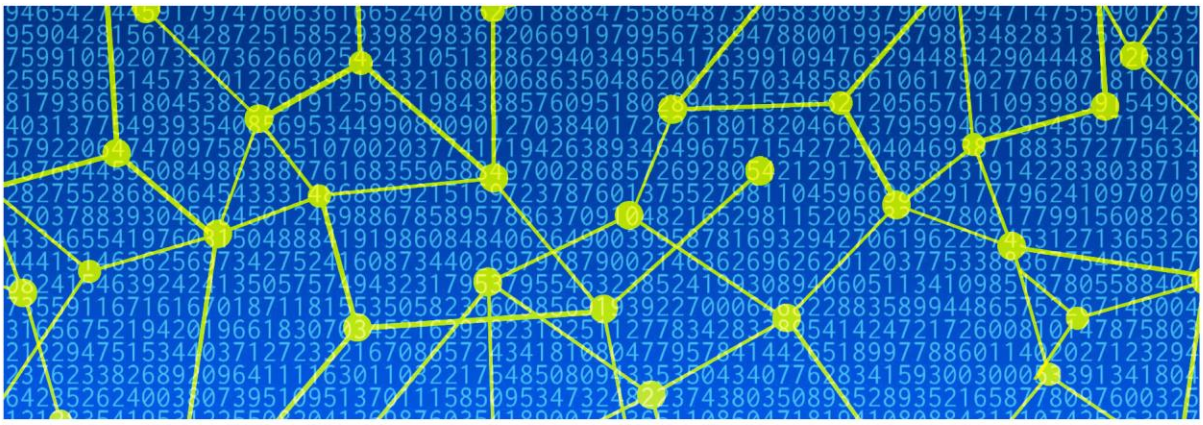

EUROPEAN DATA PROTECTION SUPERVISOR

Avis 7/2018 du CEPD

sur la proposition de règlement relatif au renforcement de la sécurité des cartes d'identité des citoyens de l'Union et d'autres documents

EDPS

10 août 2018

Le contrôleur européen de la protection des données («CEPD») est une institution indépendante de l'Union chargée, en vertu de l'article 41, paragraphe 2, du règlement nº 45/2001, «[...] en ce qui concerne le traitement de données à caractère personnel, [...] de veiller à ce que les libertés et droits fondamentaux des personnes physiques, notamment leur vie privée, soient respectés par les institutions et organes communautaires», et «[...] de conseiller les institutions et organes communautaires et les personnes concernées pour toutes les questions concernant le traitement des données à caractère personnel». Conformément à l'article 28, paragraphe 2, du règlement nº 45/2001, la Commission a l'obligation, «lorsqu'elle adopte une proposition de législation relative à la protection des droits et libertés des personnes à l'égard du traitement de données à caractère personnel [...]», de consulter le CEPD.

Le CEPD et le contrôleur adjoint ont été nommés en décembre 2014 avec comme mission spécifique d'adopter une approche constructive et proactive. Le CEPD a publié en mars 2015 une stratégie quinquennale exposant la manière dont il entend mettre en œuvre ce mandat et en rendre compte.

Le présent avis découle de la mission de conseil du CEPD auprès des institutions européennes sur les implications de leurs politiques en matière de protection des données, et de promotion d'une élaboration responsable des politiques, conformément à l'action nº 9 de la stratégie du CEPD: «Faciliter l'élaboration responsable et éclairée de politiques». Si le CEPD soutient les objectifs visant à renforcer la sécurité des cartes d'identité et des titres de séjour, qui contribue à une Union globalement plus sûre, il estime que la proposition devrait être améliorée sur certains aspects essentiels afin de garantir le respect des principes de protection des données.

Résumé

Le présent avis expose la position du CEPD concernant la proposition de règlement du Parlement européen et du Conseil relatif au renforcement de la sécurité des cartes d'identité des citoyens de l'Union et des titres de séjour délivrés aux citoyens de l'Union et aux membres de leur famille exerçant leur droit à la libre circulation.

Dans ce cadre, le CEPD constate que la Commission a clairement choisi d'accorder la priorité aux aspects de la proposition portant sur la libre circulation et de traiter l'objectif de sécurité correspondant en corollaire. Le CEPD fait remarquer que cela pourrait d'avoir une incidence sur l'analyse de la nécessité et de la proportionnalité des éléments de la proposition.

Le CEPD soutient l'objectif de la Commission européenne de renforcer les normes de sécurité applicables aux cartes d'identité et aux titres de séjour, contribuant ainsi à la sécurité de l'Union dans son ensemble. Dans le même temps, le CEPD estime que la proposition ne justifie pas suffisamment la nécessité de traiter deux types de données biométriques (image faciale et empreintes digitales) dans ce cadre, alors que l'objectif déclaré pourrait être atteint par une approche moins intrusive.

En vertu du cadre juridique de l'Union, ainsi que de la convention 108 modernisée, les données biométriques sont considérées comme des données sensibles et font l'objet d'une protection spéciale. Le CEPD souligne que les images faciales et les empreintes digitales qui seraient traitées en application de la proposition relèvent clairement de cette catégorie de données sensibles.

En outre, le CEPD estime que la proposition aurait une incidence considérable qui toucherait jusqu'à 370 millions de citoyens de l'Union, soumettant potentiellement 85 % de la population de l'Union au relevé obligatoire d'empreintes digitales. Cette large portée, conjuguée au caractère très sensible des données traitées (images faciales combinées aux empreintes digitales), appelle un examen attentif selon un critère de nécessité strict.

Par ailleurs, le CEPD reconnaît que, compte tenu des différences entre les cartes d'identité et les passeports, l'introduction dans les cartes d'identité d'éléments de sécurité pouvant être considérés comme appropriés dans le cas des passeports ne peut être automatique, mais exige une réflexion et une analyse approfondie.

De plus, le CEPD tient à souligner que l'article 35, paragraphe 10, du règlement général sur la protection des données (ci-après le «*RGPD*»)[1] s'appliquerait au traitement dont il est ici question. À cet égard, le CEPD fait observer que l'analyse d'impact accompagnant la proposition ne semble pas soutenir l'option stratégique retenue par la Commission, à savoir l'intégration obligatoire d'images faciales et de deux empreintes digitales dans les cartes d'identité (et les titres de séjour). Il s'ensuit que l'analyse d'impact accompagnant la proposition ne peut être considérée comme suffisante aux fins de la conformité avec l'article 35, paragraphe 10, du RGPD. Par conséquent, le CEPD recommande de réévaluer la nécessité et la proportionnalité du traitement des données biométriques (image faciale combinée aux empreintes digitales) dans ce cadre.

En outre, la proposition devrait explicitement prévoir des garanties contre l'établissement de bases de données dactyloscopiques nationales par les États membres dans le cadre de la mise en œuvre de la proposition. Une disposition devrait être ajoutée à la proposition précisant de façon explicite que les données biométriques traitées dans son contexte doivent être effacées immédiatement après leur intégration dans la puce et ne peuvent être traitées ultérieurement à d'autres fins que celles expressément établies dans la proposition.

Le CEPD convient que l'utilisation des données biométriques peut être considérée comme une mesure antifraude légitime; cependant, la proposition ne justifie pas la nécessité de stocker deux types de données biométriques aux fins considérées. L'une des solutions envisageables serait de restreindre les données biométriques utilisées à une seule (par exemple, image faciale uniquement).

En outre, le CEPD tient à souligner qu'il comprend que le stockage d'images d'empreintes digitales renforce l'interopérabilité mais, dans le même temps, celui-ci accroît la quantité de données biométriques traitées et les risques d'usurpation d'identité en cas de violation des données à caractère personnel. Le CEPD recommande par conséquent de limiter les données dactyloscopiques stockées dans la puce des documents à des points caractéristiques ou des motifs, un sous-ensemble des caractéristiques extraites de l'image de l'empreinte digitale.

Enfin, en raison de la large portée et de l'incidence considérable éventuelle de la proposition précédemment soulignées, le CEPD recommande de fixer l'âge minimum pour le relevé d'empreintes digitales des enfants au titre de la proposition à 14 ans, conformément à d'autres instruments du droit de l'Union.

TABLE DES MATIÈRES

LE CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES,

vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 16,

vu la Charte des droits fondamentaux de l'Union européenne, et notamment ses articles 7 et 8,

vu le 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)[2],

vu le règlement (CE) nº 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données[3], et notamment son article 28, paragraphe 2, son article 41, paragraphe 2, et son article 46, point d),

vu la 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[4],

A ADOPTÉ L'AVIS SUIVANT:

1. INTRODUCTION ET CONTEXTE

1. Le 17 avril 2018, la Commission européenne (ci-après *«la Commission»*) a présenté la proposition de règlement du Parlement européen et du Conseil relatif au renforcement de la sécurité des cartes d'identité des citoyens de l'Union et des titres de séjour délivrés aux citoyens de l'Union et aux membres de leur famille exerçant leur droit à la libre circulation[5], qui vise à améliorer les éléments de sécurité des cartes d'identité des citoyens de l'Union et des cartes de séjour des membres de leur famille qui n'ont pas la nationalité d'un État membre (ci-après *«la proposition»*).

2. Ladite proposition fait partie du plan d'action de décembre 2016 *«visant à renforcer la réponse européennes aux fraudes liées aux documents de voyage»* (ci-après *«le plan d'action de décembre 2016»*[6], dans lequel la Commission définissait des mesures destinées à renforcer la sécurité des documents, notamment des cartes d'identité et des titres de séjour, dans le contexte des attentats terroristes qui avaient récemment frappé l'Europe.

3. Les cartes d'identité jouent un rôle important dans la sécurisation de l'identification des personnes à des fins administratives et commerciales, ce que la Commission a souligné dans sa communication *«Accroître la sécurité dans un monde de mobilité: améliorer l'échange d'informations dans la lutte contre le terrorisme et renforcer les frontières extérieures»*[7] adoptée le 14 septembre 2016. La nécessité d'améliorer la sécurité de ces documents a également été mise en avant dans le rapport sur la citoyenneté de l'Union 2017.

4. L'une des missions du CEPD consiste à conseiller les services de la Commission lors de la rédaction de nouvelles propositions législatives ayant des conséquences en matière de protection des données.

5. Le CEPD se réjouit d'avoir déjà été consulté par la Commission européenne, de manière informelle, au sujet du projet de proposition et d'avoir eu l'occasion d'apporter sa contribution concernant les aspects relatifs à la protection des données.

2. OBJECTIFS ET CONTEXTE DE LA PROPOSITION

6. Le CEPD relève que la proposition met un accent particulier **sur la sécurité et la lutte contre le terrorisme et la criminalité organisée**. L'exposé des motifs commence par indiquer que *«[p]our lutter contre le terrorisme et la criminalité organisée [...] il est essentiel de garantir la sécurité des documents d'identité et de voyage»*. Il souligne plus loin que *«[l]e renforcement de la sécurité des documents est un élément important pour améliorer la sécurité à l'intérieur de l'UE et à ses frontières et pour soutenir l'évolution vers une Union de la sécurité réelle et effective»*[8]. L'objectif principal de la proposition est de *«renforce[r] les normes de sécurité applicables aux cartes d'identité délivrées par les États membres à leurs ressortissants et aux titres de séjour délivrés par les États membres aux citoyens de l'Union et aux membres de leur famille lorsqu'ils exercent leur droit à la libre circulation»*[9].

7. L'analyse d'impact accompagnant la proposition mentionne également d'autres objectifs de la proposition, qui sont notamment de *«réduire la fraude documentaire, améliorer l'acceptation et l'authentification des cartes d'identité et des titres de séjour et améliorer l'identification des personnes à partir de ces documents»;* mais aussi de *«faire mieux connaître aux citoyens, aux autorités nationales et au secteur privé les documents délivrés et le droit à la liberté de circulation qui y est attaché»;* enfin de *«simplifier la vie quotidienne des citoyens de l'UE, réduire la paperasserie et diminuer les coûts à la fois pour les citoyens et les entités privées et publiques, en réduisant les barrières administratives [...] liées à l'utilisation des cartes d'identité et des titres de séjour»*[10].

8. Le CEPD relève que la base juridique de la proposition est l'article 21, paragraphe 2, du TFUE. Cet article dispose que *«[s]i une action de l'Union apparaît nécessaire pour atteindre cet objectif [la libre circulation des personnes], le Parlement européen et le Conseil, statuant conformément à la procédure législative ordinaire, peuvent arrêter des dispositions visant à faciliter l'exercice des droits»* à la libre circulation. **Le CEPD constate que la Commission a clairement choisi d'accorder la priorité aux aspects de la proposition portant sur la libre circulation et de traiter l'objectif de sécurité correspondant en corollaire. Le CEPD remarque que cela pourrait avoir une incidence sur l'analyse de la nécessité et de la proportionnalité des éléments de la proposition** (voir ci-après).

9. À l'heure actuelle, la directive (UE) 2004/38 relative aux droits des citoyens[11] **ne réglemente pas le format et les normes minimales applicables aux cartes d'identité ni ne prévoit de normes spécifiques** en ce qui concerne les **titres de séjour** délivrés aux citoyens de l'Union et aux membres de leur famille qui n'ont pas la nationalité d'un État membre. Par conséquent, la directive (UE) 2004/38 **n'exige pas** que les cartes d'identité,

les documents de séjour délivrés aux citoyens de l'Union ou les cartes de séjour délivrées aux membres de la famille de citoyens de l'Union qui n'ont pas la nationalité d'un État membre, **intègrent des données biométriques** telles qu'une image faciale du titulaire de la carte et/ou ses empreintes digitales dans des formats interopérables.

10. La proposition vise à renforcer la sécurité des cartes d'identité des citoyens de l'Union et des cartes de séjour des membres de leur famille qui n'ont pas la nationalité d'un État membre en établissant **l'intégration obligatoire de données biométriques (deux empreintes digitales et une image faciale) dans les cartes d'identité** délivrées par les États membres à leurs citoyens ainsi que **dans les cartes de séjour des membres de leur famille** qui n'ont pas la nationalité d'un État membre. À cet égard, la proposition prévoit que les cartes d'identité délivrées par les États membres sont de format ID-1 et sont conformes aux normes minimales de sécurité définies dans le document 9303 de l'OACI (septième édition, 2015). Conformément au document 9303 de l'OACI (septième édition, 2015) (ci-après *«le document de l'OACI»*), les données biométriques seront stockées en vue de leur utilisation avec des systèmes de reconnaissance faciale, d'empreintes digitales ou de l'iris[12].

11. En ce qui concerne les **cartes de séjour des membres de la famille** qui n'ont pas la nationalité d'un État membre, l'article 7, paragraphe 1, de la proposition dispose que: *«[l]orsqu'ils délivrent des cartes de séjour aux membres de la famille d'un citoyen de l'Union qui n'ont pas la nationalité d'un État membre, les États membres utilisent le même modèle que celui établi par les dispositions du règlement (CE) nº 1030/2002 du Conseil établissant un modèle uniforme de titre de séjour pour les ressortissants de pays tiers»*. Actuellement, l'article 5 du règlement (UE) nº 1030/2002[13], qui établit un modèle uniforme de titre de séjour pour les ressortissants de pays tiers, prévoit que le règlement (UE) nº 1030/2002 ne s'applique pas, entre autres, aux *«ressortissants des pays tiers qui sont membres de la famille de citoyens de l'Union européenne exerçant leur droit à la libre circulation [...]»* Par conséquent, à l'heure actuelle, l'article 4 *bis* du règlement (UE) nº 1030/2002, qui impose d'inclure dans le titre de séjour des ressortissants de pays tiers une image faciale et deux empreintes digitales comme éléments d'identification biométriques, ne s'applique pas aux ressortissants de pays tiers qui sont membres de la famille de citoyens de l'Union.

12. **Le CEPD soutient l'objectif de la Commission européenne de renforcer les normes de sécurité applicables aux cartes d'identité et aux titres de séjour, contribuant ainsi à la sécurité de l'Union dans son ensemble.** Dans le même temps, comme exposé ci-après, **le CEPD estime que la proposition ne justifie pas suffisamment la nécessité dans ce cadre de traiter deux types de données biométriques (image faciale et empreintes digitales), alors que l'objectif déclaré pourrait être atteint par une approche moins intrusive.**

3. PROPORTIONNALITÉ ET NÉCESSITÉ DU TRAITEMENT DES DONNÉES BIOMÉTRIQUES

3.1. Caractère sensible des données biométriques

13. Le CEPD souhaite insister sur le fait que **le traitement des données biométriques constitue une limitation des droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel** et, comme toute atteinte à un droit fondamental, **doit satisfaire aux critères énoncés à l'article 52, paragraphe 1, de la Charte des droits fondamentaux de l'Union européenne (ci-après *«la Charte»*)**[14]. Toute limitation doit, en plus d'être prévue par la loi, respecter le contenu essentiel du droit en cause et, dans le respect du principe de proportionnalité, être nécessaire et répondre effectivement à des objectifs reconnus par l'Union ou au besoin de protection des droits et libertés d'autrui.

14. Les empreintes digitales constituent des données à caractère personnel car elles contiennent objectivement des informations uniques sur les individus qui permettent leur identification précise[15]. Dans l'ordre juridique de l'Union, **les données biométriques sont définies comme des données à caractère personnel** résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, qui **permettent ou confirment son identification unique, telles que des images faciales ou des données dactyloscopiques**[16]. **En vertu du cadre juridique de l'Union[17], ainsi que de la convention 108[18] modernisée, les données biométriques sont considérées comme constituant l'une des catégories particulières de données à caractère personnel[19] et sont soumises à une protection spéciale**: leur traitement est en principe interdit et il existe un nombre limité de conditions dans lesquelles un tel traitement est licite. Ceci s'applique en particulier aux données biométriques traitées aux fins de l'identification des personnes. **Le CEPD souligne que les images faciales et les empreintes digitales qui seraient traitées en application de la proposition relèvent clairement de cette catégorie de données sensibles.**

15. En conséquence, le CEPD insiste sur la nécessité de veiller à ce que le traitement des données biométriques en application de la proposition demeure **limité à ce qui est strictement nécessaire pour atteindre les objectifs fixés.** De surcroît, compte tenu du caractère particulièrement sensible des données biométriques, il sera nécessaire de prévoir des **garanties appropriées** (voir ci-après).

3.2. Étendue du champ d'application et incidence de la proposition

16. Le CEPD tient à rappeler, comme cela est exposé dans son guide sur la nécessité[20], que **la nécessité constitue un principe essentiel dans l'évaluation de la limitation des droits fondamentaux**, tels que le droit à la protection des données à caractère personnel. Selon la jurisprudence, en raison du rôle joué par le traitement des données à caractère personnel pour un ensemble de droits fondamentaux, la limitation du droit fondamental à la protection des données à caractère personnel doit être strictement nécessaire. **La nécessité doit être justifiée sur le fondement d'éléments objectifs et constitue l'étape préalable**

à l'évaluation de la proportionnalité de la limitation. Le critère de nécessité est également essentiel lors de l'appréciation de la licéité du traitement des données à caractère personnel. Les opérations de traitement, les catégories de données traitées et la durée de conservation des données doivent être nécessaires aux fins du traitement.

17. La proposition n'impose pas aux États membres d'introduire des cartes d'identité ou des titres de séjour lorsque ces documents ne sont pas prévus par le droit national, pas plus qu'elle n'affecte la compétence des États membres en matière de délivrance d'autres titres de séjour prévus par le droit national mais en dehors du champ d'application du droit de l'Union[21]. Par conséquent, **les nouvelles règles prévues par la proposition affecteront les États membres qui délivrent déjà des cartes d'identité ou des titres de séjour**, qu'ils soient obligatoires ou non.

18. À cet égard, il convient de souligner que le Danemark et le Royaume-Uni n'émettent pas de cartes d'identité. Sur les 26 États membres délivrant des cartes d'identité, seuls 15 en imposent la possession[22]. Et dans 13 États membres les cartes d'identité délivrées n'incluent actuellement pas de données biométriques[23]. Ainsi, **jusqu'à 370 millions de citoyens dans 26 États membres seraient affectés par la proposition, ce qui correspond à près de 85 % des 440 millions de citoyens de l'Union**[24]. Ces 370 millions de citoyens correspondent au «*nombre total de titulaires potentiels de cartes d'identité dans 26 États membres*»[25], parmi lesquels 175 millions seraient soumis à l'obligation nouvelle de fournir leurs empreintes digitales pour établir leur carte d'identité[26] (16 États membres). Les 195 millions de citoyens européens restants, qui sont déjà soumis à l'obligation de posséder une carte d'identité conformément à la législation nationale existante, seraient également affectés par les nouvelles exigences – une fois introduite au niveau de l'Union, l'obligation d'inclure les empreintes digitales dans les cartes d'identité ne pourrait être supprimée par les États membres au moyen de seules mesures nationales[27].

19. Par conséquent, **le CEPD estime que la proposition aurait une incidence considérable, touchant jusqu'à 370 millions de citoyens de l'Union et soumettant potentiellement 85 % de la population de l'Union au relevé obligatoire d'empreintes digitales. Cette large portée, conjuguée au caractère très sensible des données traitées (images faciales combinées à des empreintes digitales), appelle un examen attentif selon un critère de nécessité strict.**

3.3. Justification de la proposition: cartes d'identité nationales contre passeports et conséquences sur la libre circulation

20. Le CEPD relève dans la proposition plusieurs tentatives de présentation des cartes d'identité nationales délivrées par les États membres de l'Union à leurs citoyens comme **juridiquement et fonctionnellement équivalentes aux passeports**. L'exposé des motifs de la proposition dispose[28] que l'ajout des deux identifiants biométriques *«alignera le niveau de sécurité des documents d'identité des citoyens de l'Union et des cartes de séjour délivrées aux ressortissants de pays tiers, membres de la famille d'un citoyen de l'Union, sur les normes respectivement applicables aux passeports délivrés aux citoyens de l'Union et aux titres de séjour délivrés aux ressortissants de pays tiers qui ne sont pas membres de la famille d'un citoyen de l'Union.»*

21. La proposition fait référence aux cartes d'identité et aux passeports de manière presque interchangeable en ce qui a trait à l'exercice du droit à la libre circulation des citoyens de l'Union (et des membres de leur famille) et introduit des exigences équivalentes à celles applicables aux passeports. Conformément au règlement (CE) nº 2252/2004 du Conseil, **les passeports et les documents de voyage** délivrés par les États membres doivent actuellement **comporter un support de stockage hautement sécurisé contenant une image faciale et deux empreintes digitales**, relevées à plat, en formats interopérables. La proposition introduit ainsi l'obligation d'intégrer une image faciale et deux empreintes digitales comme éléments d'identification biométriques dans les cartes de séjour qui sont délivrées par les États membres à des membres de la famille de citoyens de l'Union.

22. À cet égard, **le CEPD soutient l'objectif de la Commission visant à faciliter la libre circulation**. **Néanmoins, le CEPD fait observer que les deux types de documents – cartes d'identité et passeports – sont en fait très différents, tant du point de vue juridique qu'au niveau de leur utilisation pratique.** Même lorsqu'elles sont utilisées en tant que documents de voyage dans le cadre de la libre circulation, les cartes d'identité nationales, contrairement aux passeports, ne peuvent l'être que pour se rendre dans des États membres de l'Union et les pays tiers concernés, ce qui permet aux citoyens de l'Union de voyager grâce à leurs cartes d'identité nationales. Dans ce contexte, le CEPD met en doute la valeur ajoutée de l'intégration des données biométriques dans les cartes d'identité, étant donné qu'elles ne sont pas systématiquement contrôlées lors des voyages entre États membres de l'Union.

23. Plus important encore, **les cartes d'identité font l'objet de diverses utilisations qui vont bien au-delà de l'exercice du droit à la libre circulation** lié à la citoyenneté de l'Union, depuis les démarches auprès des administrations du pays d'origine du citoyen jusqu'aux relations avec différents acteurs du secteur privé (banques, compagnies aériennes, etc.). En outre, selon l'analyse d'impact accompagnant la proposition, environ 15 millions de citoyens de l'Union résident dans un autre État membre, et 11 millions travaillent dans un autre État membre[29]. Le CEPD en conclut que, pour la grande majorité des citoyens de l'Union, les fonctions principales d'une carte d'identité ne sont pas directement associées à la libre circulation. On ne peut présumer que tous les citoyens de l'Union potentiellement concernés par l'obligation d'inclure leurs empreintes digitales dans leur carte d'identité nationale, introduite par la proposition, exercent effectivement leurs droits en matière de libre circulation, loin de là. Les citoyens mobiles de l'Union constituent au contraire une petite minorité de ceux qui sont potentiellement concernés par la proposition. En outre, même ceux qui exercent concrètement leur droit à la libre circulation peuvent le faire, et le font souvent, sur la base d'un passeport, et non d'une carte d'identité. **La justification de la proposition** avancée par la Commission **n'est donc pas totalement convaincante**.

24. La proposition fait également référence à la nécessité de lutter contre la fraude documentaire, en particulier la falsification de documents ou la description fallacieuse d'un fait matériel concernant le droit de séjour. Il est difficile de discerner dans quelle mesure le renforcement des éléments de sécurité, y compris biométriques, pourrait contribuer à résoudre les problèmes de *«description fallacieuse»*. Quoi qu'il en soit, comme mentionné dans l'analyse d'impact accompagnant la proposition, **au cours de la**

période 2013-2017, l'Agence européenne de garde-frontières et de garde-côtes (Frontex) a compilé des statistiques sur les cartes d'identité et les titres de séjour frauduleux et **n'a relevé que 38 870 cartes d'identité frauduleuses**[30].

25. De surcroît, comme indiqué à l'annexe 6 de l'analyse d'impact, le nombre de personnes en provenance de pays tiers utilisant des cartes d'identité et des titres de séjour frauduleux **a diminué de 11 % en 2015 (8 373)**[31]. Cette tendance est également confirmée par l'analyse des risques pour 2017 de Frontex[32], qui montre une **nouvelle diminution à 7 044 en 2016** du nombre de personnes utilisant des documents frauduleux. La tendance concernant spécifiquement les **cartes d'identité** est similaire à celle des documents frauduleux dans leur ensemble, avec une **diminution des détections en 2016**[33].

26. Selon le CEPD, **ce nombre relativement faible**[34] de cartes d'identité et de titres de séjour frauduleux et le fait que **le nombre de personnes** en provenance de pays tiers utilisant des cartes d'identité et des titres de séjour frauduleux **diminue progressivement**, ne justifient pas en soi les solutions de grande ampleur mises en avant dans la proposition.

27. Par conséquent, **le CEPD estime que, compte tenu des différences entre les cartes d'identité et les passeports, l'introduction dans les cartes d'identité d'éléments de sécurité pouvant être considérés comme appropriés dans le cas des passeports ne peut être automatique, mais exige une réflexion et une analyse approfondie.**

3.4. Nécessité d'une analyse d'impact relative à la protection des données

28. Le CEPD relève également que, conformément à l'article 35, paragraphe 1, du règlement général sur la protection des données (ci-après «*RGPD*»)[35], une analyse d'impact relative à la protection des données (ci-après l'«*AIPD*») doit être effectuée avant qu'une activité de traitement «*susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques*» soit mise en place. Le CEPD estime que cette exigence est pleinement applicable dans le contexte de la proposition. L'**AIPD devrait porter sur l'ensemble des opérations de traitement envisagées pour les deux catégories de données biométriques couvertes, à savoir les images faciales et les empreintes digitales.** En particulier, elle devrait comprendre une évaluation des risques au regard des droits et libertés des personnes concernées, ainsi que les mesures envisagées pour faire face à ces risques, telles que des garanties et mesures de sécurité.

29. Le CEPD tient à souligner à cet égard que **l'article 35, paragraphe 10, du RGPD serait applicable au traitement considéré** (qui aurait une base juridique dans le droit de l'Union, à savoir la proposition). Par conséquent, **à moins que l'AIPD ne soit menée dans le cadre de l'adoption de la proposition, les États membres seront tenus de l'exécuter ultérieurement**. À cet égard, **le CEPD fait remarquer que l'analyse d'impact accompagnant la proposition ne semble pas soutenir l'option stratégique retenue par la Commission**, à savoir l'intégration obligatoire d'images faciales et de deux empreintes digitales dans les cartes d'identité (et les titres de séjour).

30. En effet, dans le cadre de l'examen des différentes options stratégiques, l'analyse d'impact indique ce qui suit: ***«Pour les options ID 2) et ID 3), les citoyens seront tenus de fournir***

leurs empreintes digitales lors de la demande de cartes d'identité. *Cette obligation empiète sur les droits fondamentaux au respect de la vie privée et à la protection des données. Si, dans l'affaire Schwarz*[36]*, la Cour de justice de l'Union européenne a jugé que l'ingérence en ce qui concerne les passeports est proportionnée à l'objectif de préservation de la sécurité,* ***dans le cas des cartes d'identité, le seuil de satisfaction au critère de nécessité se situe sans doute à un niveau supérieur, les cartes d'identité étant obligatoires dans certains États membres qui n'imposent actuellement pas le relevé d'empreintes digitales****»*[37].

31. Après la comparaison des options stratégiques, l'analyse d'impact indique que l'option ID 1) est la plus appropriée pour promouvoir les objectifs de renforcement de la sécurité aux frontières et au sein des États membres, ainsi que la liberté de circulation. Il est à noter que l'option ID 1) privilégiée par le rapport d'analyse d'impact intégrerait une «***puce RFID obligatoire contenant des données biométriques (image faciale obligatoire, empreintes digitales facultatives)***»[38]. Autrement dit, l'option stratégique soutenue par l'analyse d'impact accompagnant la proposition inclurait les empreintes digitales **de manière optionnelle, et non comme une condition obligatoire.**

32. Étonnamment, la Commission a décidé, malgré les résultats de l'analyse d'impact accompagnant la proposition, d'introduire dans la proposition l'intégration obligatoire des empreintes digitales dans les cartes d'identité. Dans l'exposé des motifs de la proposition, il est souligné que: ***«Le relevé obligatoire des empreintes digitales a été ajouté à l'option privilégiée pour les cartes d'identité afin de renforcer l'efficacité en termes de sécurité.*** *L'ajout de deux identificateurs biométriques (image faciale, empreintes digitales) améliorera l'identification des personnes et alignera le niveau de sécurité des documents d'identité des citoyens de l'Union et des cartes de séjour délivrées aux ressortissants de pays tiers, membres de la famille d'un citoyen de l'Union, sur les normes respectivement applicables aux passeports délivrés aux citoyens de l'Union et aux titres de séjour délivrés aux ressortissants de pays tiers qui ne sont pas membres de la famille d'un citoyen de l'Union.»*[39]

33. **Il s'ensuit que l'analyse d'impact accompagnant la proposition ne peut être considérée comme suffisante aux fins de la conformité avec l'article 35, paragraphe 10, du RGPD.** Par conséquent, **le CEPD recommande de réévaluer la nécessité et la proportionnalité du traitement des données biométriques (image faciale combinée aux empreintes digitales) dans ce cadre.**

4. TRAITEMENT DES DONNÉES BIOMÉTRIQUES: GARANTIES NÉCESSAIRES

34. L'article 3, paragraphe 3, de la proposition imposerait d'intégrer dans les cartes d'identité délivrées dans l'Union **un support de stockage hautement sécurisé qui contient une image faciale du titulaire de la carte et deux empreintes digitales dans des formats interopérables.**

4.1. Spécification de la finalité

35. Le principe de limitation de la finalité[40] exige que les données à caractère personnel soient recueillies pour des finalités déterminées, explicites et légitimes, et qu'elles ne puissent être traitées ultérieurement de manière incompatible avec ces finalités. À cet égard, **le CEPD note avec satisfaction que l'article 10 de la proposition énumère de manière exhaustive les finalités du traitement des données à caractère personnel**.

36. En outre, en vertu de l'article 10, paragraphe 3, de la proposition, le traitement des données biométriques intégrées dans les cartes d'identité et les titres de séjour est autorisé à deux fins:

> *«pour vérifier:*
> *a) l'authenticité de la carte d'identité ou du titre de séjour;*
> *b) l'identité du titulaire grâce à des éléments comparables directement disponibles lorsque la loi exige la présentation de la carte d'identité ou du titre de séjour.»*

37. À titre liminaire, le CEPD fait remarquer que **la correspondance entre les données biométriques stockées dans la puce du document** et **les données biométriques fournies par le titulaire du document** prouve uniquement **que le document appartient au titulaire du document**. Cette concordance ne constitue pas en soi une preuve d'identité, à moins que l'authenticité du document ait également été prouvée.

38. L'authenticité du document pourrait être démontrée par **la correspondance entre les données biométriques stockées dans la puce** et **une copie des données biométriques collectées lors de l'enrôlement.** Cependant, il convient d'éviter la création de bases de données dactyloscopiques nationales, qui de toute façon n'est pas envisagée dans la proposition. La seule option consisterait donc à vérifier la concordance entre les données stockées dans la puce et les données imprimées sur le document. L'intégrité des données stockées dans la puce repose sur le certificat numérique également stocké dans la puce. Les certificats numériques ont une date d'expiration et peuvent être révoqués par l'autorité de délivrance. Par conséquent, tout système de vérification nécessiterait une connexion internet, ou une autre méthode, pour mettre à jour sa liste de révocation des certificats.

39. Il faut reconnaître que l'utilisation de données biométriques réduit le risque de falsification avec succès d'un document, de sorte qu'elle peut être considérée comme une mesure justifiée de lutte contre la fraude. Cependant, la mise en œuvre pratique d'une procédure d'authentification fondée sur les données biométriques stockées dans les cartes d'identité constitue un projet à long terme complexe. Quoi qu'il en soit, il n'est pas fait mention d'un tel projet dans la proposition et, en son absence, le stockage de données biométriques ne permet pas d'atteindre la finalité visée.

40. En outre, le plan d'action de décembre 2016 indique que «***[p]our contrôler les composants électroniques des passeports et titres de séjour électroniques, les autorités concernées ont besoin que les certificats requis leur soient fournis par l'État membre qui a délivré le document***»[41] de façon à ce qu'elles puissent accéder aux empreintes digitales stockées dans la puce. Le contrôle électronique systématique des données de la puce permettrait de

détecter les cas les plus courants de fraude documentaire, comme les manipulations de la photo du titulaire. **Malheureusement, tous les États membres n'échangent pas leurs certificats.** Le plan d'action de décembre 2016 comporte une action prévoyant que la Commission «*pourvoit à la mise en place au cours du troisième trimestre de 2017 d'une liste régulièrement mise à jour des certificats nécessaires à l'authentification électronique des documents de voyage*»[42]. Cependant, l'analyse d'impact accompagnant la proposition indique que «*les clés d'accès aux données changent au fil du temps et ne sont pas toujours immédiatement communiquées aux autorités nationales compétentes*»[43].

41. **Le CEPD constate également qu'il est explicitement reconnu dans l'analyse d'impact accompagnant la proposition qu'il est difficile de justifier la nécessité et la proportionnalité des limitations du droit fondamental à la protection des données à caractère personnel envisagées dans la proposition**, en particulier pour ce qui a trait à l'intégration d'empreintes digitales dans les cartes d'identité délivrées par les États membres à leurs ressortissants. Elle souligne qu'en ce qui concerne l'intégration des empreintes digitales, il convient de tenir compte de la jurisprudence de la Cour de justice. À cet égard, dans l'*affaire Schwarz*[44], la Cour a conclu que, bien que le prélèvement d'empreintes digitales et leur conservation dans les passeports constituent une atteinte aux droits au respect de la vie privée et à la protection des données à caractère personnel, l'ajout d'empreintes digitales dans les passeports est licite compte tenu de l'objectif d'intérêt général visant à empêcher «*l'entrée illégale de personnes sur le territoire de l'Union*»[45]. Toutefois, l'analyse d'impact admet que ***«compte tenu du fait que les cartes d'identité servent à d'autres fins que le franchissement des frontières et que les utilisations traditionnelles des cartes d'identité diffèrent d'un État membre à un autre, il ne va pas de soi que la même conclusion puisse s'imposer»***[46].

42. En outre, le CEPD insiste sur le fait que le traitement des données à caractère personnel doit être limité à la finalité légitime pour lesquelles lesdites données ont été collectées initialement auprès de la personne concernée. En particulier, la proposition **devrait explicitement prévoir des garanties contre l'établissement de bases de données dactyloscopiques nationales par les États membres** dans le cadre de la mise en œuvre de la proposition. Une disposition devrait être ajoutée à la proposition précisant de façon explicite que **les données biométriques traitées dans son contexte doivent être effacées immédiatement après leur intégration dans la puce** et ne peuvent être traitées ultérieurement à d'autres fins que celles expressément établies dans la proposition.

4.2. Minimisation des données

43. Le CEPD tient à souligner que l'**un des principes clés de la législation de l'Union en matière de protection des données est la minimisation des données**. En vertu de ce principe, les données à caractère personnel doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées[47].

44. Si les techniques de biométrie présentent des avantages inhérents par rapport aux techniques traditionnelles d'identification des personnes, la garantie de la sécurité et de l'intégrité des données biométriques constitue un problème crucial. Ainsi, dans l'hypothèse où les données biométriques d'une personne (par exemple, l'image de ses

empreintes digitales) seraient volées (par accès ou copie illégale par exemple), il ne serait pas possible de les remplacer, contrairement à une carte de crédit, une carte d'identité papier ou un mot de passe perdus ou volés. Un système de vérification fondé sur la biométrie ne fonctionne correctement que si le système informatique vérificateur est à même de garantir que les données biométriques recueillies au moment de l'enrôlement provenaient de la personne légitime.

45. Dans ce contexte, les technologies de reconnaissance d'empreintes digitales peuvent être divisées en trois classes[48]:
    - celles qui stockent et comparent des **images** d'empreintes digitales
    - celles qui stockent et comparent des **points caractéristiques**, un sous-ensemble de caractéristiques extrait des images d'empreintes digitales
    - celles qui stockent et comparent des **motifs** extraits des images d'empreintes digitales

46. Le document de l'OACI[49] exige que les images des empreintes digitales soient stockées afin d'assurer l'interopérabilité entre les différents types de technologies de reconnaissance d'empreintes digitales. Des normes permettent de rendre les systèmes de reconnaissance d'empreintes digitales de différents éditeurs interopérables au sein de leur classe, mais les systèmes de reconnaissance d'empreintes digitales ne sont pas interopérables entre classes.

47. Le stockage d'images d'empreintes digitales permet le calcul de sous-ensembles de leurs caractéristiques, alors que l'inverse n'est pas possible. Le fait de disposer de l'image des empreintes digitales stockées dans la puce électronique permet aux États membres d'utiliser les données biométriques quel que soit le type de technologie de reconnaissance d'empreintes digitales choisi. Cependant, si les données stockées sur la puce sont des points caractéristiques, un État membre qui aura déployé une technologie de reconnaissance d'images d'empreintes digitales ne pourra pas utiliser ces données car il est impossible d'obtenir une image d'empreinte digitale à partir de points caractéristiques. En outre, dans l'hypothèse d'une faille de sécurité, l'image des empreintes digitales stockée sur un document d'identité perdu ou volé pourrait être récupérée et utilisée de manière criminelle pour émettre un faux jeu d'empreintes digitales permettant d'usurper l'identité du titulaire de la carte.

48. **Le CEPD convient que le stockage d'images d'empreintes digitales renforce l'interopérabilité** mais, dans le même temps, **celui-ci accroît la quantité de données biométriques traitées et le risque d'usurpation d'identité en cas de violation des données à caractère personnel**. Par conséquent, **le CEPD recommande de limiter les données dactyloscopiques stockées dans la puce des documents à des points caractéristiques ou des motifs, un sous-ensemble de caractéristiques extrait de l'image de l'empreinte digitale.**

49. **En outre, le CEPD estime que le traitement de deux types de données biométriques distincts (image faciale obligatoire, empreintes digitales obligatoires) prévu dans la proposition n'est pas justifié, compte tenu des objectifs indiqués.** Les finalités visées à

l'article 10, paragraphe 3, de la proposition peuvent être atteintes en utilisant seulement un type de données biométriques. La proposition ne précise pas si les deux types de données biométriques devraient être vérifiés pour s'assurer de l'identité du détenteur ou non.

50. Le double contrôle des données biométriques comporte ses propres risques, associés au taux de faux négatifs (résultat d'une défaillance dans un processus de vérification qui aurait dû se conclure avec succès) de la technologie en question (empreinte digitale ou image faciale). Le contrôle des empreintes digitales et des images faciales pourrait donner lieu à des situations dans lesquelles la vérification de l'image faciale serait concluante mais pas celle des empreintes digitales ou inversement. Même si le pourcentage de faux négatifs d'une technologie déterminée de reconnaissance biométrique est faible, cela pourrait affecter un nombre significatif d'individus lorsqu'il est appliqué à une très grande population, comme c'est le cas en l'espèce. Enfin, il se peut que les deux types de données biométriques ne soient pas utilisés. Dans ce cas, seul celui qui sera utilisé devrait être stocké.

51. L'article 3, paragraphe 1, de la proposition indique les normes minimales de sécurité définies dans le document de l'OACI. Les mesures de sécurité exigées, recommandées et facultatives sont détaillées dans la partie 11 (Mécanismes de sécurité) du document de l'OACI. Au point 3.1, il est indiqué que l'*authentification passive* est la seule mesure requise concernant la puce. Selon le document de l'OACI, cette mesure n'empêche pas la copie exacte ni la substitution du circuit intégré (CI), ni l'écrémage[50]. Au point 3.1, il est indiqué que le *contrôle d'accès de base* est la seule mesure requise concernant le système de vérification. Selon le document de l'OACI, cette mesure n'empêche pas la copie exacte ni la substitution du CI, bien qu'elle exige aussi de copier le document conventionnel et qu'elle ajoute une certaine complexité. Le CEPD estime que, si des données biométriques de 85 % de la population de l'Union doivent être stockées sur les cartes d'identité, la proposition devrait relever les exigences minimales afin d'éviter ces risques.

52. En vertu de la présente proposition, toute personne ayant accès à une carte d'identité et à un lecteur répondant aux normes définies dans le document de l'OACI pourrait accéder aux données biométriques d'une personne par un simple accès au document, même si les données biométriques ne sont pas utilisées pour vérifier l'identité du titulaire par le tiers.

53. Par conséquent, l'intégration obligatoire d'empreintes digitales dans les cartes d'identité des citoyens de l'Union prévue dans **la proposition n'est pas conforme au principe de minimisation des données**, selon lequel un responsable du traitement des données devrait limiter le traitement des données à caractère personnel à ce qui est pertinent et nécessaire à une finalité spécifique.

54. Cependant, **le CEPD souhaite souligner que les techniques d'impression sécurisée**, telles que les hologrammes ou les filigranes, **n'impliquent pas le traitement de données à caractère personnel mais permettraient d'empêcher la falsification et de vérifier l'authenticité d'une carte d'identité ou d'un titre de séjour.**

4.3 Exemptions au relevé d'empreintes digitales

55. L'article 3, paragraphe 5, point a), de la proposition prévoit que les enfants de moins de 12 ans et les personnes qui sont physiquement incapables de donner leurs empreintes digitales sont exemptés de l'obligation de donner leurs empreintes digitales. **Le CEPD accueille avec satisfaction l'introduction d'exemptions fondées sur l'âge de la personne ou sa capacité à donner des empreintes digitales.** Ces exemptions font partie des procédures de secours qui devraient être mises en œuvre.

56. Dans le même temps, le CEPD attire l'attention sur la nécessité de tenir compte de l'**intérêt de l'enfant** dans toutes les mesures prises par les pouvoirs publics et les acteurs du secteur privé concernant les enfants, conformément à l'article 24 de la Charte. De même, le considérant 38 du RGPD énonce que «*[l]es enfants méritent une protection spécifique en ce qui concerne leurs données à caractère personnel parce qu'ils peuvent être moins conscients des risques, des conséquences et des garanties concernées et de leurs droits liés au traitement des données à caractère personnel*».

57. Dans ce cadre, le CEPD souhaite souligner qu'en ce qui concerne les populations de grande taille, la limite d'âge pour la collecte des empreintes digitales des enfants est actuellement fixée à 14 ans[51]. En raison de **la large portée et de l'incidence considérable éventuelle de la proposition** soulignées ci-dessus, le CEPD recommande de **fixer l'âge minimum pour le relevé des empreintes digitales des enfants au titre de la proposition à 14 ans, conformément à d'autres instruments du droit de l'Union.**

58. Nous notons en outre que la proposition vise également à **étendre les exigences relatives au relevé des empreintes digitales des enfants à ceux qui sont titulaires de titres de séjour** en raison du fait qu'ils sont membres de la famille de citoyens de l'Union et n'ont pas la nationalité d'un État membre. Conformément aux remarques précédentes, **le CEPD recommande de fixer l'âge minimum dans la proposition à 14 ans.**

7. CONCLUSIONS

Le CEPD constate que la Commission a clairement choisi d'accorder la priorité aux aspects de la proposition portant sur la libre circulation et de traiter l'objectif de sécurité correspondant en corollaire. Le CEPD fait remarquer que cela pourrait avoir une incidence sur l'analyse de la nécessité et de la proportionnalité des éléments de la proposition.

Le CEPD soutient l'objectif de la Commission européenne de renforcer les normes de sécurité applicables aux cartes d'identité et aux titres de séjour, contribuant ainsi à la sécurité de l'Union dans son ensemble. Dans le même temps, le CEPD estime que la proposition ne justifie pas suffisamment la nécessité de traiter deux types de données biométriques (image faciale et empreintes digitales) dans ce cadre, alors que l'objectif déclaré pourrait être atteint par une approche moins intrusive.

En vertu du cadre juridique de l'Union, ainsi que de la convention 108 modernisée, les données biométriques sont considérées comme des données sensibles et font l'objet d'une protection spéciale. Le CEPD souligne que les images faciales et les empreintes digitales qui seraient traitées en application de la proposition relèvent clairement de cette catégorie de données sensibles.

En outre, le CEPD estime que la proposition aurait une incidence considérable qui toucherait jusqu'à 370 millions de citoyens de l'Union, soumettant potentiellement 85 % de la population de l'Union au relevé obligatoire d'empreintes digitales. Cette large portée, conjuguée au caractère très sensible des données traitées (images faciales combinées à des empreintes digitales), appelle un examen attentif selon un critère de nécessité strict.

Par ailleurs, le CEPD reconnaît que, compte tenu des différences entre les cartes d'identité et les passeports, l'introduction dans les cartes d'identité d'éléments de sécurité pouvant être considérés comme appropriés dans le cas des passeports ne peut être automatique, mais exige une réflexion et une analyse approfondie.

De surcroît, le CEPD tient à souligner que l'article 35, paragraphe 10, du RGPD s'appliquerait au traitement considéré. À cet égard, le CEPD fait observer que l'analyse d'impact accompagnant la proposition ne semble pas soutenir l'option stratégique retenue par la Commission, à savoir l'intégration obligatoire d'images faciales et de deux empreintes digitales dans les cartes d'identité (et les titres de séjour). Il s'ensuit que l'analyse d'impact accompagnant la proposition ne peut être considérée comme suffisante aux fins de la conformité avec l'article 35, paragraphe 10, du RGPD. Par conséquent, le CEPD recommande de réévaluer la nécessité et la proportionnalité du traitement des données biométriques (image faciale combinée aux empreintes digitales) dans ce cadre.

En outre, la proposition devrait explicitement prévoir des garanties contre l'établissement de bases de données dactyloscopiques nationales par les États membres dans le cadre de la mise en œuvre de la proposition. Une disposition devrait être ajoutée à la proposition précisant de façon explicite que les données biométriques traitées dans son contexte doivent être effacées immédiatement après leur intégration dans la puce et ne peuvent être traitées ultérieurement à d'autres fins que celles expressément établies dans la proposition.

Le CEPD comprend que l'utilisation de données biométriques puisse être considérée comme une mesure antifraude légitime; cependant, la proposition ne justifie pas la nécessité de stocker deux types de données biométriques aux fins considérées. L'une des solutions envisageables serait de restreindre les données biométriques utilisées à une seule (par exemple, image faciale).

En outre, le CEPD tient à souligner qu'il comprend que le stockage d'images d'empreintes digitales renforce l'interopérabilité mais, dans le même temps, celui-ci accroît la quantité de données biométriques traitées et les risques d'usurpation d'identité en cas de violation des données à caractère personnel. Le CEPD recommande donc de limiter les données dactyloscopiques stockées dans la puce des documents à des points

caractéristiques ou des motifs, un sous-ensemble des caractéristiques extraites de l'image de l'empreinte digitale.

Enfin, en raison de la large portée et de l'incidence considérable éventuelle de la proposition soulignées ci-dessus, le CEPD recommande de fixer l'âge minimum pour le relevé d'empreintes digitales des enfants au titre de la proposition à 14 ans, conformément à d'autres instruments du droit de l'Union.

Bruxelles,

Giovanni BUTTARELLI

Notes

[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), JO L 119 du 4.5.2016, p. 1.
[2] JO L 119 du 4.5.2016, p. 1.
[3] JO L 8 du 12.1.2001, p. 1.
[4] JO L 119 du 4.5.2016, p. 89.
[5] Proposition de règlement du Parlement européen et du Conseil du 17 avril 2018 *relatif au renforcement de la sécurité des cartes d'identité des citoyens de l'Union et des titres de séjour délivrés aux citoyens de l'Union et aux membres de leur famille exerçant leur droit à la libre circulation*, COM (2018) 212 final, 2018/0104 (COD)
[6] Communication de la Commission au Parlement européen et au Conseil du 8 décembre 2016: *Plan d'action visant à renforcer la réponse de l'UE aux fraudes liées aux documents de voyage*, COM(2016) 790 final
[7] Communication de la Commission au Parlement européen, au Conseil européen et au Conseil *Accroître la sécurité dans un monde de mobilité: améliorer l'échange d'informations dans la lutte contre le terrorisme et renforcer les frontières extérieures*, COM(2016) 602 final.
[8] Exposé des motifs de la proposition, p. 2.
[9] Article premier de la proposition
[10] Analyse d'impact accompagnant la proposition, SWD (2018) 110 final, p. 21
[11] Directive 2004/38/CE du Parlement européen et du Conseil du 29 avril 2004 relative au droit des citoyens de l'Union et des membres de leurs familles de circuler et de séjourner librement sur le territoire des États membres, modifiant le règlement (CEE) nº 1612/68 et abrogeant les directives 64/221/CEE, 68/360/CEE, 72/194/CEE, 73/148/CEE, 75/34/CEE, 75/35/CEE, 90/364/CEE, 90/365/CEE et 93/96/CEE, JO L 158 du 30.4.2004, p. 77.
[12] Document 9303 de l'OACI (septième édition, 2015), partie 9, chapitre 3.1.
[13] Règlement (CE) nº 1030/2002 du Conseil du 13 juin 2002 établissant un modèle uniforme de titre de séjour pour les ressortissants de pays tiers, JO L 157 du 15.6.2002, p. 1.
[14] L'article 2 du traité sur l'Union européenne (TUE) dispose que «*[l]'Union est fondée sur les valeurs de respect de la dignité humaine, de liberté, de démocratie, d'égalité, de l'État de droit, ainsi que de respect des droits de l'homme, y compris des droits des personnes appartenant à des minorités*». Par ailleurs, l'article 6, paragraphe 1, du TUE reconnaît les droits, les libertés et les principes énoncés dans la Charte des droits fondamentaux de l'Union européenne du 7 décembre 2000, telle qu'adoptée à Strasbourg le 12 décembre 2007, laquelle a la même valeur juridique que les traités. De même, l'article 6, paragraphe 3, du TUE établit que «*[l]es droits fondamentaux, tels qu'ils sont garantis par la Convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales et tels qu'ils résultent des traditions constitutionnelles communes aux États membres, font partie du droit de l'Union en tant que principes généraux*».
[15] Arrêt de la CEDH du 13 mai 2008, *affaire S. et Marper c. Royaume-Uni*, §§ 68 et 84, CEDH 2008
[16] Article 4, paragraphe 14, du 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), JO L 119 du 4.5.2016, p. 1.
[17] Voir l'article 9 du 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), JO L 119 du 4.5.2016, p. 1, et l'article 10 de la 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*, JO L 119 du 4.5.2016, p. 89.
[18] Article 6 de la convention modernisée pour la protection des personnes à l'égard du traitement des données à caractère personnel, adoptée les 17 et 18 mai 2018
[19] Le règlement général sur la protection des données entend par données personnelles sensibles les *«catégories particulières de données à caractère personnel»* [voir l'article 9 du 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), JO L 119 du 4.5.2016, p. 1]
[20] Guide du CEPD: *Guide pour l'évaluation de la nécessité des mesures limitant le droit fondamental à la protection des données à caractère personnel*, 11 avril 2017

[21] Considérant 6 de la proposition
[22] Annexe 5 de l'analyse d'impact accompagnant la proposition, p. 104 et 105. Voir également la section 2.3 du rapport CSES, qui contient de plus amples informations sur les types de cartes d'identité et titres de séjour délivrés par les autorités nationales.
[23] Analyse d'impact accompagnant la proposition, p. 12
[24] Analyse d'impact accompagnant la proposition, p. 9 et annexe 8 de l'analyse d'impact accompagnant la proposition, p. 123
[25] Annexe 8 de l'analyse d'impact accompagnant la proposition, p. 123
[26] 16 États membres seraient soumis à cette nouvelle obligation: l'Autriche, la Croatie, la République tchèque, la Finlande, la France, la Grèce, l'Irlande, l'Italie, le Luxembourg, Malte, les Pays-Bas, la Pologne, la Roumanie, la Slovaquie, la Slovénie et la Suède. Voir: annexe 8 de l'analyse d'impact accompagnant la proposition, p. 123
[27] http://www.statewatch.org/analyses/no-331-biometrics-for-identity-cards.pdf
[28] Page 7 de la proposition.
[29] Analyse d'impact accompagnant la proposition, p. 4. Bien que cela ne ressorte pas clairement du rapport, on suppose qu'il existe un chevauchement significatif entre ces deux chiffres.
[30] Analyse d'impact accompagnant la proposition, p. 12
[31] Annexe 6 de l'analyse d'impact accompagnant la proposition, p. 109, Analyse des risques annuelle FRONTEX 2016, p. 14.
[32] Analyse des risques FRONTEX, p. 22
[33] Annexe 6 de l'analyse d'impact accompagnant la proposition, p. 109
[34] À cet égard, il convient de souligner que même la Commission, dans l'analyse d'impact susmentionnée, admet que «*le nombre de documents détectés ne semble pas très élevé*». Voir: analyse d'impact accompagnant la proposition, p. 12
[35] 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), JO L 119 du 4.5.2016, p. 1.
[36] Arrêt de la Cour de justice du 17 octobre 2013, *Schwarz*, C-291/12, ECLI:EU:C:2013:670
[37] Analyse d'impact accompagnant la proposition, p. 51.
[38] Analyse d'impact accompagnant la proposition, p. 27
[39] Exposé des motifs de la proposition, p. 6
[40] Garanti à l'article 5, paragraphe 1, point b), du RGPD
[41] Plan d'action de décembre 2016, p. 10
[42] Plan d'action de décembre 2016, p. 11
[43] Analyse d'impact accompagnant la proposition, p. 14
[44] Arrêt de la Cour de justice du 17 octobre 2013, *Schwarz*, C-291/12, ECLI:EU:C:2013:670
[45] Arrêt de la Cour de justice du 17 octobre 2013, *Schwarz*, C-291/12, ECLI:EU:C:2013:670, point 37
[46] Analyse d'impact accompagnant la proposition, p. 60
[47] Article 5, paragraphe 1, point c), du RGPD
[48] Motif digital coupé et sous-échantillonné suivi de la représentation cellulaire de l'image du motif digital afin de créer les données d'échange du motif digital.
[49] Partie 9, chapitre 4.2.
[50] L'écrémage est un type d'attaque qui utilise un dispositif à proximité de la carte d'identité pour recueillir les données des documents au moment de leur utilisation.
[51] Voir par exemple: article 14 du règlement (UE) nº 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) nº 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) nº 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*, JO L 180 du 29.6.2013, p. 1.