Avis n° 39/2017 du 26 juillet 2017

Objet : avant-projet de loi portant modification de la loi relative aux traitements automatisés de données à caractère personnel nécessaires aux passeports et titres de voyage belges (CO-A-2017-034)

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 Service public fédéral Affaires étrangères, Commerce extérieur et Coopération au Développement (ci-après le « demandeur »), reçue le 30 mai 2017 ;

Vu le rapport de Madame Mireille Salmon ;

Émet, le 26 juillet 2017, l'avis suivant :

Remarque préliminaire

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, aussi appelé RGPD (Règlement Général sur la Protection des Données), 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.

[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:L:2016:119:TOC

I. OBJET ET CONTEXTE DE LA DEMANDE

1. La loi du 10 février 2015 *relative aux traitements automatisés de données à caractère personnel nécessaires aux passeports et titres de voyage belges*[2] (ci-après la « loi du 10 février 2015 ») encadre les différents traitements automatisés qui découlent de la mission légale du Ministre des Affaires étrangères de délivrer les passeports et les titres de voyage belges, en vertu de l'article 51 du code consulaire. La Commission s'était prononcée sur l'avant-projet ayant précédé cette loi dans son avis n° 60/2013 du 27 novembre 2013[3].

2. Le chapitre 6 de cette loi énumère les données traitées en vue de la lutte contre la fraude aux passeports[4]. Il s'agit des données traitées en vue de la production des passeports qui sont transmises et enregistrées dans le cadre du traitement automatisé en vue de la lutte contre la fraude aux passeports et qui vont permettre aux autorités en charge de la délivrance des passeports, du contrôle aux frontières, des enquêtes sur les fraudes à l'identité et du blocage des documents d'identité perdus ou volés d'effectuer les contrôles pertinents et de disposer d'éléments de comparaison.

3. L'avant-projet de loi portant modification de la loi relative aux traitements automatisés de données à caractère personnel nécessaires aux passeports et tires de voyage belges (ci-après l'« avant-projet ») vise à permettre l'enregistrement et la conservation des empreintes digitales du titulaire de passeport pendant 20 ans dans le traitement automatisé en vue de la lutte contre la fraude aux passeports.

II. EXAMEN DE L'AVANT-PROJET

Traitement automatisé des empreintes digitales en vue de la lutte contre la fraude aux passeports (article 2 l'avant-projet / insertion d'un point f) à l'article 21, 1° de la loi du 10 février 2015)

4. L'article 2 de l'avant-projet prévoit d'insérer un point f) dans l'article 21, 1° de la loi du 10 février 2015. Cet article énumère les données relatives au titulaire du passeport issues du traitement automatisé en vue de la production des passeports enregistrées dans le traitement automatisé en vue de la lutte contre la fraude aux passeports.

5. Ces données sont actuellement les suivantes :
   a) le nom de famille, les prénoms, la date et le lieu de naissance, le sexe ;
   b) la signature ;
   c) le numéro du Registre national ;

---

[2] http://www.ejustice.just.fgov.be/eli/loi/2015/02/10/2015015026/justel.

[3] https://www.privacycommission.be/sites/privacycommission/files/documents/avis_60_2013_0.pdf.

[4] Sous l'acception générale « passeport », le présent avis vise également le terme « titre de voyage ».

d) l'image numérisée de la photo faciale du titulaire ;
e) la nationalité (sauf pour les titres de voyage pour étrangers, apatrides et réfugiés).

6. Le demandeur souhaite y ajouter « l'image numérisée des empreintes digitales de l'index de la main droite et de la main gauche du titulaire ou, en cas d'invalidité ou d'inaptitude, d'un autre doigt de chaque main ».

7. Cette donnée est actuellement déjà collectée dans le cadre du traitement automatisé en vue de la production des passeports. Elle est conservée pendant 3 mois et en principe détruite après cette période (articles 4 et 5 de la loi du 10 février 2015). Elle est également stockée sur la puce électronique du passeport et conservée sur la puce tant que le passeport n'a pas été détruit (articles 8 et 9 de la loi du 10 février 2015). Au même titre que l'image numérisée de la photo faciale, les empreintes digitales doivent en effet être intégrées dans les passeports conformément au règlement européen n° 2252/2004 du Conseil du 13 décembre 2004[5].

8. L'article 22 de la loi du 10 février 2015 prévoit que les données enregistrées dans le traitement automatisé en vue de la lutte contre la fraude aux passeports sont conservées pendant 20 ans et ensuite détruites. L'image numérisée des empreintes digitales serait donc conservée pendant 20 ans également.

9. Le demandeur fait valoir dans l'exposé des motifs que la reconnaissance faciale au moyen d'un logiciel pour comparer la photo du demandeur de passeport avec celles de demandes précédentes n'est plus suffisante pour lutter contre la fraude aux passeports.

10. Il évoque plusieurs raisons pour lesquelles une conservation de plus longue durée des empreintes digitales est nécessaire et indiquée en vue de la lutte contre la fraude :
- la marge d'erreurs de la reconnaissance faciale ;
- l'amplification du problème du « photo morphing »[6] : des études indiquent que ces photos manipulées ne sont détectées ni lors d'une inspection visuelle ni en appliquant une reconnaissance faciale automatisée ;

[5] Règlement 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, http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32004R2252.

[6] Des applications commerciales permettent d'assembler les photos de deux personnes différentes dans une seule photo.

- la difficulté de mettre en place à court terme le « live enrollment »[7] par manque d'expertise photographique et en raison du coût matériel, alors que le matériel pour l'enregistrement et la comparaison des empreintes est disponible (ce qui n'empêche pas le demandeur de faire des tests de « live enrollment » dans une commune sensible à la fraude et d'espérer pouvoir intéresser progressivement de plus en plus de communes à la prise de photo « live »).

11. Le demandeur en conclut qu'il est indiqué de combiner la technique de la reconnaissance faciale et la comparaison des empreintes digitales, aussi longtemps que le « live enrollment » ne peut pas être introduit de manière générale. Il explique que la comparaison des empreintes est presque à 100% fiable, à condition que les empreintes digitales de la première demande de passeport soient conservées dans une banque de données afin qu'on puisse vérifier, lors d'une nouvelle demande, s'il s'agit de la même personne. Il précise que la comparaison des empreintes du demandeur avec uniquement les empreintes sur la puce du passeport précédent, peut en effet être facilement contournée, puisque le demandeur peut déclarer son passeport volé ou perdu ou rendre délibérément la puce du passeport illisible.

12. Dans son avis n° 60/2013, la Commission avait adhéré aux arguments du demandeur concernant la possibilité de disposer des photos des 2 derniers passeports. Elle reconnaissait également que l'utilisation d'un logiciel de reconnaissance faciale permet d'obtenir une analyse plus fiable qu'une comparaison de visu et de détecter d'éventuelle tentatives d'obtenir un passeport authentique sous une fausse d'identité.

13. La Commission prend note des justifications apportées par le demandeur à l'appui de la transmission des empreintes digitales au traitement automatisé en vue de la lutte contre la fraude aux passeports et de leur conservation prolongée. Elle regrette que le « live enrollment » ne puisse pas être généralisé à court terme.

14. La Commission note cependant que la conservation de longue durée des empreintes digitales n'apportera pas la garantie de l'absence de fraude si les empreintes digitales viennent à l'appui d'une usurpation d'identité au moyen d'une photo « morphée » lors de la délivrance d'un premier passeport. Au contraire, le mécanisme de contrôle des empreintes digitales lors d'une demande de renouvellement donnera beaucoup de fiabilité à cette fraude.

[7] Prise de la photo d'identité en direct.

15. Elle fait également remarquer que le Groupe de l'article 29 regroupant les autorités de protection des données européennes émet des réserves à l'égard d'une base de données nationale des passeports reprenant des éléments biométriques[8]. Il estime en effet que la création d'une base de données centralisée contenant les données personnelles et en particulier les données biométriques de tous les citoyens risquerait de violer le principe de proportionnalité. Toute base de données centralisée accroîtrait les risques d'utilisation abusive et d'appropriation frauduleuse. Elle accroîtrait également le risque d'abus et de dérapages. Enfin, elle augmenterait le risque d'utilisation des éléments d'identification biométrique comme « clés d'accès » à diverses bases de données, et partant d'interconnexion de différents fichiers.

16. La Commission rappelle que les données à caractère personnel doivent être adéquates, pertinentes et non excessives au regard des finalités poursuivies et conservées pendant une durée n'excédant pas celle nécessaire à la réalisation de ces finalités, conformément à l'article 4, § 1er, 3° et 5° de la LVP. La Commission note que la conservation à long terme des empreintes digitales va concerner un pourcentage important de la population étant donné que chaque année une centaine de milliers de passeports sont émis et que les empreintes seront conservées pendant 20 ans. La Commission y voit la création indirecte d'une banque de données des empreintes digitales (d'un pourcentage élevé) de la population belge sans commune mesure avec le nombre de fraudeurs.

17. La Commission fait également valoir le principe de minimisation des données figurant à l'article 5, c) du RGPD selon lequel les données doivent être non seulement adéquates et pertinentes mais également limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées.

18. La Commission note ensuite que la fraude aux passeports n'est pas un problème nouveau et l'urgence de la problématique par rapport à il y a deux ans lorsque la loi du 10 février 2015 a été adoptée n'est pas démontrée, d'autant que le procédé et l'accessibilité du « photo morphing » ne semblent pas dater d'hier.

19. Elle rappelle enfin que les empreintes digitales sont déjà conservées sur la puce électronique du passeport afin d'identifier les titulaires des passeports belges, et utilisées notamment par les personnes en charge de la délivrance des passeports.

[8] Avis 3/2005 sur l'application du règlement (CE) n° 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 États membres, adopté le 30 septembre 2005, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2005/wp112_fr.pdf.

20. Afin de lutter efficacement contre la fraude, la Commission préconise la généralisation du « live enrollment » qui permet au demandeur de ne pas devoir traiter plus de données que nécessaires et de ne pas traiter des données présentant un caractère particulièrement sensible. A cet égard, elle invite le demandeur à continuer activement ses démarches pour introduire le « live enrollment » de manière généralisée, de telle manière que la reconnaissance faciale constitue un outil efficace et suffisant pour la lutte contre la fraude aux passeports.

21. Dans l'attente de la mise en place généralisée du « live enrollment », la Commission peut admettre que les empreintes digitales soient traitées de manière additionnelle aux images numérisées des photos faciales, afin de lutter contre la fraude aux passeports, et qu'elles soient conservées plus de 3 mois. Au vu des arguments développés supra, elle considère néanmoins que les empreintes digitales du titulaire de passeport peuvent être uniquement conservées pour une durée n'excédant pas la période de validité du passeport qui est en principe de 7 ans[9]. A l'issue de cette période, elles devront être détruites et seules d'éventuelles nouvelles empreintes dans le cadre d'un renouvellement ou d'une nouvelle demande de passeport pourront être conservées.

22. A cet égard, et étant donné que le demandeur souhaite principalement lutter contre le phénomène de fraude lié au « photo morphing » en conservant les empreintes digitales, la Commission prie le demandeur de fournir dans l'exposé des motifs des chiffres ou à tout le moins des exemples de cas concrets d'utilisation du « photo morphing » dans le cadre de la délivrance des passeports belges. La Commission estime en effet que des éléments objectivables doivent soutenir la pertinence de conserver pendant la durée de validité du passeport les empreintes digitales dans une banque de données centrale et ce, pour l'ensemble des détenteurs de passeports belges.

23. Elle précise également que les empreintes digitales ne pourront être conservées pendant la durée de validité du passeport que pour la seule finalité invoquée, de la lutte contre la fraude aux passeports[10] et ne pourront donc pas être utilisées à d'autres fins non légalement prévues.

[9] Arrêté royal du 19 avril 2014 *relatif à la durée de validité des passeports*.

[10] En dehors de la conservation dans le cadre du traitement automatisé qui est encadré dans l'article 15 et sur une base volontaire.

24. La Commission fait aussi remarquer que, suivant le RGPD les empreintes digitales sont des données biométriques[11] dont le traitement est interdit sauf s' il est nécessaire pour des motifs d'intérêt public importants, sur la base du droit de l'Union ou du droit d'un État membre et que dans ce cas, il doit être proportionné à l'objectif poursuivi, respecter l'essence du droit à la protection des données et prévoir des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée[12].

25. Elle prie dès lors le demandeur de prévoir notamment des mesures techniques et organisationnelles appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée.

26. La Commission fait par ailleurs remarquer que l'utilisation des empreintes digitales dans le traitement automatisé en vue de la lutte contre la fraude implique une modification de l'article 5, alinéa 2 de la loi du 10 février 2015 selon lequel les empreintes digitales sont en principe détruites après 3 mois suivant leur collecte dans le cadre du traitement automatisé en vue de la production des passeports.

Reformulation de la disposition concernant l'accès des autorités répressives (article 3 de l'avant-projet/ modification de l'article 23, § 1er, 6° de la loi du 10 février 2015)

27. L'article 3 de l'avant-projet reformule l'article 23, § 1er, 6° de la loi du 10 février 2015 en ce qui concerne l'accès des autorités répressives et de renseignement aux données traitées en vue de la lutte contre la fraude aux passeports, et notamment aux données relatives au titulaire du passeport incluant l'image numérisée de la photo faciale de ce dernier. L'article 23, § 1er, 6° prévoit actuellement l'accès du « personnel dûment habilité ou les magistrats auprès des services de police, des services judiciaires ou des services de renseignements, et ce uniquement aux fins de rechercher ou d'établir une fraude relative à l'identité d'une personne ». La modification permettra l'accès par « les services de police et les services de renseignement dans le cadre d'une recherche ou d'une enquête relative à la fraude à l'identité ». D'après l'exposé des motifs, « l'article 23, § 1er a été modifié en vue de redéfinir la liste du personnel et des services qui ont accès aux données, suite à la conservation des empreintes digitales ».

[11] De même que les images faciales, article 4, 14) du RGPD.

[12] Article 9, § 2, g) du RGPD.

28. Concernant la justification de cette redéfinition en ce qui concerne les autorités répressives et de renseignement, le demandeur explique que l'ancienne disposition n'était pas claire et contenait des erreurs et que le but est de rendre le texte plus clair, correct et cohérent. Il n'y a pas de magistrats auprès des services de police ou des services de renseignements. Le demandeur a donc décidé d'enlever les magistrats de cette catégorie, puisqu'ils peuvent toujours avoir accès aux données dans le cadre d'une enquête judiciaire moyennant une apostille d'un juge d'instruction ou d'un magistrat du parquet. Ils n'ont donc pas besoin d'une disposition légale séparée pour assurer cet accès. Le demandeur a également reformulé le but puisqu'il existe deux types d'enquêtes possibles : la recherche et l'enquête.

29. La Commission prend acte des explications du demandeur et l'invite à les faire figurer dans l'exposé des motifs pour plus de clarté.

Accès aux empreintes digitales dans le cadre du traitement automatisé en vue de la lutte contre la fraude aux passeports (article 4 de l'avant-projet / modification de l'article 23, § 2, alinéa 2 de la loi du 10 février 2015)

30. Actuellement, les autorités en charge respectivement du contrôle aux frontières, des enquêtes sur les fraudes à l'identité et du blocage des documents d'identité perdus ou volés ont notamment accès aux données relatives au titulaire du passeport, en ce compris l'image numérisée de la photo faciale de ce dernier.

31. L'avant-projet prévoit que seul le personnel en charge de la délivrance des passeports aura accès aux empreintes digitales conservées, via un système automatisé intégré dans le logiciel pour la délivrance des passeports, en vue de détecter une fraude à l'identité à l'aide des empreintes digitales.

32. L'exposé des motifs mentionne à cet égard que les autres autorités n'ont pas besoin d'avoir un accès direct aux empreintes digitales, n'étant pas en charge de délivrance des passeports. Il précise que les services de police qui pourraient être chargés de recherche ou d'enquêtes sur la fraude à l'identité, pourront toujours dans ces cas obtenir accès aux empreintes digitales moyennant une apostille d'un magistrat, garantissant un contrôle judiciaire pour l'accès à ces données.

33. La Commission prend acte de la limitation de l'accès aux services en charge de la délivrance des passeports et estime également que l'accès des autres autorités ne serait pas pertinent. Ainsi notamment le personnel chargé du contrôle aux frontières a accès aux empreintes digitales stockées sur la puce, afin d'identifier les titulaires des passeports belges.

PAR CES MOTIFS,

La Commission émet un avis défavorable sur l'avant-projet vu ses remarques formulées aux points 14 à 25 et invite par ailleurs le demandeur à tenir compte de ses remarques reprises aux points 26 et 29.

L'Administrateur f.f., Le Président,

(sé) An Machtens (sé)Willem Debeuckelaere