à la discussion qui est menée depuis plusieurs années déjà entre les USA et l'UE au sujet de ce qu'on appelle l' "Umbrella-Agreement" ou "Accord-cadre"[5]. Lorsqu'il entrera en vigueur, cet accord régira la manière dont les autorités policières et judiciaires américaines et européennes devront utiliser les données à caractère personnel en matière pénale lorsqu'elles les échangeront par exemple dans le cadre d'une enquête portant sur le terrorisme ou d'autres délits. Les discussions relatives à cet accord sont entrées dans une phase finale, étant donné que tant le Parlement européen que le Conseil européen ont approuvé le texte négocié, respectivement le 1er décembre 2016 et le 2 décembre 2016. L'Accord-cadre produira ses effets dès que les USA auront également fait savoir qu'ils l'approuvent formellement[6]. Bien que l'accord ne soit donc pas encore juridiquement entré en vigueur, il est fort probable que ce sera le cas dans un tout proche avenir. Dans le présent avis, la Commission confronte d'ores et déjà le MOU à certaines dispositions de l'accord tel qu'approuvé par l'UE[7] (ci-après "l'Accord-cadre")[8].

II. Quant au fond

A. Point de vue de base de la Commission : nécessité d'une base légale solide

a) Introduction

5. La Commission constate que les USA n'apparaissent pas sur la liste dressée par la Commission européenne des pays offrant une protection adéquate des données à caractère personnel. Dans le contexte actuel, on ne peut donc pas appliquer le fondement juridique des transferts de données internationaux prévu à l'article 21 de la LVP. Parmi les autres fondements possibles d'un transfert de données à caractère personnel à des pays tiers, la Commission estime que seul l'article 22, 4° de la LVP ("*le transfert est nécessaire ou rendu juridiquement obligatoire pour la sauvegarde d'un intérêt public important* (...)") doit être analysé plus avant, étant donné que les autres fondements énumérés à l'article 22 de la LVP, ne sont manifestement pas d'application.

---

[5] Accord entre les États-Unis d'Amérique et l'Union européenne sur la protection des informations à caractère personnel traitées à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière.

[6] http://www.consilium.europa.eu/fr/press/press-releases/2016/12/02-umbrella-agreement/.

[7] http://ec.europa.eu/justice/data-protection/files/dp-umbrella-agreement_en.pdf.

[8] La Commission fait également remarquer que tous les traitements de données prévus dans le MOU ne relèvent pas du champ d'application de l'Accord-cadre. Le champ d'application de l'Accord-cadre (Article 3, point 2) ne contient par exemple pas de questions de sécurité nationale, alors qu'elles relèvent bien du champ d'application du MOU (point 3). Étant donné que la grande majorité des traitements envisagés dans le MOU relèvent bel et bien de l'Accord-cadre, la Commission examinera aussi le MOU à la lumière de cet accord.

6. La Commission estime que l'article 22, 4° précité de la LVP – et plus spécifiquement le passage suivant : "*le transfert est* (...) *rendu juridiquement obligatoire pour la sauvegarde d'un intérêt public important* (...)" – doit être lu conjointement avec l'article 22 de la Constitution, qui requiert une base légale formelle pour toute ingérence dans la vie privée. Les traitements de données décrits dans le MOU ainsi que les traitements de données nécessaires pour alimenter les banques de données nationales (cf. supra, point 2) qui seraient consultées dans le cadre du MOU constituent en effet – vu la nature et la quantité de données traitées, le contexte et les finalités avancées – une ingérence importante dans la vie privée. Les traitements envisagés on un impact potentiel sur les personnes concernées, dans ce sens que la consultation et la mise à disposition des données peuvent avoir des conséquences négatives. La Commission estime dès lors que les traitements de données en question doivent être couverts par une base légale spécifique ou par un accord bilatéral ou multilatéral, approuvé par le parlement belge. À défaut d'une telle base légale explicite, la Commission estime qu'il n'est pas non plus pertinent d'analyser plus avant si l'on pourrait appliquer l'autre fondement repris à l'article 22, 4° de la LVP ("*le transfert est nécessaire* (...) *pour la sauvegarde d'un intérêt public important* (...)"),vu qu'à son avis, ce fondement n'est pas suffisant en soi pour pouvoir justifier le transfert massif et automatisé en question de données à caractère personnel sensibles. La Commission considère en effet que ce volet de l'article 22, 4° de la LVP ne peut être invoqué que pour des échanges de données ponctuels[9] [10].

7. À l'avenir, une fois que la nouvelle Directive Police et Justice précitée sera transposée en droit belge, l'importance d'une base juridique solide pour ce type de traitements de données ne fera d'ailleurs qu'augmenter, étant donné que l'article 10 de cette Directive dispose ce qui suit : *"(...) Le traitement (...) des données biométriques aux fins d'identifier une personne physique de manière unique (...) est autorisé uniquement en cas de nécessité absolue, sous réserve de garanties appropriées pour les droits et libertés de la personne concernée, et uniquement : a) lorsqu'ils sont autorisés par le droit de l'Union ou le droit d'un État membre ;* (...)"[11].

---

[9] La Commission se réfère ici aussi au point de vue adopté par le Groupe 29, selon lequel, en résumé :

- les exceptions à la règle générale doivent être interprétées de manière restrictive ;

- il n'est pas souhaitable que des transferts de données à caractère personnel susceptibles d'être qualifiés de volumineux, répétitifs ou structurels reposent sur des dérogations (voir la p. 16 de l'avis n° 4/2009 du Groupe 29).

[10] Voir aussi le point 16 en ce qui concerne les demandes ponctuelles.

[11] Tous les traitements énoncés dans le MOU ne relèveront pas du champ d'application de la nouvelle Directive Police et Justice. Les traitements dans le cadre de la législation en matière d'immigration relèvent par exemple du RGPD (en vertu de l'article 9, point 2 de la Directive Police et Justice), mais dans cet instrument aussi, on a prévu une disposition similaire – à savoir l'article 9 du RGPD – à la Directive Police et Justice.

b) Le MOU comme base légale possible

8. Vu la nature de l'instrument choisi (un memorandum of understanding), la Commission part du principe qu'une fois signé, le MOU ne sera plus soumis à l'approbation du Parlement belge et **conclut dès lors que le MOU ne constitue en soi pas une base légale suffisante permettant de légitimer le transfert automatique de données à caractère personnel qui est envisagé.** Pour étayer ce point de vue, la Commission attire également l'attention sur deux autres éléments :

a. le MOU prévoit en son point 22, b un mécanisme de modification impliquant que les adaptations du MOU pourraient être effectuées de manière très souple, de nouveau sans aucune intervention du Parlement.
b. la manière dont le texte du MOU est rédigé (par exemple, utilisation fréquente des termes "*Participants intend to*" au lieu de par exemple "*Participants shall*") donne fortement l'impression que cet instrument comporte peu d'engagements juridiquement contraignants.

9. Étant donné que le MOU ne suffit pas en soi en tant que base juridique à la lumière des articles 22 de la Constitution et 22, 4° de la LVP, la Commission examine ci-après dans quelle mesure le MOU pourrait être lu conjointement avec d'autres instruments nationaux et/ou internationaux afin que les traitements de données envisagés puissent quand même encore le cas échéant répondre (en partie) aux exigences d'une base légale formelle.

c) Autres instruments internationaux comme base légale possible

10. L'article 1, point 3 de l'Accord-cadre dispose ce qui suit : *"Le présent accord ne saurait, en soi, constituer la base juridique d'éventuels transferts d'informations à caractère personnel. Une base juridique est toujours requise pour de tels transferts."* En d'autres termes : l'Accord-cadre confirme bien qu'une base légale est indispensable, mais il indique aussi qu'il ne peut pas lui-même faire office de base légale. Cet accord ne peut dès lors apporter aucune aide pour compenser l'absence de base juridique formelle.

11. Le Traité "Prüm-like" – qui a été approuvé par le Parlement belge, comme précisé plus haut – comporte bel et bien sur plusieurs points une base juridique claire et solide pour certains traitements de données, mais vu que le MOU va encore beaucoup plus loin que les échanges de données prévus dans le Traité "Prüm-like", ce dernier n'offre évidemment pas de base juridique pour les traitements uniquement prévus dans le MOU et qui ne font pas l'objet du Traité "Prüm-like".

12. Par ailleurs, il existe encore aussi trois Règlements européens qui pourraient éventuellement avoir une influence dans ce contexte[12], mais ces Règlements prévoient une interdiction de principe de transférer à des pays tiers certaines données à caractère personnel qui sont potentiellement visées dans le MOU[13]. Ces instruments européens ne peuvent dès lors pas non plus servir de base légale pour les traitements de données visés dans le MOU.

d) Instruments nationaux comme base légale possible

13. Au niveau national, il convient de tenir compte de plusieurs instruments réglementaires :

a. En ce qui concerne l'accès à la banque de données AFIS :

i. La loi sur la fonction de police prévoit simplement un certain nombre de principes généraux concernant le transfert de données à caractère personnel à des institutions étrangères déterminées :

"Art. 44/11/13. § 1. Les données à caractère personnel et les informations peuvent être communiquées aux services de police étrangers, aux organisations internationales de coopération judiciaire et policière et aux services de répression internationaux dans les conditions prévues par une règle de droit international liant la Belgique ou visées aux articles 21 et 22 de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel. (...)

§ 2. La communication récurrente ou volumineuse de données à caractère personnel ou informations vers un service ou organisation visé au § 1er n'est possible que dans les conditions prévues par une règle de droit international liant la Belgique (...).

§ 4. Un accès direct à tout ou partie des données et informations de la B.N.G. ou une interrogation directe de tout ou partie de ces données et informations n'est octroyé à un service ou organisation visé au § 1er que

---

[12] À savoir dans la mesure où certains traitements décrits dans le MOU pourraient relever (en partie) du champ d'application de ces Règlements respectifs.

[13] 1) Article 39 du 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)*;

2) Article 35 et considérant 41 du Règlement (UE) n° 603/2013 du Parlement européen et du Conseil du 26 juin 2013 *relatif à la création d'Eurodac pour la comparaison des empreintes digitales aux fins de l'application efficace du règlement (UE) n° 604/2013 établissant les critères et mécanismes de détermination de l'État membre responsable de l'examen d'une demande de protection internationale introduite dans l'un des États membres par un ressortissant de pays tiers ou un apatride et relatif aux demandes de comparaison avec les données d'Eurodac présentées par les autorités répressives des États membres et Europol à des fins répressives, et modifiant le règlement (UE) n° 1077/2011 portant création d'une agence européenne pour la gestion opérationnelle des systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice* ;

3) Article 31 du Règlement (CE) n° 767/2008 du Parlement européen et du Conseil du 9 juillet 2008 *concernant le système d'information sur les visas (VIS) et l'échange de données entre les États membres sur les visas de court séjour (règlement VIS)*.

dans les conditions visées par une règle de droit international liant la Belgique.
§ 5. Le présent article s'applique sans préjudice des règles applicables à la coopération judiciaire en matière pénale."

La loi sur la fonction de police ne peut dès lors pas en soi faire office de base légale pour le transfert de données ADN prévu dans le MOU.

ii. Le traitement de données biométriques, comme des empreintes digitales, n'est pas régi explicitement dans la législation relative à la police. Il existe bien une circulaire du Collège des Procureurs généraux (circulaire n° 20/2010) qui aborde ces traitements, mais un tel instrument ne peut évidemment pas être considéré comme une base légale au sens de l'article 22 de la Constitution[14].

iii. Étant donné qu'il est également question dans le MOU du transfert de données ADN (voir point 6, b du MOU), il faut également tenir compte de la loi ADN[15]. L'article 8 de cette loi prévoit effectivement la possibilité d'échanger de telles données avec d'autres pays, mais uniquement dans le cadre d'une enquête en matière pénale et uniquement *"au cas par cas"* [16], autrement dit uniquement pour des demandes d'entraide judiciaire individuelles. La loi ADN ne peut dès lors pas servir de base légale pour le transfert de données ADN prévu dans le MOU.

b. En ce qui concerne l'accès à la banque de données du Service Printrak et à la banque de données Visanet :

i. La loi sur les étrangers[17] dispose explicitement que les données biométriques relevées par exemple lors d'une demande de visa "*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*

[14] La Commission profite également de l'occasion pour souligner le fait que cette circulaire, de manière plus générale et certainement pour l'avenir (cf. mise en œuvre de la Directive Police et Justice), constitue une base juridique insuffisante. Elle plaide à cet égard en faveur d'un cadre légal.

[15] Loi du 22 mars 1999 *relative à la procédure d'identification par analyse ADN en matière pénale*.

[16] Article 8, § 2, premier alinéa de la loi ADN.

[17] Loi du 15 décembre 1980 *sur l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers*.

le Conseil de l'Union européenne." (article 30bis, § 4 van de loi sur les étrangers).

Seules les deux premières finalités citées semblent au premier abord correspondre partiellement aux finalités décrites dans le MOU[18]. Étant donné que la loi sur les étrangers n'indique toutefois nulle part explicitement que les données en question peuvent également être transmises à des pays tiers pour ces finalités, la Commission estime que cette loi ne constitue pas une base légale suffisante pour pouvoir légitimer les transferts prévus dans le MOU.

ii. Il ressort du Code consulaire et de la loi sur les passeports[19] que les données biométriques collectées par le SPF Affaires étrangères dans le cadre de de la confection de passeports peuvent uniquement être traitées et communiquées à d'autres autorités belges (donc *a fortiori* pas à des autorités étrangères) sur la base d'une législation spécifique. Une telle législation visant à étendre les possibilités de traitement des données de passeport et de voyage - incluant la collaboration avec des états tiers - n'est toutefois pas disponible à l'heure de la rédaction/finalisation du présent avis[20].

14. La Commission conclut que les instruments nationaux décrits au point 13 ne peuvent pas non plus faire office de base légale pour les traitements de données visés dans le MOU.

e) Conclusion

15. Vu ce qui précède, la Commission conclut qu'à l'heure actuelle – et pour autant qu'elle ait pu le vérifier – il n'existe pas d'instruments juridiques, ni au niveau national, ni au niveau international (sauf, dans une mesure limitée, dans le Traité "Prüm-like"), qui pourraient compenser l'absence de base légale évoquée au point 8. **Compte tenu du ce contexte et vu l'interaction entre l'article 22, 4° de la LVP et l'article 22 de la Constitution, elle émet un avis défavorable à l'égard de la proposition de baser les transferts de données à caractère personnel en question sur un *"memorandum of understanding"*, étant donné que cet instrument n'offre pas de fondement juridique suffisant.** Ce point de vue vaut tant pour les échanges de données opérationnels visés dans le MOU que pour la phase de

[18] On a déjà démontré au point 12 que dans le contexte du MOU, il ne peut être question de la troisième finalité décrite à l'article 30*bis*, § 4 de la loi sur les étrangers.

[19] Loi du 10 février 2015 *relative aux traitements automatisés de données à caractère personnel nécessaires aux passeports et titres de voyage belges*.

[20] Points 36-42 de l'avis n° 32/2016.

test proposée (dans la mesure où ces tests seraient réalisés avec des données à caractère personnel réelles).

16. Par souci d'exhaustivité, la Commission attire l'attention sur le fait que cette évaluation négative n'implique pas que les données en question ne puissent être transférées aux USA dans aucune mesure ni à aucune condition. À l'heure actuelle, une partie de ces données peut déjà, comme indiqué ci-avant, être échangée dans le cadre du Traité "Prüm-like", et des échanges sont évidemment aussi possibles dans le cadre de demandes d'entraide judiciaire individuelles[21]. À l'avenir, un échange plus poussé, plus systématique ou plus automatisé des données en question peut éventuellement être envisagé pour des finalités bien définies et bien distinctes, basé par exemple sur un accord bilatéral avec les USA, approuvé par le Parlement belge.

B. Remarques quant au contenu du MOU

17. Outre l'objection fondamentale abordée au point A concernant la base légale, la Commission a aussi d'ores et déjà – à titre subsidiaire – plusieurs remarques de fond à formuler concernant le texte du MOU.

18. Premièrement, la Commission estime que le texte du MOU semble perdre de vue un des principes de base du droit de protection des données, à savoir le principe de finalité. Ce principe est non seulement prévu dans la LVP mais il est aussi répété à l'article 6 de l'Accord-cadre. Dans le MOU, il est au moins question de trois finalités différentes, qui se chevauchent complètement, et la possibilité d'utilisation est même laissée ouverte pour n'importe quelle autre finalité[22] :

a. Lutte contre le terrorisme et lutte contre la criminalité en général ;
b. Prévention de menaces pour la sécurité nationale ;
c. Respect de la législation en matière d'immigration et traitement des demandes d'asile ;
d. N'importe quelle finalité, moyennant consentement de l'état qui a fourni les données[23].

La Commission estime que chacune de ces finalités est beaucoup trop vague et rédigée de manière trop générale[24] et que de surcroît, elles se chevauchent et s'entremêlent. Elle en conclut que le texte du MOU est à cet égard contraire à l'article 4, § 1, 2° de la LVP.

---

[21] Voir à cet égard par exemple aussi le point 41 de l'avis n° 32/2016 et les points 23 e.s. de l'avis n° 27/2010.

[22] Voir les points 3 et 4, b, iv du MOU.

[23] Point 12, a, v du MOU.

[24] Voir dans le même sens les points 39-41 de l'avis n° 27/2010.

19. Deuxièmement, la Commission estime que le principe de proportionnalité n'est pas non plus respecté, notamment parce que

a. non seulement les informations "hit/no hit" seraient transmises (complétées éventuellement par plusieurs données de référence), mais que toutes les données à caractère personnel sous-jacentes seraient aussi échangées en même temps ;
b. les données sous-jacentes ne sont pas énumérées de manière limitative dans le MOU, mais qu'au contraire la porte est laissée grand ouverte à l'échange de n'importe quelle donnée (biométrique)[25].

À titre de comparaison et d'illustration, la Commission se réfère au Traité "Prüm-like"[26] et à la loi ADN[27], qui prévoient la possibilité de transmettre les données sous-jacentes au pays demandeur de manière non automatisée et uniquement sous plusieurs conditions strictes[28]. D'après la Commission, un mécanisme de protection similaire fait défaut dans le MOU.

20. Troisièmement, le MOU comporte peu ou pas de règles concernant le délai de conservation des données échangées, alors que cela est cependant obligatoire en vertu de l'article 12, alinéa 2 de l'Accord-cadre. Les seules traces de délais de conservation que l'on retrouve dans le MOU sont les suivantes :

a. Point 12, in fine du MOU : les données échangées qui ne donnent pas lieu à une correspondance doivent être détruites immédiatement, sauf
    i. si des traitements ultérieurs sont nécessaires parce que des doutes subsistent quant à l'exactitude des données échangées ou
    ii. si les deux états se sont mis d'accord pour conserver quand même ces données dans des cas individuels.

   La Commission estime que chaque exception à la règle générale – à savoir la destruction lorsqu'il n'y a pas de correspondance – doit faire l'objet d'une motivation

---

[25] Point 4, b, iv et point 4, c du MOU :

"b. An automated query is intended to include the following without human intervention: (…)

(v) provision of appropriate Personal Data and Encounter Information which may include, subject to availability and practicality, information such as surname, first names, former names, other names, aliases, alternative spelling of names, sex, date and place of birth, photographs, current and former nationalities, passport data, numbers from other identity documents, immigration history and descriptions of past enforcement actions.

c. Where applicable and mutually decided by the Participants, queries, comparisons and further analysis may also be made concerning other biometric data."

[26] Articles 5, 8 et 10 du Traité "Prüm-like".

[27] Article 8 de la loi ADN.

[28] Par exemple demande d'entraide judiciaire individuelle & respect du droit national de l'état qui fournit les données.

scrupuleuse. Surtout pour l'exception citée au point ii, elle ne voit *prima facie* pas de motivation objective.

b. Point 14 du MOU : Les deux états doivent conserver des informations concernant la "*transmission and receipt of data (…) under this MOU*" et concernant "*information on the data supplied, the date of supply, the recipient of the data (…) and any applicable reference data".* Les états ont l'intention de conserver ces informations pendant deux ans "(...) *unless doing so is inconsistent with laws of the Participant* (...)".
La Commission remarque avant tout que cette disposition ne semble concerner que certains traitements de données déterminés, qui concernent la sécurité des flux de données. Cette règle ne semble donc pas s'appliquer à tous les autres traitements qui interviendront dans le cadre du MOU. Ce délai de conservation n'est en outre pas non plus formulé de manière contraignante ("*parties intend to keep (…) such data for two years*"), limitant ainsi sa valeur juridique. La Commission ne peut dès lors que constater que (pour la plupart des traitements de données) aucun délai de conservation explicite contraignant n'est prévu, ce qui, comme exposé plus haut, est contraire à l'Accord-cadre ainsi qu'à l'article 4, § 1, 5° de la LVP.
À titre subsidiaire, la Commission émet également des réserves à l'exception prévue au délai de conservation de 2 ans, où l'on se réfère au droit national. Dans la pratique, une telle exception pourrait en effet vider de son sens le délai de conservation prévu (par exemple dans l'hypothèse où le droit des USA aurait prévu un délai de conservation bien plus long).

21. Quatrièmement, la Commission constate qu'au point 16, a du MOU, plusieurs garanties sont prévues afin que les traitements de données soient effectués de manière transparente et dans le respect des droits des personnes concernées. Au point 16, b du MOU, trois larges motifs d'exception sont prévus simultanément :

"Such information may be denied (…) if providing this information may jeopardize:

(a) The purposes of the processing;

(b) Investigations or prosecutions conducted by the competent authorities; or

(c) The rights and freedoms of third parties."

C'est surtout la première exception que la Commission n'accueille pas favorablement car elle risque de compromettre considérablement les garanties prévues au point 16, a du MOU[29].

[29] En outre, c'est surtout la première exception qui ne paraît pas conforme à l'article 20 (*iuncto* article 16, 2) de l'Accord-cadre.

22. Enfin, la Commission estime aussi de manière générale qu'il est extrêmement important, si l'on envisageait de remplacer le MOU par exemple par un accord bilatéral avec les USA (le cas échéant à faire approuver par le Parlement belge et à faire ratifier ensuite), que le texte de cet accord soit entièrement confronté à l'Accord-cadre tel qu'il entrera définitivement en vigueur[30], étant donné que la majeure partie des traitements de données envisagés dans le MOU relève du champ d'application de cet accord (cf. supra, note de bas de page 8). En ce qui concerne les traitements qui ne relèvent pas au sens strict du champ d'action de l'Accord-cadre (à la condition bien entendu qu'ils soient compatibles en termes de finalité, ce dont la Commission doute d'ores et déjà dès lors qu'il s'agit de traitements relatifs au contrôle et à l'application des règles en matière d'immigration illégale, de traitement de demandes d'asile et de protection de la sécurité nationale), la Commission insiste pour que le cas échéant – via une clause spécifique dans le texte d'un éventuel instrument juridique remplaçant le MOU – toutes les garanties et conditions reprises dans cet accord leur soient quand même déclarées applicables[31].

C. Décision générale

23. La Commission estime que les présents traitements de données ne peuvent se faire sur la simple base d'un memorandum of understanding car un tel instrument ne constitue pas une base légale suffisante au sens de l'article 22 de la Constitution (voir ci-avant au point A).

24. Dans l'hypothèse où le demandeur utiliserait le texte du MOU comme point de départ pour négocier un autre instrument avec les USA, dans le but d'établir une telle base légale pour les traitements de données en question – par exemple sous la forme d'une convention telle que le Traité "Prüm-like" –, la Commission recommande, pour la rédaction du nouveau texte, de déjà tenir compte des remarques formulées au point B. Elle demande alors également – vu la sensibilité des traitements de données en question – à être de nouveau saisie d'une demande d'avis concernant le texte retravaillé.

25. Vu les objections fondamentales énoncées ci-avant, la Commission ne peut pas souscrire à la requête du demandeur de déjà transmettre, dans le cadre d'une sorte de phase de test, toutes les données relatives aux empreintes digitales qui ont été relevées lors des trois derniers mois et qui sont conservées dans les trois banques de données belges concernées (voir le point 1). La Commission estime qu'un tel test ne peut être réalisé que si l'on n'utilise pas de données à caractère personnel réelles.

---

[30] Voir le point 4 ci-dessus.

[31] Une tentative en ce sens est déjà réalisée au point 18, in fine, du MOU, mais la Commission estime que les termes de cette disposition sont encore trop vagues et insiste pour une formulation plus contraignante.

PAR CES MOTIFS,

La Commission estime que :

- dans le contexte actuel, un "memorandum of understanding" ne constitue pas une base juridique suffisante pour pouvoir réaliser les échanges de données avec les USA prévus dans le MOU (voir le point A). Elle émet dès lors un avis défavorable en ce qui concerne l'instrument choisi ;

- des améliorations substantielles du texte du MOU sont également nécessaires pour qu'elle puisse envisager à l'avenir une évaluation favorable du contenu d'une proposition d'instrument juridique éventuellement basée sur le texte du MOU et offrant une base juridique suffisante (comme par exemple un accord bilatéral avec les USA à faire approuver par le Parlement belge et à faire ratifier ensuite) (voir le point B).
  La Commission se réserve le droit le cas échéant d'émettre à un stade ultérieur un avis complémentaire sur une éventuelle proposition retravaillée, comme évoqué ci-avant ;

- le test proposé par le demandeur ne peut entre-temps être réalisé que s'il ne se base pas sur des données à caractère personnel réelles (voir le point 25).

L'Administrateur f.f., Le Président,

(sé) An Machtens (sé) Willem Debeuckelaere