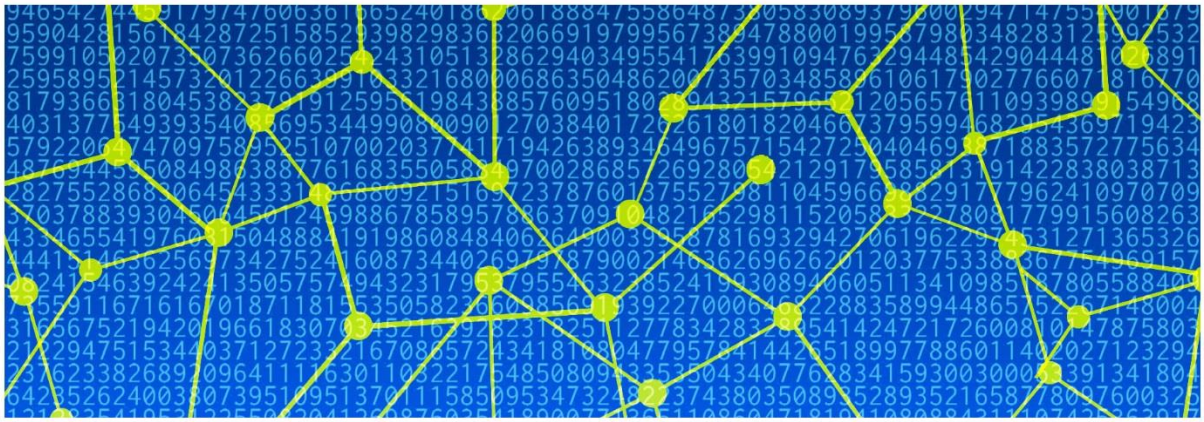

EUROPEAN DATA PROTECTION SUPERVISOR

Avis n° 9/2018

sur la proposition de nouveau règlement sur le système d'information sur les visas

12 décembre 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 (CE) nº 45/2001, «[...] [e]n 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 (CE) nº 45/2001, la Commission est tenue, «[l]orsqu'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 pour 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 se rapporte à la mission du CEPD de conseiller les institutions de l'UE 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». Il contient des recommandations sur la manière de mieux protéger le droit à la vie privée et la protection des données à caractère personnel dans le règlement proposé.

Synthèse

Afin de renforcer la sécurité et d'améliorer la gestion des frontières extérieures de l'UE, la Commission a adopté une proposition visant à améliorer le système d'information sur les visas («VIS»), la base de données centralisée de l'UE qui contient des informations sur les personnes demandant un visa Schengen.

En particulier, la proposition prévoit: a) l'abaissement de 12 à 6 ans de l'âge du relevé des empreintes digitales pour les enfants demandeurs d'un visa de court séjour, b) la centralisation au niveau de l'UE des données relatives à tous les titulaires de visas de long séjour et de titres de séjour et c) la vérification croisée des demandes de visa avec les autres systèmes d'information de l'UE dans les domaines de la liberté, de la sécurité et de la justice.

Le CEPD souligne que les données biométriques, telles que les empreintes digitales, sont très sensibles. Leur collecte et leur utilisation doivent être soumises à une analyse de stricte nécessité avant de décider de les enregistrer dans une base de données dans laquelle les données à caractère personnel d'un grand nombre de personnes seront traitées. Cette analyse est d'autant plus importante lorsqu'elle concerne des empreintes digitales d'enfants, qui sont des membres particulièrement vulnérables de la société et méritent donc une protection particulière.

Le CEPD reconnaît qu'il est de la plus haute importance de renforcer la prévention des violations des droits de l'enfant, telles que la traite des êtres humains, et la lutte contre celles-ci. Néanmoins, il constate qu'il reste difficile de savoir si et dans quelle mesure la traite d'enfants est causée ou amplifiée par les erreurs d'identification ou la non-identification des enfants entrant sur le territoire de l'UE avec un visa. Si d'autres éléments venaient à être fournis à l'appui de cette affirmation, le CEPD rappelle l'importance de veiller à ce que les empreintes digitales des enfants ne soient utilisées que lorsque cela est dans l'intérêt supérieur de l'enfant. En outre, des garanties appropriées devraient être prévues dans la proposition.

Par ailleurs, le CEPD relève qu'en enregistrant dans le VIS des données relatives à tous les titulaires de visas de long séjour et de titres de séjour, la proposition inclurait la seule catégorie de ressortissants de pays tiers qui n'est couverte actuellement par aucun des systèmes à grande échelle de l'UE dans les domaines de la liberté, de la sécurité et de la justice. Dans le contexte de la proposition d'interopérabilité des systèmes à grande échelle de l'UE, la proposition contribuerait à la création d'un réseau européen centralisé donnant accès à une quantité considérable d'informations sur tous les ressortissants de pays tiers qui ont franchi ou envisagent de franchir les frontières de l'UE (c'est-à-dire des millions de personnes). Il note que la centralisation des données relatives aux visas de long séjour et aux titres de séjour a deux objectifs: a) vérifier l'authenticité d'un document et la relation légitime avec son titulaire et b) faciliter l'échange d'informations sur les personnes dont la demande de visa a été refusée pour des raisons de sécurité. Dans ce contexte, il estime que l'harmonisation des documents sécurisés devrait faire l'objet d'un examen plus approfondi et que les données stockées dans le VIS devraient être limitées aux personnes dont le visa de long séjour ou le titre de séjour a été refusé pour des raisons de sécurité.

Enfin, la proposition prévoit la comparaison des données enregistrées dans le VIS avec les données enregistrées dans d'autres systèmes conçus et utilisés à ce jour à des fins autres que la migration. En particulier, les données relatives aux demandeurs de visas seraient comparées aux données collectées et conservées à des fins de coopération policière et judiciaire. Conformément à ses préoccupations concernant la tendance croissante consistant à brouiller les frontières entre la gestion des migrations et la lutte contre la criminalité et le terrorisme, le CEPD note que la proposition ne détermine pas clairement comment et dans quelle mesure les informations policières et judiciaires doivent être prises en compte dans le processus décisionnel de délivrance des visas. Il recommande de préciser, dans la proposition, l'objectif de la comparaison des données

du VIS avec les informations policières et judiciaires, ainsi que la procédure et les conditions applicables en ce qui concerne les résultats de cette comparaison. Il recommande également de veiller, dans la proposition, à ce que seules les informations policières et judiciaires qui font légalement partie du processus décisionnel en matière de délivrance de visas soient accessibles aux autorités chargées des visas.

TABLE DES MATIÈRES

1 INTRODUCTION 6

1.1 CONTEXTE 6

1.2 OBJECTIFS DES PROPOSITIONS 7

2 RECOMMANDATIONS PRINCIPALES 8

2.1 ABAISSEMENT DE L'ÂGE MINIMUM POUR LE RELEVÉ DES EMPREINTES DIGITALES 8

2.2 CENTRALISATION DES DONNÉES RELATIVES AUX VISAS DE LONG SÉJOUR ET AUX TITRES DE SÉJOUR 10

2.3 VÉRIFICATION CROISÉE AVEC LES DONNÉES STOCKÉES DANS D'AUTRES SYSTÈMES 13

2.3.1 ECRIS-TCN 14

2.3.2 Données Europol 14

2.3.3 Signalements SIS 15

3 RECOMMANDATIONS SPÉCIFIQUES 16

3.1 CATÉGORIES DE DONNÉES DU VIS COMPARÉES AUX DONNÉES ENREGISTRÉES DANS D'AUTRES SYSTÈMES (NOUVEL ARTICLE 9 BIS, PARAGRAPHE 3, DU RÈGLEMENT 767/2008) 16

3.2 CATÉGORIES SPÉCIFIQUES DE DEMANDEURS DE VISA (NOUVEL ARTICLE 9 TER DU RÈGLEMENT 767/2008) 17

3.3 DÉFINITION DES AUTORITÉS CENTRALES (NOUVEL ARTICLE 9 QUATER DU RÈGLEMENT 767/2008) 17

3.4 UTILISATION DES DONNÉES DU VIS AUX FINS DE L'INTRODUCTION DANS LE SIS DE SIGNALEMENTS CONCERNANT DES PERSONNES DISPARUES (NOUVEL ARTICLE 20 BIS DU RÈGLEMENT 767/2008) 18

3.5 VÉRIFICATIONS EN CAS DE RÉPONSE POSITIVE (NOUVEL ARTICLE 22 TER, PARAGRAPHES 6 ET 7, DU RÈGLEMENT 767/2008) 18

3.6 ACCÈS À DES FINS RÉPRESSIVES (NOUVEAU CHAPITRE III TER DU RÈGLEMENT 767/2008) 19

3.7 STATISTIQUES 21

3.8 UTILISATION DE DONNÉES ANONYMISÉES À DES FINS D'ESSAI 22

3.9 CONTRÔLE DE LA QUALITÉ DES DONNÉES 24

3.10 SURVEILLANCE DU VIS 24

4 CONCLUSIONS 25

REMARQUES 28

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)[1],

vu le règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) nº 45/2001 et la décision nº 1247/2002/CE[2], et en particulier les articles 42, paragraphe 1, 57, paragraphe 1, point g), et 58, paragraphe 3, point c), de celui-ci,

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[3],

A ADOPTÉ L'AVIS SUIVANT:

1 Introduction

1.1 Contexte

1 Le 6 avril 2016, la Commission a adopté une communication intitulée *Des systèmes d'information plus forts et plus intelligents pour les frontières et la sécurité*[4], afin d'engager une réflexion sur les dysfonctionnements des systèmes existants de gestion des frontières et de sécurité intérieure dans l'Union européenne et d'en optimiser les performances.

2 Le 17 juin 2016, la Commission a créé un groupe d'experts de haut niveau sur les systèmes d'information et l'interopérabilité («HLEG»), composé d'experts dans le domaine des systèmes d'information et de l'interopérabilité, désignés par les États membres, les pays associés à Schengen et les agences et organes de l'UE. L'objectif du groupe d'experts était non seulement de contribuer à une vision stratégique globale sur la manière de rendre la gestion et l'utilisation des données pour la gestion et la sécurité des frontières plus efficaces et plus efficientes, dans le plein respect des droits fondamentaux, mais aussi d'identifier des solutions pour apporter des améliorations.[5]

3 Le HLEG a présenté ses recommandations dans son rapport final en mai 2017[6]. En ce qui concerne le VIS, le groupe d'experts a formulé plusieurs recommandations, et notamment:

- étendre le champ d'application du VIS au stockage des visas de long séjour et titres de séjour,
- améliorer l'accès des services répressifs tout en respectant les normes les plus strictes en matière de protection des données,

- améliorer la qualité des données dans le système, en particulier la qualité des images faciales pour permettre des recherches multimodales à l'aide de la biométrie,
- abaisser l'âge des enfants pour le relevé des empreintes digitales, répondre aux préoccupations liées à la traite d'êtres humains impliquant des enfants et des enlèvements d'enfants, ainsi qu'aux migrations irrégulières impliquant des mineurs,
- améliorer la capacité du VIS en termes de production de statistiques et de rapports relatifs aux tendances et phénomènes migratoires.[7]

4 Le 17 août 2017, la Commission a lancé une consultation publique sur l'abaissement de 12 à 6 ans de l'âge des enfants pour le relevé des empreintes digitales dans le cadre de la procédure de visa.[8] Le 17 novembre 2017, la Commission européenne a lancé une autre consultation publique sur l'élargissement du champ d'application du système d'information sur les visas («VIS») pour y inclure des données concernant les visas de long séjour et les documents de séjour.[9] Le CEPD a participé aux deux consultations publiques et a publié deux déclarations.[10]

5 Le 15 mai 2018, la Commission a publié une proposition (ci-après la «proposition») de règlement du Parlement européen et du Conseil modifiant:

- le règlement (CE) nº 767/2008 (le «*règlement VIS*»),
- le règlement (CE) nº 810/2009 (le «*code des visas*»),
- le règlement (UE) 2017/2226 (le «*règlement EES*»),
- le règlement (UE) 2016/399 (le «*code frontières Schengen*»),
- le règlement XX/2018 (le règlement sur l'interopérabilité),
- et la décision 2004/512/CE (la «*décision VIS*»),
- et abrogeant la décision 2008/633/JAI du Conseil (la «*décision relative à l'accès des services répressifs*»).

6 Le CEPD a été invité à contribuer aux deux consultations publiques lancées par la Commission (voir point 4 ci-dessus). Étant donné que la proposition repose dans une large mesure sur le traitement de données à caractère personnel, le CEPD se demande pourquoi la Commission ne l'a pas consulté, de manière formelle ou informelle.

1.2 Objectifs des propositions

7 La proposition vise à améliorer la sécurité à l'intérieur de l'Union et de ses frontières, ainsi qu'à faciliter la gestion des frontières extérieures de l'espace Schengen. En particulier, la proposition vise à améliorer le traitement des visas, à étendre l'utilisation du VIS à de nouvelles catégories de données, à utiliser pleinement les instruments d'interopérabilité, à améliorer la qualité des données et à renforcer le système VIS.

8 À cette fin, la proposition introduit la possibilité:

- d'inclure les visas de long séjour et les titres de séjour dans le VIS, afin:
  - de vérifier l'authenticité et la validité du document ainsi que la relation légitime avec le titulaire,
  - de faciliter l'échange d'informations entre les États membres pour leur permettre de vérifier si la personne constitue une menace pour la sécurité des États membres avant qu'elle n'arrive à la frontière extérieure ou lorsqu'elle l'atteint.

- d'abaisser de 12 ans à 6 ans l'âge du relevé des empreintes digitales pour les enfants demandeurs d'un visa de court séjour afin de vérifier l'identité d'un enfant titulaire d'un visa à la frontière et de contribuer à la lutte contre la traite des êtres humains.
- de vérifier toutes les demandes de visas enregistrées dans le VIS en les comparant aux données contenues dans tous les autres systèmes d'information de l'UE dans le domaine de la liberté, de la sécurité et de la justice, en ayant recours à l'interopérabilité pour renforcer les contrôles de sécurité.
- de conserver une copie de la page des données biographiques du document de voyage du demandeur dans le VIS comme preuve à l'appui de la procédure de retour des migrants en situation irrégulière vers leur pays d'origine en cas d'absence de documents de voyage.
- d'utiliser les empreintes digitales enregistrées dans le VIS pour introduire des signalements de personnes disparues dans le système d'information Schengen (SIS).

9 Le présent avis se concentre sur les questions qui ont une incidence sur le droit fondamental des personnes à la protection des données. Le CEPD note que l'Agence des droits fondamentaux a également rendu un avis sur le système révisé d'information sur les visas et ses conséquences en matière de droits fondamentaux.[11]

10 Afin de faciliter la lecture et la compréhension de la proposition, qui modifie plusieurs textes législatifs existants, le présent avis utilise la numérotation des articles telle qu'introduite ou modifiée par la proposition dans les textes juridiques existants.

2 Recommandations principales

2.1 Abaissement de l'âge minimum pour le relevé des empreintes digitales

11 La proposition modifierait l'article 13, paragraphe 7, point a), du code des visas afin d'abaisser l'âge minimum des enfants dont les empreintes digitales peuvent être relevées lors de la procédure de demande de visa. Cet âge passerait de 12 ans à 6 ans, sur la base de deux études réalisées en 2013[12] et 2018[13]. Ces études indiquent en effet que la reconnaissance des empreintes digitales des enfants âgés de 6 à 12 ans peut être réalisée avec un niveau satisfaisant de précision dans certaines conditions.[14]

12 En abaissant l'âge à partir duquel les empreintes digitales sont relevées chez les enfants, la proposition vise:
- à permettre aux agents de vérifier l'identité d'un enfant durant la procédure de demande de visa et de procéder à des vérifications aux frontières extérieures,
- à renforcer la prévention des violations des droits de l'enfant et la lutte contre celles-ci, telles que la traite des êtres humains, en particulier en permettant d'identifier ou de vérifier l'identité des enfants ressortissants de pays tiers qui se trouvent dans l'espace Schengen dans les cas où leurs droits peuvent être ou avoir été violés (par exemple, les enfants victimes de la traite des êtres humains).

13 Le CEPD tient à souligner que le traitement des données biométriques constitue une limitation des droits fondamentaux au respect de la vie privée et à la protection des données. Comme pour toute atteinte à un droit fondamental, ce traitement doit respecter les critères énoncés à l'article 52, paragraphe 1, de la Charte des droits fondamentaux de l'Union européenne (ci-après la «Charte»)[15]. 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 En vertu du cadre juridique de l'Union[16], ainsi que de la convention 108[17] modernisée, les données biométriques sont considérées comme constituant l'une des catégories particulières de données à caractère personnel[18] 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 Le cadre juridique de l'UE identifie également les enfants comme des individus vulnérables qui méritent une protection spéciale. Le règlement général sur la protection des données («RGPD») contient un certain nombre de dispositions spécifiques pour les enfants[19]. En particulier, l'article 6, paragraphe 1, point f), du RGPD dispose que le traitement est licite lorsqu'il est «nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant».

16 Le CEPD se félicite du fait que la proposition introduise, avec les nouveaux articles 7, paragraphe 3, et 37, paragraphe 2, du règlement 767/52008, deux dispositions qui prennent en compte le bien-être des enfants et leurs besoins spécifiques. En particulier, le nouvel article 37 de la proposition dispose que les enfants doivent être informés «d'une manière adaptée à leur âge, à l'aide de brochures et/ou d'infographies et/ou de démonstrations spécialement conçues pour expliquer la procédure de relevé des empreintes digitales».

17 Par ailleurs, le CEPD insiste sur la nécessité de veiller à ce que le traitement des données biométriques des enfants 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 et de la vulnérabilité des enfants, il sera nécessaire de prévoir des garanties appropriées (voir ci-après).

18 L'analyse d'impact mentionne deux problèmes principaux:
- la difficulté de vérifier sans ambiguïté l'identité d'un enfant titulaire d'un visa, difficulté qui est amplifiée par le fait qu'un visa Schengen peut être valable 5 ans au plus, ce qui signifie qu'un enfant âgé de 12 ans lors de sa demande de visa peut obtenir un visa à entrées multiples valable jusqu'à l'âge de 17 ans,
- l'estimation selon laquelle de 1 500 à 2 000 enfants ressortissants de pays tiers âgés de moins de 12 ans pourraient être victimes de la traite dans l'espace Schengen chaque année.[20]

19 L'analyse d'impact indique que la prévention de la fraude à l'identité est considérée comme le principal avantage potentiel de la proposition par plusieurs consulats. Toutefois, elle reconnaît également qu'aucune information n'est disponible concernant l'ampleur réelle du problème.[21] Elle ne fournit aucune explication ni aucune estimation de l'étendue du problème. Les autorités compétentes n'ont signalé jusqu'à présent aucun cas concret de fraude à l'identité lié aux enfants.

20 En ce qui concerne le nombre d'enfants victimes de la traite des êtres humains, l'analyse d'impact indique que l'on estime qu'il pourrait y avoir entre 1 500 et 2 000 enfants de moins de 12 ans ressortissants de pays tiers parmi les victimes de la traite d'êtres humains dans l'espace Schengen chaque année. Bien qu'il n'existe aucune information sur le nombre d'enfants victimes de la traite qui ont voyagé avec un visa Schengen, les extrapolations indiquent qu'environ 25 % d'entre eux auraient suivi la procédure de visa (soit 375-500 enfants par an).[22]

21 L'analyse d'impact fait référence à un rapport de la Commission sur les progrès réalisés dans la lutte contre la traite des êtres humains, qui souligne que «les trafiquants exploitent les lacunes dans l'application ou le contrôle de la législation relative aux permis de travail, aux visas, aux droits des travailleurs et aux conditions de travail».[23] Il n'est toutefois pas certain que ces lacunes résultent d'erreurs d'identification ou de la non-identification des enfants de moins de 12 ans, en particulier ceux qui voyagent avec un visa pour se rendre dans l'espace Schengen.

22 **En l'absence de preuves supplémentaires attestant spécifiquement de l'existence d'une fraude à l'identité liée aux enfants, mais aussi du fait que la traite des enfants est causée ou amplifiée par les erreurs d'identification ou la non-identification des enfants entrant dans l'UE avec un visa, il est difficile de déterminer si la mesure proposée est appropriée et proportionnée. Si d'autres éléments venaient à être fournis à l'appui de cette affirmation, le CEPD rappelle l'importance de veiller à ce que les empreintes digitales des enfants ne soient utilisées que lorsque cela est dans l'intérêt supérieur de l'enfant.**

23 **Il recommande donc d'introduire dans la proposition une disposition spécifique sur les empreintes digitales des enfants afin de limiter leur utilisation et leur accès aux fins de:**

- **la vérification de l'identité de l'enfant durant la procédure de demande de visa et aux frontières extérieures et,**
- **la contribution à la prévention des violations des droits de l'enfant et à la lutte contre celles-ci dans un cas concret uniquement.**

En ce qui concerne en particulier l'accès des autorités répressives, le CEPD recommande de s'assurer que:

- **cet accès est nécessaire aux fins de la prévention ou de la détection d'un cas de traite d'enfants ou des enquêtes sur celui-ci,**
- **l'accès est nécessaire dans un cas concret,**
- **une recherche préalable dans les bases de données nationales pertinentes et dans les systèmes spécifiques au niveau de l'Union n'a donné aucun résultat,**
- **il existe des motifs raisonnables de considérer que la consultation du VIS contribuera de manière substantielle à la prévention ou à la détection du cas de traite d'enfants en question ou aux enquêtes sur celui-ci, et**
- **l'identification est dans l'intérêt supérieur de l'enfant.**

2.2 Centralisation des données relatives aux visas de long séjour et aux titres de séjour

24 Après l'identification, par le groupe d'experts de haut niveau sur les systèmes d'information et l'interopérabilité, d'un «déficit d'information»[24] en matière de visas de long séjour, de titres de séjour et de cartes de séjour, la Commission a réalisé une étude de faisabilité en vue de la mise en place d'un répertoire contenant des documents sur les

visas de long séjour, les titres de séjour et les permis de franchissement local de la frontière. L'étude recommande la mise en œuvre d'un tel répertoire dans le VIS. Cette option, qui serait la plus sûre et la moins coûteuse, pourrait être mise en œuvre avec un minimum d'efforts.[25]

25 En août 2017, la Commission a lancé une consultation publique sur l'élargissement du champ d'application du VIS pour y inclure des données concernant les visas de long séjour et les documents de séjour. Le CEPD a participé à la consultation publique. Il a souligné qu'aucun élément probant n'avait encore été fourni pour démontrer que l'extension du VIS était nécessaire et proportionnée. Par conséquent, il a invité la Commission à entreprendre une réflexion et une évaluation supplémentaires de la mesure proposée. Il a également encouragé la Commission à évaluer d'autres mesures législatives susceptibles d'atteindre les objectifs pertinents.[26]

26 En vertu de la proposition, les données biométriques (y compris deux empreintes digitales et une image faciale) relatives aux titulaires de visas de long séjour ou de titres de séjour seraient centralisées au niveau de l'UE dans le VIS. Le double problème que la proposition vise à résoudre est le suivant:

- les difficultés à vérifier de manière efficace et efficiente l'authenticité des documents, en ce qui concerne leur propriétaire légitime, ainsi qu'à vérifier pleinement l'identité de la personne qui les détient,
- l'absence d'accès et d'échange d'informations entre les États membres leur permettant de vérifier correctement que la personne ne constitue pas une menace pour la sécurité des États membres lors du contrôle des titulaires de documents aux points de passage frontaliers et sur leur territoire.[27]

27 Le CEPD rappelle que le droit à la protection des données à caractère personnel, tel que consacré à l'article 8 de la Charte des droits fondamentaux de l'Union européenne (la «Charte»), s'applique également aux ressortissants de pays tiers dont les données sont collectées, stockées et utilisées par une autorité publique soumise au droit européen. En vertu de l'article 52, paragraphe 1, de la Charte, toute limitation de ce droit doit être nécessaire et répondre véritablement à des objectifs d'intérêt général ou à la nécessité de protéger les droits et libertés d'autrui. Cela implique que la mesure envisagée doit être la moins intrusive au regard des droits en jeu.

28 Selon l'analyse d'impact, la difficulté de vérifier l'authenticité d'un document et la relation légitime avec son titulaire est due au manque d'harmonisation des documents.[28] L'analyse d'impact reconnaît qu'une harmonisation et une sécurisation plus poussées des documents contribueraient à renforcer les contrôles aux frontières extérieures et sur le territoire de l'UE, car il serait plus difficile de falsifier et de contrefaire le document, ce qui permettrait d'améliorer la sécurité au sein de l'UE.[29]

29 Le CEPD note toutefois que cette option n'a pas été retenue car «elle ne serait pas utile pour améliorer la sécurité par un meilleur échange d'informations», c'est-à-dire le deuxième objectif de la centralisation au niveau de l'UE des données relatives aux visas de long séjour et aux titres de séjour.[30] En particulier, l'analyse d'impact affirme que, «afin de pouvoir évaluer si la personne peut constituer une menace pour la sécurité des États membres ou si elle peut être un usurpateur d'identité, il est important d'avoir accès aux informations pertinentes sur les demandes antérieures présentées par cette personne et qui ont été rejetées par d'autres États membres pour des raisons de sécurité nationale

ou à cause de revendications frauduleuses établies (en matière d'identité ou de documents)».[31]

30 En vertu de la proposition, les données relatives aux visas de long séjour et aux titres de séjour seraient comparées aux données stockées dans d'autres systèmes, afin de déterminer si une personne est connue pour un refus d'autorisation de voyage, d'entrée ou de visa (de court séjour) qui est fondé sur des raisons de sécurité (nouvel article 22 ter, paragraphe 5, du règlement 767/2008). Le CEPD reconnaît que ces informations sont pertinentes pour garantir une évaluation complète du risque pour la sécurité posé par un ressortissant d'un pays tiers souhaitant entrer sur le territoire de l'UE.

31 Toutefois, le CEPD s'interroge sur la nécessité de centraliser et de stocker au niveau de l'UE les données de *tous* les titulaires d'un visa de long séjour ou d'un titre de séjour, afin de remédier au manque d'accès et d'échange d'informations entre les États membres et de leur permettre de vérifier correctement que la personne ne constitue pas une menace pour la sécurité. Les informations stockées dans le VIS devraient être limitées aux personnes physiques:

- dont les données correspondent à des données stockées dans un autre système ou pour lesquelles des doutes subsistent quant à leur identité,
- dont la demande de visa de long séjour et/ou de titre de séjour a été refusée parce qu'elles ont été considérées comme constituant une menace pour l'ordre public, la sécurité intérieure ou la santé publique, ou parce qu'elles ont présenté des documents qui ont été acquis par des manœuvres frauduleuses, falsifiés ou manipulés.

32 Le CEPD relève qu'en enregistrant dans le VIS tous les visas de long séjour et titres de séjour, la proposition inclurait la seule catégorie de ressortissants de pays tiers qui ne sont actuellement couverts par aucun des systèmes à grande échelle de l'UE.[32] Compte tenu, entre autres, de l'interconnectivité envisagée des systèmes à grande échelle de l'UE, telle qu'elle est exposée dans la proposition sur l'interopérabilité[33], la proposition contribuerait à la création d'un réseau européen centralisé donnant accès à une quantité considérable d'informations sur tous les ressortissants de pays tiers qui ont franchi ou envisagent de franchir les frontières de l'UE (c'est-à-dire des millions de personnes) et comprenant des données biométriques qui sont par nature très sensibles.

33 En particulier, en ce qui concerne les données biométriques, le CEPD note que la délivrance de visas de long séjour et de titres de séjour est principalement régie par le droit national. L'analyse d'impact souligne que la situation en matière de collecte de données biométriques est très différente d'un État membre à l'autre. En effet, certains États membres ne collectent pas et ne stockent pas les données biométriques et, même lorsqu'ils le font, le nombre d'empreintes digitales relevées et les critères de qualité diffèrent.[34] En ce qui concerne les exigences en matière de données biométriques pour les visas de long séjour et les titres de séjour, le CEPD rappelle qu'une fois introduites au niveau de l'UE, les États membres ne pourraient pas les annuler par de simples mesures nationales.

34 **Compte tenu de ce qui précède, le CEPD recommande que la possibilité d'harmoniser les documents sécurisés relatifs aux visas de long séjour et aux titres de séjour soit examinée plus avant et que les informations stockées dans le VIS soient limitées aux personnes physiques:**

- **dont les données correspondent à des données stockées dans un autre système ou pour lesquelles des doutes subsistent quant à leur identité,**
- **dont la demande de visa de long séjour ou de titre de séjour a été refusée parce qu'elles ont été considérées comme constituant une menace pour l'ordre public, la sécurité intérieure ou la santé publique ou parce qu'elles ont présenté des documents qui ont été acquis par des manœuvres frauduleuses, falsifiés ou manipulés.**

2.3 Vérification croisée avec les données stockées dans d'autres systèmes

35 Conformément au nouvel article 9 bis, paragraphe 3, et à l'article 22 ter, paragraphe 2, du règlement 767/2008, les données enregistrées dans le VIS seraient comparées aux données Europol et aux données stockées dans:

- le VIS
- le système d'information Schengen («SIS»)
- le système d'entrée/sortie («EES»)
- le système européen d'information sur les autorisations de voyage («ETIAS»)
- l'Eurodac,
- le système ECRIS-TCN,
- la base de données d'Interpol sur les documents de voyage volés et perdus (SLTD) et la base de données d'Interpol sur les documents de voyage associés aux notices (Interpol TDAWN).

36 Cette comparaison serait effectuée aux fins:

En ce qui concerne les visas de court séjour:

– d'examiner si le demandeur remplit les conditions d'entrée prévues par le code des visas et le code frontières Schengen, à savoir:
  - il est en possession d'un document de voyage valide;
  - il justifie les buts et conditions du séjour envisagé et dispose de moyens de subsistance suffisants;
  - il ne fait pas l'objet d'un signalement dans le SIS aux fins de non-admission.
– d'évaluer si le demandeur:
  - présente un risque d'immigration clandestine ou un risque pour la sécurité des États membres
  - a l'intention de quitter le territoire avant l'expiration du visa demandé.
– de vérifier que le document de voyage présenté n'est pas faux ou falsifié,
– de vérifier que le demandeur n'est pas considéré comme constituant une menace pour l'ordre public, la sécurité intérieure ou la santé publique, ou pour les relations internationales de l'un des États membres, et, en particulier, qu'il ne fait pas l'objet, pour ces mêmes motifs, d'un signalement dans les bases de données nationales des États membres aux fins de non-admission.

En ce qui concerne les visas de long séjour et les titres de séjour:

– d'évaluer si la personne peut constituer une menace pour l'ordre public, la sécurité intérieure ou la santé publique des États membres.

2.3.1 *ECRIS-TCN*

37 En vertu des nouveaux articles 9 bis, paragraphe 3, et 22 ter, paragraphe 2, du règlement 767/2008, la comparaison des données introduites dans le VIS avec les données enregistrées dans l'ECRIS-TCN sera effectuée «en ce qui concerne les condamnations relatives aux infractions terroristes et aux autres formes d'infractions pénales graves». Le CEPD se demande comment il serait possible, dans le cadre de l'interrogation automatisée de l'ECRIS-TCN, de veiller à ce que seules les informations sur les condamnations relatives à ces catégories d'infractions donnent lieu à une réponse de concordance/non-concordance (c'est-à-dire lorsque les données stockées dans le VIS correspondent à des données stockées dans un ou plusieurs autres systèmes). Il note que, conformément à la proposition qui l'établit[35], l'ECRIS-TCN ne contiendrait que des données relatives à la personne condamnée et à l'État membre qui détient les informations sur la condamnation. En d'autres termes, la consultation de l'ECRIS-TCN permettrait de savoir si la personne a été condamnée (ou non) dans un État membre mais pas pour quelle(s) infraction(s).

38 Le CEPD tient à rappeler que l'existence (ou l'absence) d'un «résultat positif» doit toujours être considérée comme une donnée à caractère personnel. En effet, même avec le minimum absolu d'informations (par exemple, connu ou inconnu dans un système donné), une «concordance» ou «non-concordance» constitue une information relative à une personne (par exemple, la personne a été condamnée ou non). En conséquence, le traitement de ces données constitue une atteinte aux droits fondamentaux protégés par les articles 7 et 8 de la Charte et doit respecter l'article 52, paragraphe 1, de la Charte en termes de nécessité et de proportionnalité. Le CEPD estime que la possibilité pour une autorité chargée des visas de savoir qu'une personne a été condamnée pour une infraction autre qu'une infraction terroriste ou une infraction pénale grave ne serait pas conforme aux exigences de nécessité et de proportionnalité. Cette divulgation trop large pourrait également nuire aux demandeurs, car les autorités chargées des visas pourraient hésiter à accorder un visa à une personne qui a été condamnée, même si sa condamnation ne concerne pas un acte terroriste ou une autre infraction pénale grave.

39 **Par conséquent, le CEPD recommande d'inclure dans la proposition des garanties selon lesquelles seules les informations stockées dans l'ECRIS-TCN relatives à des infractions terroristes et autres infractions pénales graves seraient communiquées à l'autorité centrale. Une des possibilités serait que l'autorité centrale ne soit pas informée de la réponse positive, mais qu'une notification soit automatiquement adressée à l'autorité compétente de l'État membre qui a introduit les données à l'origine de la réponse positive. L'autorité compétente de l'État membre en informerait alors l'autorité centrale, le cas échéant. Alternativement, la possibilité de consulter le système ECRIS-TCN devrait être supprimée.**

2.3.2 *Données Europol*

40 Le CEPD souligne que la proposition n'est pas claire en cas de réponse positive à la suite d'une comparaison des données du VIS avec celles d'Europol. En ce qui concerne les visas de court séjour, le nouvel article 9 quater, paragraphe 8, du règlement 767/2008 dispose que si Europol est identifié comme ayant fourni les données à l'origine de la réponse positive, «l'autorité centrale de l'État membre responsable consulte l'unité nationale d'Europol afin de prendre des mesures de suivi conformément au règlement 2016/794, et notamment son chapitre IV». En ce qui concerne les visas de long

séjour et les titres de séjour, le nouvel article 22, point b), paragraphe 7, point j), dispose seulement que «si la réponse positive est liée à des données d'Europol, l'unité nationale d'Europol est informée en vue d'un suivi».

41 Le CEPD rappelle que les données d'Europol sont collectées et utilisées à des fins répressives. Le CEPD s'interroge sur le rôle et l'impact des données traitées à des fins répressives dans le processus décisionnel de délivrance des visas. Il note que l'utilisation de l'expression «suivi» est trop vague et peu claire. Cela signifie-t-il qu'Europol donnerait un avis (motivé) sur la délivrance (ou non) du visa ou qu'il serait informé du (ou des) résultat(s) positif(s) afin d'utiliser ces informations dans le cadre de ses propres missions?

42 Dans le premier cas, le CEPD se demande dans quelle mesure, dans quelles conditions et sur quelle base juridique les données d'Europol seraient prises en compte dans le processus de délivrance des visas, et si cela permettrait aux autorités chargées des visas d'accéder à ces données. Dans le second cas, le CEPD a souligné à plusieurs reprises que l'accès aux données stockées dans des systèmes conçus à des fins autres que répressives ne devrait pas être accordé systématiquement mais uniquement dans des circonstances spécifiques, au cas par cas et dans des conditions strictes. Le transfert automatique d'informations du VIS à Europol à des fins répressives, sans aucune garantie, aurait pour effet de contourner les règles et conditions auxquelles Europol doit se conformer pour accéder aux données stockées dans le VIS. **Le CEPD recommande de préciser, dans la proposition, l'objectif de la comparaison des données du VIS avec les données d'Europol, ainsi que la procédure et les conditions applicables en ce qui concerne les résultats de cette comparaison.**

2.3.3 *Signalements SIS*

43 Le CEPD note que la proposition ne précise pas clairement les objectifs de la comparaison entre les données du VIS et les signalements SIS, tant dans le contexte de la délivrance des visas qu'au regard des objectifs du SIS.

a) Comparaison des données relatives aux visas avec les signalements SIS des services répressifs à des fins de migration (nouvel article 9 bis, paragraphe 3, du règlement 767/2008)

44 En vertu du nouvel article 9 bis, paragraphe 3, du règlement (CE) n° 767/2008, le VIS interrogerait différents systèmes, dont le SIS, afin de vérifier si le demandeur de visa remplit les conditions d'entrée énoncées dans le code des visas et le code frontières Schengen. Le CEPD relève que la proposition ne précise pas si la comparaison serait effectuée avec tous les signalements SIS ou seulement avec un ou plusieurs signalements spécifiques. Il souligne que, contrairement aux signalements liés à un refus d'entrée, les autres signalements SIS ne portent pas sur les conditions d'entrée mais sur des tâches répressives (par exemple, arrêter une personne, retrouver une personne disparue, effectuer des contrôles discrets sur des suspects, etc). Le CEPD estime que les autorités chargées des visas ne devraient pas être autorisées à accéder à ces signalements à moins qu'ils ne fassent légalement partie du processus décisionnel en matière de délivrance de visas.

45 Dans ce contexte, le CEPD note qu'en vertu de l'article 21 du code des visas tel que modifié par la proposition, le consulat tiendrait compte des signalements de personnes

recherchées en vue d'une arrestation ou aux fins de remise ou recherchées en vue d'une arrestation aux fins d'extradition. Cela supposerait que ce signalement serait pris en compte pour l'octroi (ou non) d'un visa à un demandeur. Le CEPD s'interroge sur l'incidence de ces signalements sur la procédure de délivrance des visas, compte tenu des objectifs répressifs d'un tel signalement. Un consulat hésitera à accorder un visa à des personnes faisant l'objet d'un mandat d'arrêt européen, alors qu'il serait dans l'intérêt des autorités répressives que ces personnes obtiennent un visa pour les arrêter lorsqu'elles se présentent aux frontières européennes.

46 **Le CEPD estime que la proposition devrait être clarifiée en ce qui concerne les types de signalements SIS à prendre en compte dans la procédure de délivrance des visas. Il recommande de veiller, dans la proposition, à ce que seuls les signalements qui font légalement partie du processus décisionnel en matière de délivrance de visas produisent une réponse positive accessible aux autorités chargées des visas.**

b) Utilisation des données du VIS aux fins des objectifs du SIS (nouvel article 9 bis, paragraphe 5, nouvel article 9 quater, paragraphe 7, et nouvel article 22 ter, paragraphe 4, du règlement 767/2008)

47 Les nouveaux articles 9 bis, paragraphe 5, et 22 ter, paragraphe 4, du règlement 7676/2008 prévoient qu'à l'appui des objectifs du SIS, les données du VIS sont comparées aux données stockées dans le SIS afin de détecter si la personne est:
- recherchée en vue d'une arrestation aux fins de remise ou d'extradition,
- portée disparue,
- recherchée en vue d'apporter son concours dans le cadre d'une procédure judiciaire ou
- soumise à des contrôles discrets ou spécifiques.

48 Conformément au nouvel article 9 quater, paragraphe 7, et à l'article 22 ter, paragraphe 4, dernier alinéa, en cas de réponse positive liée à un signalement SIS susmentionné, le VIS envoie une notification automatique à l'«autorité centrale de l'État membre qui a lancé la recherche afin qu'elle prenne les mesures de suivi qui s'imposent».

49 Le CEPD croit comprendre que l'objectif de cette disposition est que les services répressifs soient automatiquement informés lorsqu'une personne signalée dans le SIS a introduit une demande relative à un visa. Toutefois, il tient à souligner que l'expression «[prendre] les mesures de suivi qui s'imposent» est trop vague et ne permet pas de déterminer, avec suffisamment de précision, les objectifs et les conditions de l'utilisation (ultérieure) des données du VIS. **Il recommande donc de préciser la signification de «mesures de suivi qui s'imposent», afin de permettre une évaluation appropriée de la nécessité et de la proportionnalité de l'utilisation (ultérieure) des données du VIS.**

3 Recommandations spécifiques

3.1 Catégories de données du VIS comparées aux données enregistrées dans d'autres systèmes (nouvel article 9 bis, paragraphe 3, du règlement 767/2008)

50 Le nouvel article 9 bis, paragraphe 3, du règlement 767/2008 dispose que les données pertinentes mentionnées à l'article 9, paragraphe 4, de ce règlement seraient comparées aux données enregistrées dans d'autres systèmes. Le CEPD estime que la formulation

«pertinentes» n'est pas suffisamment précise. Il **recommande de préciser quelles données visées à l'article 9, paragraphe 4, du règlement 767/2008 seront comparées aux données enregistrées dans d'autres systèmes**. Il rappelle que les données à comparer doivent être adéquates et limitées à ce qui est nécessaire au regard de la finalité de la comparaison. Par exemple, il ne semble pas nécessaire de comparer les données relatives à l'employeur du demandeur (article 9, paragraphe 4, point l) avec les données enregistrées dans d'autres systèmes.

3.2 Catégories spécifiques de demandeurs de visa (nouvel article 9 ter du règlement 767/2008)

51 En ce qui concerne les membres de la famille des citoyens de l'UE et des autres ressortissants de pays tiers jouissant du droit à la libre circulation en vertu du droit de l'Union, le nouvel article 9 ter du règlement 767/2008 prévoit que la comparaison de leurs données avec les données enregistrées dans d'autres systèmes est effectuée «aux seules fins de vérifier qu'il n'existe aucun indice concret ni aucun motif raisonnable fondé sur des indices concrets permettant de conclure que la présence de la personne sur le territoire des États membres constitue un risque en matière de sécurité ou un risque épidémique élevé (…)».

52 Le CEPD s'interroge sur la différence entre «indices concrets» et «motif raisonnable fondé sur des indices concrets». Il suppose qu'il s'agit d'une erreur d'impression et **recommande de ne mentionner que des «motifs raisonnables fondés sur des indices concrets». Si les termes «indices concrets» et «motifs raisonnables fondés sur des indices concrets» renvoient à des situations différentes, le CEPD recommande de le préciser, au moins dans un considérant.**

3.3 Définition des autorités centrales (nouvel article 9 quater du règlement 767/2008)

53 En cas de réponse positive (c'est-à-dire lorsque les données stockées dans le VIS correspondent à des données stockées dans un ou plusieurs autres systèmes), le nouvel article 9 quater du règlement 767/2008 prévoit que l'autorité centrale de l'État membre qui traite la demande vérifie manuellement si l'identité du demandeur correspond aux données enregistrées dans les systèmes à l'origine de la réponse positive. Si les données correspondent ou qu'un doute subsiste quant à l'identité, l'autorité centrale consulte l'autorité centrale du ou des États membres qui ont été identifiés comme ayant saisi les données ayant déclenché la réponse positive. Si Europol est identifié comme ayant fourni les données à l'origine d'une réponse positive, l'autorité centrale de l'État membre responsable consulte l'unité nationale d'Europol.

54 Le CEPD note que la proposition n'introduit pas de définition de l'«autorité centrale» dans le règlement 767/2008 et que le nouvel article 9 quater comporte différentes formulations de cette notion, à savoir l'autorité centrale de l'État membre qui traite la demande (§ 1), l'autorité centrale (§ 3), les autorités centrales des autres États membres (§ 5-6), l'autorité centrale de l'État membre qui a lancé la recherche (§ 7) et l'autorité centrale de l'État membre responsable (§ 8). En outre, le CEPD croit comprendre que ces autorités centrales se réfèrent, dans certains cas, aux autorités chargées des visas (p. ex. § 1) et, dans d'autres cas, aux autorités de police (p. ex. § 7). Ce libellé est donc source de confusion. **Le CEPD recommande de préciser, dans le nouvel article 9 quater du règlement 767/2008, à quelle autorité se réfère précisément chaque paragraphe.**

3.4 Utilisation des données du VIS aux fins de l'introduction dans le SIS de signalements concernant des personnes disparues (nouvel article 20 bis du règlement 767/2008)

55 Le nouvel article 20 bis, paragraphe 1, du règlement 767/2008 prévoit la possibilité d'utiliser les données dactyloscopiques conservées dans le VIS aux fins de l'introduction d'un signalement concernant des personnes disparues conformément à la législation du SIS. Le CEPD croit comprendre que l'objectif est de «copier» les empreintes digitales conservées dans le VIS dans le SIS, lors de la création d'un signalement concernant une personne disparue en possession d'un visa (par exemple après la disparition d'un enfant voyageant avec sa famille dans le territoire Schengen). Toutefois, le CEPD estime que le libellé du nouvel article 20 bis, paragraphe 2 («en cas de réponse positive à un signalement dans le SIS tel que visé au paragraphe 1»), est ambigu, dans la mesure où il semble renvoyer à une vérification des données dactyloscopiques par rapport au SIS et non à la création d'un signalement. **Le CEPD demande que cette disposition soit clarifiée.**

3.5 Vérifications en cas de réponse positive (nouvel article 22 ter, paragraphes 6 et 7, du règlement 767/2008)

56 Le CEPD note que la proposition établit une distinction entre les visas de long séjour et les titres de séjour délivrés ou prorogés (i) par un poste consulaire ou (ii) sur le territoire d'un État membre.

a) Délivrance ou prorogation par un poste consulaire

57 En cas de délivrance ou de prorogation d'un visa de long séjour ou d'un titre de séjour par une autorité consulaire, le nouvel article 22 ter, paragraphe 6, du règlement 767/2008 dispose que le nouvel article 9 bis du règlement 767/2008 s'applique. Le CEPD note que la référence au nouvel article 9 bis n'est pas claire.

58 Premièrement, le nouvel article 9 bis relève du chapitre II, qui traite des visas de court séjour, tandis que les règles relatives aux visas de long séjour et aux titres de séjour figurent au chapitre III. Deuxièmement, conformément au nouvel article 9 bis, d'autres systèmes feront l'objet de recherches lorsqu'«un dossier de demande est créé ou un visa est délivré». Cela signifierait-il que, par dérogation au nouvel article 22 bis du règlement 767/2008, lorsque des visas de long séjour et des titres de séjour sont délivrés ou prorogés par une autorité consulaire, les autres systèmes feront l'objet de recherches dès qu'une demande aura été introduite et non après la prise d'une décision sur la demande? Ce point demande à être clarifié. En outre, le CEPD relève que la proposition ne prévoit pas l'obligation de vérifier les résultats positifs résultant des recherches effectuées dans d'autres systèmes. **Il recommande donc de clarifier la référence au nouvel article 9 bis dans le nouvel article 22 ter, paragraphe 6, et de prévoir une procédure similaire à celle prévue à l'article 9 quater, paragraphes 1 à 6, du règlement 767/2008, afin de garantir que toute réponse positive concernant un visa de long séjour ou un titre de séjour délivré ou prolongé par un poste consulaire soit vérifiée manuellement par une autorité compétente.**

b) Délivrance ou prorogation par une autorité sur le territoire d'un État membre

59 Lorsqu'une autorité sur le territoire d'un État membre délivre un titre de séjour ou proroge un visa de long séjour ou un titre de séjour, elle vérifie si les données relatives au visa de

long séjour ou au titre de séjour correspondent aux données figurant dans le VIS ou dans un des systèmes consultés (c'est-à-dire SIS, EES, ETIAS, ECRIS-TCN), dans les données Europol ou dans les bases de données d'Interpol (nouvel article 22 ter, paragraphe 7, point 7 a), du règlement 767/2008]. Lorsque les données ne correspondent pas et qu'aucune autre réponse positive n'a été obtenue, le nouvel article 22 ter, paragraphe 7, point c), dispose que l'autorité efface la fausse réponse positive du «dossier de demande». Étant donné que les données relatives aux visas de long séjour et aux titres de séjour sont stockées dans un dossier individuel (nouveaux articles 22 quater à 22 septies du règlement 767/2008), **le CEPD recommande de remplacer l'expression «dossier de demande» par «dossier individuel» dans le nouvel article 22 ter, paragraphe 7, point k), du règlement 767/2008,** afin d'éviter toute confusion avec les données relatives aux visas de court séjour qui sont stockées dans un «dossier de demande» (voir articles 8 à 14 du règlement 767/2008).

60 Enfin, le CEPD souligne que le nouvel article 22 ter, paragraphe 7, n'est pas clair en ce qui concerne le résultat des vérifications concluant que les données relatives aux visas de long séjour ou aux titres de séjour correspondent aux données stockées dans d'autres systèmes, ou lorsque des doutes subsistent quant à l'identité du titulaire d'un visa de long séjour ou d'un titre de séjour. Il note que le nouvel article 22 ter, paragraphe 7, ne fait référence qu'aux situations dans lesquelles la réponse positive se rapporte à certains signalements spécifiques dans le SIS, mais est silencieux sur la ou les réponses positives résultant des recherches effectuées dans d'autres systèmes. En outre, le CEPD constate que la proposition ne prévoit pas l'inclusion des résultats des vérifications dans le VIS, comme le prévoit le nouvel article 9 quater, paragraphe 6, du règlement 767/2008 pour les visas de court séjour. En conséquence, on peut s'interroger sur la valeur ajoutée de ces vérifications par rapport aux objectifs de sécurité poursuivis par la proposition. **Le CEPD recommande de clarifier dans la proposition le résultat des vérifications concluant que les données relatives aux visas de long séjour ou aux titres de séjour correspondent aux données stockées dans d'autres systèmes, ou lorsque des doutes subsistent quant à l'identité du titulaire d'un visa de long séjour ou d'un titre de séjour.**

3.6 Accès à des fins répressives (nouveau chapitre III ter du règlement 767/2008)

61 L'accès des services répressifs au VIS est actuellement réglementé par la décision 2008/633/JAI du Conseil[36], qui fixe les exigences et conditions spécifiques de cet accès. La proposition abrogerait la décision du Conseil et transposerait les règles régissant l'accès des services répressifs au VIS dans un nouveau chapitre III ter du règlement 767/2008. Ce chapitre réglementerait l'accès des services répressifs à toutes les données du VIS, y compris celles relatives aux visas de long séjour et aux titres de séjour.

62 Le CEPD note que le considérant 25 de la proposition indique que l'«accès aux données du VIS à des fins répressives a déjà prouvé son utilité pour identifier des personnes décédées d'une mort violente ou pour aider les enquêteurs à progresser sensiblement dans des affaires de traite d'êtres humains, de terrorisme ou de trafic de drogues». Il conclut que les données du VIS relatives aux visas de long séjour devraient donc également être mises à la disposition des services répressifs. Toutefois, le CEPD relève que l'analyse d'impact ne fournit aucune indication supplémentaire sur la manière dont l'accès aux données du VIS relatives aux visas de court séjour a prouvé son utilité, et n'explique pas pourquoi l'accès aux données relatives aux visas de long séjour serait nécessaire. En

outre, il note que si la proposition prévoit l'accès des services répressifs aux données relatives aux visas de long séjour et aux titres de séjour, le considérant 25 ne mentionne que les données relatives aux visas de long séjour.

63 Le CEPD rappelle que la simple mention de l'utilité de l'accès ne suffit pas à justifier une limitation potentiellement grave du droit à la protection des données. **En l'absence de preuves supplémentaires et d'une évaluation factuelle détaillée de la nécessité, pour les services répressifs, d'accéder aux données relatives aux visas de long séjour et aux titres de séjour à des fins répressives, il est difficile de garantir que cet accès est approprié et proportionné.**

64 En outre, le nouvel article 22 duodecies du règlement 767/2008 prévoit que les États membres doivent notifier à l'agence eu-LISA et à la Commission leurs autorités répressives désignées qui sont habilitées à consulter le VIS, ainsi que les points d'accès centraux désignés. Toutefois, si l'article 3, paragraphe 4, de la décision 2008/633/JAI du Conseil dispose que la Commission publie les déclarations des États membres au Journal officiel de l'Union européenne, le nouvel article 22 duodecies ne contient aucune disposition correspondante. Dans un souci de transparence, **le CEPD recommande d'ajouter, dans le nouvel article 22 duodecies du règlement 767/2008, l'obligation pour la Commission de publier les déclarations des États membres au Journal officiel de l'Union européenne**.

65 Le nouvel article 22 quaterdecies du règlement 767/2008 correspond à l'article 4 de la décision 2008/633 du Conseil qui réglemente l'accès au VIS en cas d'urgence exceptionnelle. Le CEPD se félicite que le paragraphe 2 de cet article instaure un délai de sept jours pour que le point d'accès central puisse vérifier si les conditions d'accès sont remplies, y compris pour déterminer s'il s'agissait effectivement d'un cas d'urgence. Il se réjouit également du fait que le paragraphe 3 de ce même article précise que si la vérification détermine que l'accès n'était pas justifié, toutes les autorités ayant accédé aux données du VIS devront les effacer et en informer le point d'accès central.

66 Le CEPD estime que le nouvel article 22 quindecies, paragraphe 4, du règlement 767/2008 manque de clarté. Cet article indique en effet que la consultation du VIS, en cas de réponse positive, permet d'accéder aux données énumérées «au présent paragraphe», ainsi qu'à toute autre donnée extraite du «dossier individuel». Premièrement, l'article 22 quindecies, paragraphe 4, ne fournit pas une telle énumération, de sorte qu'il n'établit pas clairement de quelles données il s'agit. Deuxièmement, l'utilisation de l'expression «dossier individuel» prête à confusion dans la mesure où les données relatives aux visas de court séjour sont stockées dans le VIS dans un «dossier de demande» (article 8 du règlement 767/2008) et les données relatives aux visas de long séjour et aux titres de séjour sont conservées dans un «dossier individuel» (nouvel article 22 bis du règlement 767/2008). Enfin, la dernière phrase du nouvel article 22 quindecies, paragraphe 4, renvoie à l'article 9, point 4, paragraphe 1, qui semble ne pas exister. En outre, cela semble impliquer l'existence d'une procédure de vérification spécifique pour accéder à certaines catégories de données stockées dans le VIS, en plus de la procédure prévue au nouvel article 22 quaterdecies du règlement 767/2008. **Le CEPD recommande de clarifier le nouvel article 22 quindecies, paragraphe 4, du règlement 767/2008 en ce qui concerne les catégories de données qui seront accessibles en cas de réponse positive et les conditions d'accès.**

67 Le CEPD note que le nouvel article 22 sexdecies du règlement 767/2008 prévoit des dérogations aux conditions d'accès des autorités répressives aux données du VIS aux fins de l'identification des personnes portées disparues, enlevées ou identifiées comme victimes de la traite des êtres humains. Cet accès serait autorisé lorsqu'il existe des motifs raisonnables de considérer que la consultation des données du VIS contribuera à l'identification de la personne, et/ou contribuera à enquêter sur des cas concrets de traite d'êtres humains. Le nouvel article 22 sexdecies semble faire une distinction entre, d'un côté, l'identification d'une personne après sa découverte ou sa libération, et, de l'autre, l'identification d'une personne qui contribuera à enquêter sur un cas concret de traite d'êtres humains. En ce qui concerne l'identification d'une personne qui contribuera à enquêter sur un cas concret de traite d'êtres humains, le CEPD souligne que cet accès est clairement lié à la prévention et à la détection d'une infraction pénale grave, et aux enquêtes sur celle-ci, et relèverait donc du nouvel article 22 quindecies de la proposition. **Le CEPD ne voit aucune raison pour laquelle cet accès ne devrait pas être soumis aux conditions énoncées dans le nouvel article 22 quindecies et recommande vivement de prévoir des justifications pour les dérogations.**

68 Enfin, le CEPD rappelle que les autorités nationales chargées de la protection des données ne sont pas chargées de vérifier la recevabilité d'une demande d'accès au VIS. Dans la mesure où le nouvel article 22 octodecies, paragraphe 3, du règlement 767/2008 fait référence à la recevabilité, celle-ci relèverait de la responsabilité du point d'accès central. **Le CEPD recommande de supprimer la formulation «vérification de la recevabilité de la demande» dans le nouvel article 22 octodecies, paragraphe 3, du règlement 767/2008.**

3.7 Statistiques

69 Conformément au nouvel article 45 bis du règlement 767/2008, le personnel dûment autorisé des autorités compétentes des États membres, de la Commission, de l'agence eu-LISA et de l'Agence européenne de garde-frontières et de garde-côtes est autorisé à accéder aux données conservées dans le VIS aux fins de l'établissement de rapports et de statistiques, sans que l'identification individuelle ne soit permise.

70 Le CEPD comprend la nécessité d'avoir accès aux données contenues dans le VIS aux fins de l'établissement de rapports et de statistiques. Toutefois, il convient de noter que, contrairement au libellé du nouvel article 45 bis, la combinaison de la nationalité, du sexe et de l'année de naissance d'une personne pourrait conduire à une identification individuelle.

71 Par conséquent, **le CEPD recommande de reformuler le nouvel article 45 bis du règlement 767/2008 de façon à reconnaître que les données énumérées à l'article 45 bis, paragraphe 1, pourraient conduire à l'identification de personnes et doivent donc être protégées.**

72 En outre, le CEPD observe que le nouvel article 45 bis, paragraphe 2, dispose que l'agence eu-LISA stocke les données visées au nouvel article 45 bis, paragraphe 1, dans le répertoire central des rapports et statistiques (CRRS) qui sera établi par le règlement sur l'interopérabilité[37].

73 Le CEPD rappelle qu'il a mis en garde, dans son avis sur l'interopérabilité[38], contre la création d'un tel répertoire statistique. Il réaffirme qu'un tel répertoire statistique imposerait une lourde charge à l'agence eu-LISA et au CEPD, puisque l'agence eu-LISA devrait maintenir et sécuriser un deuxième répertoire, tandis que le CEPD devrait superviser ce deuxième répertoire.

74 Dès lors, **le CEPD serait favorable à une solution qui, au lieu de rendre nécessaire un répertoire central supplémentaire, imposerait à l'agence eu-LISA l'obligation de développer des fonctionnalités permettant aux États membres, à la Commission, à l'agence eu-LISA elle-même et aux agences autorisées d'extraire automatiquement les statistiques demandées directement du système.**.

3.8 Utilisation de données anonymisées à des fins d'essai

75 Le nouvel article 26, paragraphe 8 bis, du règlement 767/2008 dispose que l'agence eu-LISA est autorisée à utiliser des données à caractère personnel réelles anonymisées à des fins d'essai a) à des fins de diagnostic et de réparation lorsque des défaillances du système central sont découvertes, ou b) pour tester de nouvelles technologies et techniques permettant d'améliorer les performances du système central ou la transmission de données à ce dernier.

76 Ni l'analyse d'impact ci-jointe, ni l'exposé des motifs ne traitent de l'utilisation de données à caractère personnel réelles anonymisées. L'annexe 4 de l'analyse d'impact, qui présente les suggestions du programme pour une réglementation affûtée et performante (REFIT), mentionne simplement la «*possibilité pour l'agence eu-LISA d'utiliser des données (alphanumériques et) dactyloscopiques anonymisées à des fins d'essai (similaires à celles prévues à l'article 5 Gestion opérationnelle de la proposition Eurodac)*», et indique également que l'«*amélioration des performances résultant des essais bénéficiera à tous les utilisateurs finals du système*».

77 En l'absence d'une explication précise de la Commission, il est difficile de savoir quelles données à caractère personnel sont visées par le nouvel article 26, paragraphe 8 bis, du règlement 767/2008, mais aussi pourquoi l'agence eu-LISA a besoin d'utiliser des données réelles pour améliorer le VIS. Or, l'annexe 4 de l'analyse d'impact semble laisser entendre que certaines données alphanumériques et dactyloscopiques (abrégées en «FP») devraient être utilisées.

78 Le CEPD reconnaît qu'une fois que les données alphanumériques ont été réellement anonymisées et que les personnes ne sont plus identifiables, le droit européen en matière de protection des données ne s'applique plus. Toutefois, il rappelle que l'anonymisation des données alphanumériques constitue un traitement ultérieur de données à caractère personnel et qu'à ce titre, elle doit satisfaire à l'exigence de compatibilité en tenant compte des motifs et circonstances juridiques du traitement ultérieur.

79 L'anonymisation correcte d'un ensemble de données implique bien plus que la simple suppression d'identifiants évidents comme le nom.[39] En ce qui concerne les empreintes digitales, il convient de noter que, par définition, elles feront toujours référence à une personne identifiable. L'utilisation de données d'essai synthétiques permet d'éviter tous ces problèmes.

80 Le CEPD souhaite également attirer l'attention sur le fait que le groupe de travail «Article 29» a souligné, dans son avis sur les techniques d'anonymisation[40], que, si la création d'un ensemble de données véritablement anonyme n'est pas en soi une proposition simple, même un ensemble de données anonyme peut être combiné avec un autre ensemble de données de telle manière qu'une ou plusieurs personnes puissent être identifiées.

81 En outre, le processus consistant à rendre anonymes les données de production implique que les données réelles doivent être copiées et traitées par l'agence eu-LISA dans un environnement technique distinct de l'infrastructure sécurisée du VIS, ce qui pose des risques spécifiques pour la sécurité et le respect de la vie privée et exige de définir un processus spécifique d'évaluation des risques en matière de sécurité permettant de traiter ces risques.

82 En outre, le CEPD rappelle que les données dactyloscopiques (ainsi que les images faciales) sont considérées comme des données biométriques, qui sont par nature très sensibles. À la différence des autres données à caractère personnel, les données biométriques ne sont ni communiquées par un tiers, ni choisies par la personne; elles sont immanentes à l'organisme lui-même et se réfèrent de façon distinctive et définitive à une personne. Par conséquent, les données biométriques se rapportent toujours à une personne identifiable, d'où l'impossibilité de rendre les données biométriques anonymes.

83 Dans ce contexte, le règlement 2018/1725 s'appliquerait pleinement au traitement des données biométriques à des fins d'essai. En conséquence, l'agence eu-LISA agirait en tant que responsable du traitement au sens de l'article 3, paragraphe 8, du règlement 2018/1725, et devrait mettre en œuvre des mesures techniques et organisationnelles appropriées pour garantir un traitement sécurisé. Cela imposerait à l'agence eu-LISA l'obligation d'établir un environnement d'essai sécurisé distinct de la production.

84 Le CEPD a toujours recommandé d'éviter autant que possible, conformément aux meilleures pratiques généralement acceptées en matière de sécurité de l'information[41], l'utilisation de données de production à des fins d'essai en raison des risques supplémentaires qu'elle présente. Dans la mesure du possible, d'autres moyens, tels que des données d'essais artificielles, devraient être utilisés à la place, même si cela peut nécessiter des ressources supplémentaires.

85 Dans les cas où il est absolument nécessaire d'utiliser des données de production, même après les avoir rendues anonymes (p. ex. à des fins spécifiques de validation des systèmes), le CEPD recommande que l'agence eu-LISA réalise et documente une évaluation spécifique des risques centrée sur cette utilisation concrète des données de production. Cela permettrait à la direction de l'agence eu-LISA de prendre une décision éclairée sur ces risques, en tenant compte d'autres facteurs tels que les coûts en termes de ressources humaines, d'argent ou d'adéquation des essais.

86 Le CEPD a déjà souligné, dans son avis sur le premier paquet de réformes sur le régime d'asile européen commun[42], qu'il n'est pas convaincu que l'utilisation de données réelles soit nécessaire à des fins d'essai. En outre, l'ISO/CEI 27002:2013[43] met l'accent sur le fait que l'utilisation de données à caractère personnel réelles présente un risque pour la sécurité et devrait être totalement évitée.

87 **Pour les raisons susmentionnées, le CEPD recommande de supprimer le nouvel article 26, paragraphe 8 bis, du règlement 767/2008.**

3.9 Contrôle de la qualité des données

88 Le CEPD se félicite du nouvel article 29, paragraphe 2 bis, et du nouvel article 29 bis du règlement 767/2008, qui confèrent à l'agence eu-LISA un mandat clair pour aider les États membres à remplir leur obligation d'assurer la qualité des données dans le système et mettent l'accent sur l'obligation des États membres d'introduire des données exactes et complètes dans le système. Le CEPD estime que le rôle renforcé de l'agence eu-LISA peut contribuer à garantir une meilleure qualité des données dans le système, tout comme l'établissement d'obligations plus claires pour les États membres. S'assurer que les données à caractère personnel contenues dans le système sont correctes peut permettre d'éviter de prendre des décisions erronées. Naturellement, cela est sans préjudice du principe de minimisation des données, selon lequel seules les données nécessaires à la finalité poursuivie doivent être traitées.[44]

3.10 Surveillance du VIS

89 Le règlement 767/2008 répartit la responsabilité du contrôle entre les autorités de contrôle nationales (ci-après les «autorités de protection des données») et le CEPD. Si les autorités de protection des données sont chargées de contrôler la licéité du traitement des données à caractère personnel par les États membres (article 41 du règlement 767/2008), le CEPD est chargé, quant à lui, de vérifier que le traitement des données à caractère personnel par l'agence eu-LISA est conforme au règlement (article 42 du règlement 767/2008).

90 Afin d'assurer un contrôle coordonné du VIS et des systèmes nationaux, l'article 43 du règlement 767/2008 prévoit que les autorités de protection des données et le CEPD coopèrent activement dans le cadre de leurs responsabilités en échangeant les informations utiles, en s'assistant mutuellement pour mener les audits et inspections, en examinant les difficultés d'interprétation ou d'application du règlement 767/2008, en formulant des propositions harmonisées en vue de trouver des solutions communes aux éventuels problèmes, en assurant la sensibilisation aux droits en matière de protection des données et en étudiant les problèmes pouvant se poser dans l'exercice des droits de la personne concernée. Les autorités de protection des données et le CEPD se réunissent à cet effet au moins deux fois par an, le coût et l'organisation de ces réunions étant à la charge du CEPD.

91 Le CEPD note que les modifications introduites par la proposition à l'article 43, paragraphe 1, du règlement 767/2008 prêtent à confusion. En effet, si l'article 43, paragraphe 1, prévoit un nouveau modèle de coopération inspiré du règlement Europol[45], le paragraphe 2 renvoie au modèle envisagé à l'article 62 du règlement (UE) 2018/1725, qui remplace le règlement (CE) 45/2001. Le CEPD rappelle que ces deux modèles diffèrent sensiblement. En outre, il constate que le nouvel article 43, paragraphe 1, du règlement 767/2008 fait référence de manière confuse aux canaux de communication des éléments d'interopérabilité et non au système d'information sur les visas.

92 Dans son avis sur la proposition de règlement révisé 45/2001[46], le CEPD s'est vivement félicité de l'approche d'un modèle unique et cohérent de contrôle coordonné des systèmes d'information à grande échelle de l'UE, qui contribuera à l'exhaustivité, à l'efficacité et à la cohérence du contrôle de la protection des données. Cela garantira également la mise

en place d'un environnement solide pour la poursuite du développement dans les années à venir. Le CEPD estime que l'objectif du règlement (UE) 2018/1725 est d'utiliser le modèle prévu en son article 62 pour contrôler tant les futurs systèmes que les systèmes existants. En particulier, le considérant 78 du règlement (UE) 2018/1725 dispose que «[l]e cas échéant, la Commission devrait donc soumettre des propositions législatives visant à amender les actes législatifs de l'Union prévoyant un modèle de contrôle coordonné, afin de les aligner sur le modèle de contrôle coordonné prévu par le présent règlement». **Le CEPD recommande donc que l'article 43 du règlement 767/2008 se réfère simplement à l'article 62 du règlement (UE) 2018/1725 en se contentant d'indiquer que: «Les autorités de contrôle nationales et le contrôleur européen de la protection des données, agissant chacun dans le cadre de leurs compétences respectives, coopèrent activement dans le cadre de leurs responsabilités et assurent une surveillance coordonnée du VIS et des systèmes nationaux conformément à l'article 62 du règlement (UE) 2018/1725».**

4 Conclusions

93 Le CEPD souligne que les données biométriques telles que les empreintes digitales sont très sensibles. Leur collecte et leur utilisation doivent être soumises à une analyse de stricte nécessité avant de décider de les enregistrer dans une base de données dans laquelle les données à caractère personnel d'un grand nombre de personnes seront traitées. Cette analyse est d'autant plus importante lorsqu'elle concerne des empreintes digitales d'enfants, qui sont des membres particulièrement vulnérables de la société et méritent donc une protection particulière.

94 Le CEPD reconnaît qu'il est de la plus haute importance de renforcer la prévention des violations des droits de l'enfant, telles que la traite des êtres humains, et la lutte contre celles-ci. Néanmoins, il constate qu'il reste difficile de savoir si et dans quelle mesure la traite d'enfants est causée ou amplifiée par les erreurs d'identification ou la non-identification des enfants entrant sur le territoire de l'UE avec un visa.

95 Si d'autres éléments venaient à être fournis à l'appui de cette affirmation, le CEPD rappelle l'importance de veiller à ce que les empreintes digitales des enfants ne soient utilisées que lorsque cela est dans l'intérêt supérieur de l'enfant. Il recommande donc d'introduire dans la proposition une disposition spécifique sur les empreintes digitales des enfants afin de limiter leur traitement aux fins de:

- la vérification de l'identité de l'enfant durant la procédure de demande de visa et aux frontières extérieures et,
- la contribution à la prévention des violations des droits de l'enfant et à la lutte contre celles-ci dans un cas concret uniquement.

En ce qui concerne en particulier l'accès des autorités répressives, le CEPD recommande de s'assurer que:

- cet accès est nécessaire aux fins de la prévention ou de la détection d'un cas de traite d'enfants ou des enquêtes sur celui-ci,
- l'accès est nécessaire dans un cas concret,
- une recherche préalable dans les bases de données nationales pertinentes et dans les systèmes spécifiques au niveau de l'Union n'a donné aucun résultat,
- il existe des motifs raisonnables de considérer que la consultation du VIS contribuera de manière substantielle à la prévention ou à la détection du cas de traite d'enfants en question ou aux enquêtes sur celui-ci, et,

- l'identification est dans l'intérêt supérieur de l'enfant.

96 Le CEPD relève qu'en enregistrant dans le VIS des données relatives à tous les titulaires de visas de long séjour et de titres de séjour, la proposition inclurait la seule catégorie de ressortissants de pays tiers qui n'est actuellement couverte par aucun des systèmes à grande échelle de l'UE dans les domaines de la liberté, de la sécurité et de la justice. Dans le contexte de la proposition d'interopérabilité des systèmes à grande échelle de l'UE, la proposition contribuerait à la création d'un réseau européen centralisé donnant accès à une quantité considérable d'informations sur tous les ressortissants de pays tiers qui ont franchi ou envisagent de franchir les frontières de l'UE (c'est-à-dire des millions de personnes). Compte tenu du double objectif de la centralisation des données relatives aux visas de long séjour et aux titres de séjour: a) vérifier l'authenticité d'un document et la relation légitime avec son titulaire et b) faciliter l'échange d'informations sur les personnes dont la demande de visa a été refusée pour des raisons de sécurité, le CEPD estime que la possibilité d'harmoniser les documents sécurisés relatifs aux visas de long séjour et aux titres de séjour devrait être examinée plus avant et que les informations stockées dans le VIS devraient être limitées aux personnes physiques:
- dont les données correspondent à des données stockées dans un autre système ou pour lesquelles des doutes subsistent quant à leur identité,
- dont la demande de visa de long séjour ou de titre de séjour a été refusée parce qu'elles ont été considérées comme constituant une menace pour l'ordre public, la sécurité intérieure ou la santé publique ou parce qu'elles ont présenté des documents qui ont été acquis par des manœuvres frauduleuses, falsifiés ou manipulés.

97 En ce qui concerne la comparaison des données stockées dans le VIS avec les données figurant dans d'autres systèmes, le CEPD recommande d'inclure dans la proposition des garanties selon lesquelles seules les informations stockées dans l'ECRIS-TCN relatives à des infractions terroristes et autres infractions pénales graves seraient communiquées à l'autorité centrale. Une des possibilités pour cela serait que l'autorité centrale ne soit pas informée de la réponse positive, mais qu'une notification soit automatiquement adressée à l'autorité compétente de l'État membre qui a introduit les données à l'origine de la réponse positive. L'autorité compétente de l'État membre en informerait alors l'autorité centrale, le cas échéant. Alternativement, la possibilité de consulter le système ECRIS-TCN devrait être supprimée.

98 Le CEPD recommande également de préciser dans la proposition l'objectif de la comparaison des données du VIS avec les données d'Europol, ainsi que la procédure et les conditions applicables en ce qui concerne les résultats de cette comparaison. En outre, il estime que la proposition devrait être clarifiée en ce qui concerne les types d'alertes du SIS à prendre en compte dans la procédure de délivrance des visas, et recommande de veiller, dans la proposition, à ce que seuls les signalements qui font légalement partie du processus décisionnel en matière de délivrance des visas produisent une réponse positive accessible aux autorités chargées des visas.

99 Enfin, au-delà des observations générales et des questions clés recensées ci-dessus, le CEPD formule des recommandations supplémentaires concernant les aspects suivants des propositions:
- Catégories de données du VIS comparées aux données enregistrées dans d'autres systèmes,
- Catégories spécifiques de demandeurs de visas,
- Définition des autorités centrales,

- Utilisation des données du VIS aux fins de l'introduction dans le SIS de signalements concernant des personnes disparues,
- Vérifications en cas de réponse positive,
- Accès à des fins répressives,
- Statistiques,
- Utilisation de données anonymisées à des fins d'essai,
- Contrôle de la qualité des données,
- Supervision du VIS.

100 Le CEPD reste disponible pour apporter des conseils supplémentaires concernant la proposition, ainsi que tout acte délégué ou d'exécution adopté portant sur les règlements proposés qui serait susceptible d'avoir une incidence sur le traitement de données à caractère personnel.

Bruxelles, le

Giovanni BUTTARELLI

Remarques

[1] JO L 119 du 4.5.2016, p. 1.
[2] JO L 295 du 21.11.2018, p. 39.
[3] JO L 119 du 4.5.2016, p. 89.
[4] https://ec.europa.eu/home-affairs/what-is-new/news/news/2016/20160406_3_en
[5] C (2016) 3780 final, décision de la Commission du 17 juin 2016 instituant le groupe d'experts de haut niveau sur les systèmes d'information et l'interopérabilité.
[6] http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=32600&no=1.
[7] Ibidem, p. 19.
[8] https://ec.europa.eu/home-affairs/news/public-consultation-lowering-fingerprinting-age-children-visa-procedure-12-years-6-years_en.
[9] https://ec.europa.eu/home-affairs/content/consultation-extending-scope-visa-information-system-vis-include-data-long-stay-visas-and_en.
[10] Réponse du CEPD à la consultation publique de la Commission sur l'élargissement du champ d'application du système d'information sur les visas (VIS) pour y inclure des données concernant les visas de long séjour et les documents de séjour, disponible à l'adresse suivante: https://edps.europa.eu/sites/edp/files/publication/18-02-09_formal_comments_vis_consultation_long_stay_visas_residence_documents_en.pdf et observations formelles du CEPD en réponse à la consultation publique de la Commission sur l'abaissement de 12 à 6 ans de l'âge des enfants pour le relevé des empreintes digitales dans le cadre de la procédure de visa, disponible à l'adresse suivante: https://edps.europa.eu/sites/edp/files/publication/17-11-09_formal_comments_2017-0809_en.pdf.
[11] Avis de l'Agence des droits fondamentaux sur le système révisé d'information sur les visas et ses conséquences en matière de droits fondamentaux, 30 août 2018, disponible à l'adresse suivante: http://fra.europa.eu/en/opinion/2018/visa-system.
[12] «Fingerprint Recognition for Children», rapport technique du Centre commun de recherche, 2013, disponible à l'adresse http://publications.jrc.ec.europa.eu/repository/bitstream/JRC85145/fingerprint%20recognition%20for%20children%20final%20report%20%28pdf%29.pdf
[13] «Automated fingerprint recognition: from children to elderly ageing and age effects», rapport technique du Centre commun de recherche, 2018, disponible à l'adresse https://ec.europa.eu/jrc/en/publication/automatic-fingerprint-recognition-children-elderly-ageing-and-age-effects
[14] Considérant 8 de la proposition.
[15] 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*».
[16] 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 à 131.
[17] 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
[18] 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 à 88]
[19] Voir les considérants 38, 58, 65, 71, 75, l'article 6, paragraphe 1, point f), et les articles 8, 12, 40 et 57 du règlement général sur la protection des données.
[20] Analyse d'impact, p. 14.
[21] Analyse d'impact, annexe 8, p. 104
[22] Analyse d'impact, p. 14 et 105.

[23] Rapport de la Commission au Parlement européen et au Conseil sur les progrès réalisés dans la lutte contre la traite des êtres humains, SWD (2016) 159 final, p. 16.
[24] http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=32600&no=1.
[25] https://ec.europa.eu/home-affairs/sites/homeaffairs/files/docs/pages/201709_ibm_feasibility_study_final_report_en.pdf.
[26] https://edps.europa.eu/sites/edp/files/publication/18-02-09_formal_comments_vis_consultation_long_stay_visas_residence_documents_en.pdf.
[27] Voir l'analyse d'impact p. 17-18 et l'exposé des motifs p. 7-8.
[28] Analyse d'impact, p. 18,
[29] Analyse d'impact, p. 45 et 59.
[30] Analyse d'impact, p. 45
[31] Analyse d'impact, p. 19
[32] Exposé des motifs, p. 7.
[33] COM(2017) 794 final, proposition de règlement du Parlement européen et du Conseil portant établissement d'un cadre pour l'interopérabilité des systèmes d'information de l'UE (coopération policière et judiciaire, asile et migration).
[34] Voir annexe 10 de l'analyse d'impact, p. 119.
[35] Proposition de règlement du Parlement européen et du Conseil portant création d'un système centralisé permettant d'identifier les États membres détenant des informations relatives aux condamnations concernant des ressortissants de pays tiers et des apatrides, qui vise à compléter et à soutenir le système européen d'information sur les casiers judiciaires (système ECRIS-TCN), et modifiant le règlement (UE) no 1077/201, COM(2017) 0344 final.
[36] Décision 2008/633/JAI du Conseil du 23 juin 2008 concernant l'accès en consultation au système d'information sur les visas (VIS) par les autorités désignées des États membres et par Europol aux fins de la prévention et de la détection des infractions terroristes et des autres infractions pénales graves, ainsi qu'aux fins des enquêtes en la matière
[37] COM(2017) 793 final, proposition de règlement du Parlement européen et du Conseil portant établissement d'un cadre pour l'interopérabilité des systèmes d'information de l'UE (frontières et visas) et modifiant la décision 2004/512/CE du Conseil, le règlement (CE) nº 767/2008, la décision 2008/633/JAI du Conseil, le règlement (UE) 2016/399 et le règlement (UE) 2017/2226.
[38] https://edps.europa.eu/sites/edp/files/publication/2018-04-16_interoperability_opinion_en.pdf.
[39] Avis 05/2014 du groupe de travail «Article 29» sur les techniques d'anonymisation, WP216. Si ce document analyse les techniques d'anonymisation dans le cadre de l'ancienne directive 95/46 sur la protection des données, son raisonnement demeure valable pour le RGPD.
[40] Avis 05/2014 du groupe de travail «Article 29» sur les techniques d'anonymisation, WP216.
[41] ISO/IEC 27002:2013, section 14.3.
[42] https://edps.europa.eu/sites/edp/files/publication/16-09-21_ceas_opinion_en.pdf.
[43] Cf. section 14.3 de l'ISO/CEI 27002:2013, Lignes directrices en matière de normes organisationnelles relatives à la sécurité de l'information et de bonnes pratiques de gestion de la sécurité de l'information, y compris la sélection, la mise en œuvre et la gestion des contrôles en tenant compte de l'environnement ou des environnements de l'organisation en matière de risques pour la sécurité de l'information.
[44] Article 5, paragraphe 1, point c), 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 (le règlement général sur la protection des données), JOCE L 119/1 du 4 mai 2016
[45] Règlement (UE) 2016/794 du Parlement européen et du Conseil du 11 mai 2016 relatif à l'Agence de l'Union européenne pour la coopération des services répressifs (Europol) et remplaçant et abrogeant les décisions du Conseil 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI et 2009/968/JAI, J.O.C.E.,L 135/53 du 24.05.2016.
[46] Avis 5/2017 «Renforcement des règles de protection des données pour les institutions et organes de l'UE, avis du CEPD sur la proposition de règlement relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) nº 45/2001 et la décision nº 1247/2002/CE, 15 mars 2017, disponible à l'adresse https://edps.europa.eu/sites/edp/files/publication/17-03-15_regulation_45-2001_en.pdf.