



EUROPEAN DATA PROTECTION SUPERVISOR

Avis 06/2016

**Avis du CEPD sur le
deuxième train de
mesures «Frontières
intelligentes» de
l'Union européenne**

*Recommandations sur la proposition révisée
visant à créer un système d'entrée/sortie*



21 septembre 2016

Le contrôleur européen de la protection des données (CEPD) est une institution indépendante de l'UE chargée, en vertu de l'article 41, paragraphe 2, du règlement n° 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 n° 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 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 n° 9 de la stratégie du CEPD: «Faciliter l'élaboration responsable et éclairée de politiques». Le CEPD considère que la conformité aux exigences en matière de protection des données sera un élément clé du succès du nouveau train de mesures «Frontières intelligentes» et de l'échange d'informations sur les entrées et les sorties des ressortissants de pays tiers au travers du système d'entrée/sortie.

Résumé

La création d'un système d'entrée/sortie (EES) qui enregistrera les entrées et les sorties des ressortissants de pays tiers sur le territoire de l'Union européenne est envisagée depuis longtemps par le législateur de l'Union européenne (UE). La Commission a adopté trois propositions dans le cadre du premier train de mesures «Frontières intelligentes» en 2013; les colégislateurs ayant exprimé leurs vives préoccupations, aucun consensus n'a été atteint sur ce train de mesures. La Commission a alors lancé un exercice de validation de principe en réponse à ces préoccupations; elle a publié cette année un deuxième train de mesures «Frontières intelligentes», désormais composé de deux propositions révisées.

Après avoir analysé avec soin ces propositions, le CEPD formule des recommandations en vue d'apporter son assistance au législateur et d'assurer la pleine conformité du cadre juridique applicable à l'EES avec la législation de l'UE en matière de respect de la vie privée et de protection des données, et en particulier les articles 7 et 8 de la Charte des droits fondamentaux de l'UE.

Le CEPD reconnaît la nécessité de systèmes d'information cohérents et efficaces pour les frontières et la sécurité. Ces propositions sont présentées à un moment crucial, alors que l'UE est confrontée à de graves difficultés dans ce domaine. Le CEPD souligne néanmoins l'ampleur du traitement des données à caractère personnel prévu par l'EES et son caractère potentiellement intrusif. Il estime que ce traitement doit dès lors être appréhendé à la lumière des articles 7 et 8 de la Charte. La nécessité et la proportionnalité de l'EES doivent être appréciées aussi bien de manière globale, compte tenu des systèmes informatiques à grande échelle qui existent déjà au sein de l'UE, que de manière spécifique, dans le cas particulier des ressortissants de pays tiers qui se rendent légalement dans l'UE. Le CEPD observe que les données de l'EES seront traitées à deux fins différentes: à des fins de gestion des frontières et d'allègement des formalités, d'une part, et à des fins répressives, d'autre part. Le CEPD recommande vivement de différencier clairement ces objectifs tout au long de la proposition de 2016 relative à l'EES étant donné que ces finalités ont des conséquences différentes sur les droits au respect de la vie privée et à la protection des données.

S'il se réjouit de l'attention accordée aux préoccupations qui ont été exprimées précédemment au sujet du respect de la vie privée et de la protection des données, ainsi que des améliorations apportées aux propositions remaniées, le CEPD nourrit de vives appréhensions à l'égard de plusieurs aspects de la proposition relative à l'EES. Ces aspects devraient être mieux justifiés, voire reconsidérés par le législateur. Sont notamment visés ici:

- la durée de conservation des données de l'EES, fixée à cinq ans. Le CEPD fait remarquer que la nécessité de conserver pendant cinq ans les données des personnes ayant dépassé la durée de séjour autorisée devrait être mieux démontrée et qu'une durée de conservation de cinq ans pour toutes les données à caractère personnel enregistrées dans l'EES semble disproportionnée;
- la capture de l'image faciale des voyageurs soumis à l'obligation de visa, dont l'image faciale est déjà enregistrée dans le système d'information sur les visas (VIS);
- la nécessité d'accorder aux autorités répressives l'accès aux données de l'EES, qui n'est pas suffisamment étayée par des preuves convaincantes;

- le fait que la personne concernée doit d'abord fournir ses empreintes digitales lorsqu'elle exerce ses droits d'accès, de rectification ou d'effacement de ses données à caractère personnel, ce qui pourrait constituer un obstacle de taille à l'exercice effectif de ces droits.

Le présent avis contient également des recommandations supplémentaires en matière de protection des données et de respect de la vie privée, qui devraient être prises en considération dans le processus législatif, notamment en ce qui concerne la sécurité du système.

TABLE DES MATIÈRES

1. INTRODUCTION ET CONTEXTE	5
2. OBJECTIF DES PROPOSITIONS	6
3. ANALYSE DES PROPOSITIONS	7
I. INCIDENCES DE L'EES SUR LE RESPECT DE LA VIE PRIVÉE ET LA PROTECTION DES DONNÉES.....	7
II. OBJECTIFS DE L'EES	9
III. GESTION DES FRONTIÈRES ET ALLÈGEMENT DES FORMALITÉS.....	9
<i>III.1 Conservation des données pendant cinq ans</i>	10
<i>III.2 Données collectées</i>	12
<i>III.3 Recommandations supplémentaires sur les propositions</i>	13
IV. ACCÈS DES AUTORITÉS RÉPRESSIVES	21
<i>IV.1 Répression en tant qu'objectif secondaire</i>	21
<i>IV.2 Nécessité de l'accès des autorités répressives</i>	21
<i>IV.3 Conditions d'accès et sauvegardes</i>	22
4. CONCLUSION	23
NOTES	Error! Bookmark not defined.

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 la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données¹,

vu le règlement (CE) n° 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 données², et notamment son article 28, paragraphe 2, son article 41, paragraphe 2, et son article 46, point d),

vu la décision-cadre 2008/977/JAI du Conseil du 27 novembre 2008 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale³,

A ADOPTÉ L'AVIS SUIVANT:

1. INTRODUCTION ET CONTEXTE

1. La Commission a d'abord annoncé en 2008 son intention de créer un système européen d'entrée/sortie afin de contrôler les entrées et les sorties des ressortissants de pays tiers sur le territoire de l'Union européenne⁴. À l'époque, le CEPD a, dans un premier temps, fait part de ses observations préliminaires⁵ sur l'idée, puis mis en évidence certains aspects spécifiques dans son avis de juillet 2011⁶. La Commission a précisé ses vues dans une communication⁷ d'octobre 2011 intitulée «Frontières intelligentes: options et pistes envisageables», que le groupe de travail «Article 29» a commentée⁸. Le CEPD a également participé à une table ronde commune réunissant diverses parties prenantes⁹.

2. En février 2013, la Commission a adopté trois propositions dans le cadre du premier train de mesures «Frontières intelligentes»: une proposition de création d'un système d'entrée/sortie¹⁰ (ci-après la «proposition de 2013 relative à l'EES»), une proposition de création d'un programme d'enregistrement des voyageurs¹¹ (ci-après la «proposition de 2013 relative au RTP») et une proposition modifiant le code frontières Schengen¹² en fonction de ces changements. Le train de mesures a immédiatement essuyé les critiques des deux colégislateurs en raison de problèmes techniques, opérationnels et de coûts ainsi que d'importants problèmes liés à la protection des données. La même année, le CEPD a émis ses premières recommandations concrètes sur les trois propositions sous la forme d'un avis¹³. L'avis que le groupe de travail «Article 29» a également rendu¹⁴, et auquel le CEPD a contribué, remet en question la nécessité du système d'entrée/sortie en tant que tel.

3. En réponse à ces préoccupations, la Commission a annoncé, début 2014, le lancement d'un exercice de validation de principe en deux étapes: d'abord, une étude technique¹⁵ et une étude de coût¹⁶ devant déterminer les options et les solutions les plus adéquates pour mettre en œuvre les frontières intelligentes, suivies, au cours de l'année 2015, d'un projet pilote¹⁷ dirigé par l'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 (ci-après l'«eu-LISA») afin de mettre à l'épreuve les différentes options recensées. En parallèle, la Commission a lancé en juillet 2015 une consultation publique de trois mois¹⁸ afin de recueillir les positions et les opinions de citoyens et d'organisations, consultation à laquelle le CEPD a également participé¹⁹.

4. Le 6 avril 2016, la Commission a publié un deuxième train de mesures «Frontières intelligentes»²⁰. Cette fois-ci, un seul système est proposé: le système d'entrée/sortie (ci-après l'«EES»). La Commission a décidé de revoir sa proposition de 2013 relative à l'EES et la proposition de 2013 modifiant le code frontières Schengen et de retirer sa proposition de 2013 relative au RTP. Aujourd'hui, le train de mesures «Frontières intelligentes» se compose des documents suivants:

- une communication intitulée «Des systèmes d'information plus robustes et plus intelligents au service des frontières et de la sécurité»²¹;
- une proposition de règlement du Parlement européen et du Conseil portant création d'un système d'entrée/sortie pour enregistrer les données relatives aux entrées et aux sorties des ressortissants de pays tiers qui franchissent les frontières extérieures des États membres de l'Union européenne ainsi que les données relatives aux refus d'entrée les concernant, portant détermination des conditions d'accès à l'EES à des fins répressives et portant modification du règlement (CE) n° 767/2008 et du règlement (UE) n° 1077/2011²² (ci-après la «proposition de 2016 relative à l'EES»); et
- une proposition de règlement du Parlement européen et du Conseil modifiant le règlement (UE) 2016/399²³ en ce qui concerne l'utilisation du système d'entrée/sortie²⁴ (ci-après la «proposition de 2016 modifiant le code frontières Schengen»).

5. Une analyse d'impact détaillée²⁵ accompagne en outre les deux propositions.

6. Le train de mesures «Frontières intelligentes» a pris un nouvel élan à la suite de la crise actuelle des migrations et des récents attentats terroristes en Europe. Les présidences néerlandaise et slovaque ont annoncé leur intention de travailler d'arrache-pied sur le train de mesures afin d'atteindre un accord politique d'ici la fin 2016²⁶.

7. Le CEPD se félicite d'avoir été consulté de manière informelle par la Commission avant l'adoption des nouvelles propositions. Il a également salué la bonne coopération²⁷ entre la DG HOME et ses services pendant tout le processus de révision du premier train de mesures «Frontières intelligentes».

2. OBJECTIF DES PROPOSITIONS

8. La proposition relative à l'EES est présentée à un moment crucial où l'UE est confrontée à de graves difficultés sur le front du contrôle de ses frontières et de sa sécurité. Elle complètera les systèmes informatiques à grande échelle concernant les demandeurs d'asile et les demandeurs de visa, dont l'UE dispose actuellement. Dans ce contexte, la **proposition de 2016 relative à l'EES** vise à améliorer la gestion des frontières extérieures de l'UE et à réduire la migration irrégulière en s'attaquant au phénomène du «dépassement de la durée de séjour autorisée»²⁸. Actuellement, la seule méthode dont disposent les gardes-frontières et les services d'immigration pour calculer la durée de séjour des ressortissants de pays tiers et vérifier s'ils ne

l'ont pas dépassée consiste à examiner les cachets apposés dans leurs documents de voyage. À cette fin, la proposition s'appliquera aux ressortissants de pays tiers entrant légalement dans l'UE. Le CEPD comprend que les circonstances dans lesquelles les ressortissants de pays tiers entrent dans l'UE détermineront si leurs données seront enregistrées dans l'EES ou la base de données Eurodac: ceux qui entrent légalement à un point de passage frontalier officiel et sont admis pour un court séjour (c'est-à-dire ne dépassant pas 90 jours sur une période de 180 jours) dans la zone Schengen verront leurs données enregistrées dans l'EES, tandis que les ressortissants de pays tiers qui demandent l'asile ou entrent illégalement dans l'UE, ou qui sont entrés illégalement et sont repérés dans l'UE, verront leurs données enregistrées dans Eurodac. Le système EES collectera leurs données à caractère personnel, y compris leurs données biométriques, et enregistrera la date et le lieu de leurs entrées et de leurs sorties. Le système enregistrera également les refus d'entrée.

9. En outre, l'EES proposé vise à contribuer à la prévention et à la détection des infractions terroristes ou d'autres infractions pénales graves et aux enquêtes en la matière et à servir d'outil d'identification et de renseignement.

10. Par comparaison avec la proposition de 2013 relative à l'EES, les principaux changements apportés par la proposition de 2016 prévoient un allongement à cinq ans de la durée de conservation des données pour *l'ensemble* des données de l'EES, l'accès des autorités répressives dès la mise en service du système, la spécification des éléments d'identification biométriques utilisés et l'interopérabilité avec le système d'information sur les visas (ci-après le «VIS») par le biais d'un canal de communication direct entre ces deux bases de données.

11. La **proposition de 2016 modifiant le code frontières Schengen** a pour objectif d'introduire dans le code frontières Schengen les modifications techniques découlant de la proposition de 2016 relative à l'EES, en particulier l'enregistrement dans l'EES des refus d'entrée des ressortissants de pays tiers, les procédures de secours en cas d'impossibilité d'utiliser l'EES et l'interopérabilité entre l'EES et le VIS. La proposition de 2016 innove aussi en introduisant la possibilité pour les États membres de créer, sur une base volontaire, des programmes nationaux prévoyant des mesures d'allègement des formalités.

3. ANALYSE DES PROPOSITIONS

I. Incidences de l'EES sur le respect de la vie privée et la protection des données

12. Le CEPD reconnaît que, face aux défis migratoires importants auxquels elle est confrontée, l'UE doit prendre des mesures. Ces mesures doivent toutefois respecter pleinement le cadre juridique de l'UE. Le système d'entrée/sortie proposé concernera les ressortissants de pays tiers qui se rendent légalement dans l'UE. Le législateur doit notamment tenir compte de leurs droits fondamentaux au respect de la vie privée et à la protection des données, droits consacrés par les articles 7 et 8 de la Charte des droits fondamentaux de l'UE (ci-après la «Charte»), qui s'appliquent tous deux, parce que l'EES impliquera d'importantes activités de collecte, de conservation et d'utilisation de données à caractère personnel les concernant.

13. En principe, un tel traitement est compatible avec les droits fondamentaux protégés par la Charte s'il respecte les conditions fixées à son article 52, paragraphe 1; les limitations doivent:

- être prévues par la loi;
- respecter le contenu essentiel du droit;
- répondre effectivement à des objectifs d'intérêt général reconnus par l'Union; et
- si elles s'avèrent nécessaires, respecter le principe de proportionnalité.

14. La nécessité et la proportionnalité de ce système doivent être appréciées aussi bien de manière globale, compte tenu des systèmes informatiques à grande échelle qui existent déjà au sein de l'UE, que de manière spécifique, dans le cas particulier des ressortissants de pays tiers qui se rendent légalement dans l'UE. **Le CEPD souhaite tout d'abord souligner que, sous l'angle des articles 7 et 8 de la Charte, le traitement des données à caractère personnel entraîné par le système proposé d'entrée/sortie est important et intrusif**, compte tenu du nombre de personnes concernées par ce système, du type d'informations traitées, des moyens utilisés à cet effet et des différentes finalités poursuivies, comme expliqué ci-dessous.

15. Premièrement, l'EES couvrira *toutes* les entrées et sorties des ressortissants de pays tiers²⁹ qui pénètrent ou quittent le territoire de l'UE. Il concernera donc des millions d'individus chaque année. D'après la Commission elle-même, le nombre total de franchissements réguliers des frontières devrait passer à 887 millions en 2025, dont environ un tiers devraient être le fait de ressortissants de pays tiers³⁰. Le volume même des données à caractère personnel qui seraient traitées dans ce système fera de l'EES l'une des plus vastes bases de données européennes. À cet égard, le CEPD se réjouit de ce que la proposition de 2016 relative à l'EES vise à réduire le volume de données à caractère personnel traitées, conformément au principe de minimisation des données: 26 éléments de données par personne tout au plus devraient être enregistrés dans l'EES³¹ (au lieu des 36 prévus dans la proposition de 2013³²).

16. Deuxièmement, l'EES devrait donner lieu au relevé des empreintes digitales et à la capture de l'image faciale des ressortissants de pays tiers lors de leur entrée, ce qui augmentera considérablement le volume de données biométriques que l'UE conserve déjà dans les bases de données existantes telles qu'Eurodac, le système d'information Schengen (ci-après le «SIS») et le VIS. Les données biométriques revêtent un caractère particulier et sont considérées comme plus sensibles dans la mesure où elles sont reliées sans équivoque à un individu unique, dont le corps est ainsi rendu «lisible»³³. Le CEPD prend acte de la nécessité d'utiliser des données biométriques pour s'assurer avec un plus grand degré de certitude de l'identité des ressortissants de pays tiers qui franchissent les frontières de l'UE. Toutefois, de par la nature même des données biométriques, leur traitement implique une ingérence plus grave et nécessite par conséquent un niveau plus élevé de protection des données.

17. Troisièmement, le CEPD note également qu'à la suite du projet pilote dirigé par l'eu-LISA, la proposition de 2016 relative à l'EES prévoit une diminution du nombre de données biométriques devant être stockées. La proposition de 2016 relative à l'EES, s'appuyant sur les conclusions de ce projet pilote, propose l'enregistrement de quatre empreintes digitales et de l'image faciale, qu'elle considère suffisants aux fins de la vérification et de l'identification (alors que la proposition de 2013 prévoyait les dix empreintes digitales, mais pas l'image faciale). Le CEPD fait néanmoins observer qu'un nombre plus faible de données biométriques n'équivaut pas nécessairement à une ingérence moins importante, étant donné que la proposition prévoit la collecte d'une combinaison de deux types de données biométriques, ce qui permet d'utiliser

à la fois un logiciel de comparaison des empreintes digitales et un logiciel de reconnaissance faciale pour traiter et passer au crible rapidement les données stockées.

18. Enfin, les incidences de l'EES seront doubles puisque les données de l'EES seront traitées aussi bien à des fins de gestion des frontières et d'allègement des formalités qu'à des fins répressives

II. Objectifs de l'EES

19. Dans l'exposé des motifs de la proposition de 2016 relative à l'EES³⁴, la Commission expose les trois objectifs généraux poursuivis par l'EES:

- 1) réduire les temps d'attente lors des vérifications aux frontières et améliorer la qualité de ces vérifications pour les ressortissants de pays tiers («allègement des formalités»);
- 2) garantir l'identification systématique et fiable des personnes ayant dépassé la durée de séjour autorisée («gestion des frontières»);
- 3) soutenir la lutte contre le terrorisme et les formes graves de criminalité et contribuer au final à un niveau plus élevé de sécurité intérieure («répression»).

20. Le CEPD observe que les objectifs 1) et 2) sont souvent présentés comme les «*deux objectifs principaux de l'EES*»³⁵ dans l'analyse d'impact accompagnant la proposition de 2016 relative à l'EES, tandis que l'accès aux données de l'EES à des fins répressives est qualifié d'«*objectif secondaire*» du système³⁶. Cette différence n'apparaît cependant pas dans le texte de la proposition de 2016 relative à l'EES: ni dans ses articles ni dans ses considérants. Au contraire, la proposition de 2016 relative à l'EES met ces trois objectifs généraux sur le même pied à l'article 1^{er}, qui en définit l'objet, et à l'article 5, qui énumère les douze finalités spécifiques de la collecte et de la conservation des données de l'EES et de l'accès à celles-ci. **Le CEPD recommande vivement de différencier clairement les objectifs tout au long de la proposition de 2016 relative à l'EES.**

21. Le CEPD comprend que le système européen d'entrée/sortie sera créé essentiellement à des fins de gestion des frontières et d'allègement des formalités et qu'un accès à ses données sera éventuellement accordé à des fins répressives. Par conséquent, le présent avis analysera successivement la création de l'EES à des fins de gestion des frontières et d'allègement des formalités, en tant qu'objectifs principaux du système, et l'accès des autorités répressives à cet outil de contrôle des frontières, qui en est l'objectif secondaire, aux sections III et IV, respectivement.

III. Gestion des frontières et allègement des formalités

22. Le CEPD reconnaît que l'UE est actuellement confrontée à des défis migratoires de plus en plus pressants. Il observe que la proposition de 2016 relative à l'EES s'inscrit dans une politique plus globale de l'UE en matière de contrôle des frontières et de gestion des migrations. Il est nécessaire d'évaluer les incidences réelles de l'EES sur cette politique en combinaison avec l'ensemble des systèmes informatiques à grande échelle déjà disponibles dans ce domaine, tels qu'Eurodac, le SIS et le VIS, dont le développement se poursuivra également dans un proche avenir.

23. Le CEPD se réjouit de ce que la Commission a prêté attention aux préoccupations qui ont été exprimées précédemment au sujet du respect de la vie privée et de la protection des données dans le contexte de l'EES et qu'elle a pris le temps de rassembler et de produire une documentation plus fournie à l'appui de la création de ce système et des choix politiques effectués dans le deuxième train de mesures «Frontières intelligentes», au travers de divers exercices tels que le projet pilote dirigé par l'eu-LISA, l'étude de la FRA, la consultation publique et l'analyse d'impact détaillée accompagnant les propositions de 2016. Bien que les preuves ne soient pas toujours pleinement détaillées³⁷, il semble y avoir suffisamment d'éléments justifiant la création de l'EES à des fins de gestion des frontières et d'allègement des formalités.

24. Étant donné les incidences majeures que l'EES proposé aurait sur le respect de la vie privée et la protection des données³⁸, il importe que le futur règlement relatif à l'EES respecte pleinement l'exigence de proportionnalité énoncée à l'article 52, paragraphe 1, de la Charte au cas où il serait soumis au contrôle de la Cour de justice de l'Union européenne (ci-après la «CJUE»). À supposer qu'il soit nécessaire, il conviendrait de mieux démontrer que les avantages de la création d'un système d'entrée/sortie l'emportent sur l'intrusion dans la vie privée de l'ensemble des ressortissants de pays tiers. La CJUE a fourni des orientations dans l'arrêt Digital Rights Ireland qu'elle a rendu dans les affaires jointes C-293/12 et C-594/12³⁹ (ci-après l'«arrêt DRI»). Le CEPD a pris note du critère de proportionnalité appliqué par la Commission dans l'analyse d'impact⁴⁰.

25. Le CEPD souhaite commenter deux aspects majeurs de la proposition de 2016 relative à l'EES qui sont directement liés à la proportionnalité d'un tel système à des fins de gestion des frontières et d'allègement des formalités (sections III.1 et III.2). Le CEPD émet des recommandations supplémentaires concernant certains aspects spécifiques de la proposition de 2016 relative à l'EES (section III.3) et invite la Commission à les prendre en considération.

III.1 Conservation des données pendant cinq ans

26. Les normes en matière de protection des données en vigueur dans l'UE imposent de choisir une durée de conservation des données qui soit la plus courte possible. Le considérant 25 de la proposition de 2016 relative à l'EES indique à juste titre que «[l]es données à caractère personnel stockées dans l'EES ne devraient pas être conservées plus longtemps que ce qui est nécessaire pour les besoins de l'EES». La proposition prévoit désormais⁴¹ un allongement à cinq ans de la durée de conservation de l'ensemble des fiches d'entrée/sortie de tous les ressortissants de pays tiers à compter de la date de la fiche de sortie (article 31, paragraphe 1) et une durée de conservation de cinq ans et un jour pour les dossiers individuels⁴² «à compter de la dernière sortie enregistrée, si aucune nouvelle entrée n'est enregistrée dans les cinq ans suivant ce dernier enregistrement de sortie» (article 31, paragraphe 2). En outre, la proposition de 2016 relative à l'EES prévoit à l'article 31, paragraphe 4, une exception mineure pour les fiches d'entrée/sortie des ressortissants de pays tiers membres de la famille de citoyens de l'Union, qui seront conservées pendant un an, tandis que leurs dossiers individuels devraient être conservés pendant la même durée de cinq ans.

27. Le CEPD fait tout d'abord remarquer qu'étant donné la date de début de la durée de conservation des dossiers individuels fixée à l'article 31, paragraphe 2, les ressortissants de pays tiers qui se rendent au moins une fois tous les cinq ans dans l'UE verront leurs données à caractère personnel, y compris leur image faciale et quatre de leurs empreintes digitales,

conservées dans l'EES non pas pour une durée de cinq ans, mais de manière permanente. En effet, s'ils se rendent à nouveau dans l'UE dans un délai de moins de cinq ans, leur dossier personnel ne sera pas supprimé mais conservé pour une nouvelle période de cinq ans à compter de leur sortie du territoire de l'UE.

28. Le CEPD souhaite attirer l'attention du législateur sur la nécessité de justifier pleinement la proportionnalité d'une durée de conservation de cinq ans pour les données à caractère personnel, en vue de l'objectif consistant à réduire les temps d'attente lors des vérifications aux frontières et à améliorer la qualité de ces vérifications pour les ressortissants de pays tiers et en vue de l'objectif visant à identifier les personnes ayant dépassé la durée de séjour autorisée.

29. La proposition de 2016 relative à l'EES devrait en effet respecter les exigences fixées par la Cour de justice dans l'arrêt DRI. À cet égard, la CJUE a jugé que *«la détermination de la durée de conservation doit être fondée sur des critères objectifs afin de garantir que celle-ci est limitée au strict nécessaire»*⁴³. Le CEPD prend note du fait qu'une durée de cinq ans correspondrait à la durée de validité moyenne des passeports délivrés par les pays tiers, ainsi qu'à la durée de validité maximale des visas à entrées multiples, comme indiqué dans l'analyse d'impact⁴⁴ accompagnant les propositions. Toutefois, le fait que la durée de conservation choisie s'aligne sur celle d'autres systèmes existants tels que le VIS ne rend pas forcément ce choix proportionné.

30. La proposition prévoit aussi l'effacement anticipé du dossier individuel et des fiches d'entrée/sortie avant la fin de la durée choisie lorsque la personne concernée a acquis la nationalité ou un titre de séjour d'un État membre de l'UE⁴⁵ (article 32, paragraphe 6). Le CEPD salue le fait que la proposition désigne l'État membre responsable de l'effacement et que cet effacement doit avoir lieu «sans délai». Toutefois, le CEPD suggère de préciser l'expression «sans délai» dans le contexte de l'effacement des données conservées qui sont devenues excessives et ne sont plus nécessaires pour les besoins de l'EES.

31. Dans le cas spécifique des personnes ayant dépassé la durée de séjour autorisée, l'article 31, paragraphe 3, de la proposition de 2016 relative à l'EES prévoit (tout comme la proposition de 2013⁴⁶) une durée de cinq ans pour la conservation des données à compter du dernier jour du séjour autorisé. Cependant, les considérants de la proposition actuelle ne justifient pas plus cette nécessité que la proposition précédente⁴⁷, alors que le CEPD avait recommandé au législateur de mieux justifier, dans un considérant de la proposition relative à l'EES, la nécessité de conserver aussi longtemps les données des personnes ayant dépassé la durée de séjour autorisée, ou de limiter sensiblement cette durée⁴⁸.

32. En outre, la proposition de 2016 relative à l'EES prévoit que le système futur préviendra automatiquement l'État membre concerné, trois mois à l'avance, de l'effacement programmé des données relatives aux personnes ayant dépassé la durée de séjour autorisée, afin qu'il puisse prendre les mesures appropriées (article 31, paragraphe 3). À cet égard, l'exposé des motifs de la proposition relative à l'EES explique que les données concernant les personnes ayant dépassé la durée de séjour autorisée et n'ayant pas été trouvées à la fin de la période de conservation de cinq ans pourraient être enregistrées en tant que signalement aux fins de non-admission dans le SIS à la suite d'une décision nationale⁴⁹. Toutefois, l'adoption de mesures appropriées, notamment la création d'une alerte dans le SIS, pourrait survenir avant la période de cinq ans à compter de l'identification d'un ressortissant d'un pays tiers en tant que personne ayant dépassé la durée de séjour autorisée.

33. **Par conséquent, le CEPD ne comprend toujours pas la nécessité de conserver aussi longtemps ces données afin d'identifier les personnes ayant dépassé la durée de séjour autorisée. Il demande au législateur de justifier cette durée ou de la réduire de manière à ce qu'elle soit limitée au strict nécessaire.**

III.2 Données collectées

34. La proposition de 2016 relative à l'EES prévoit la collecte, le stockage et l'utilisation de données alphanumériques et de données biométriques concernant les ressortissants de pays tiers qui entrent et sortent de l'UE, telles qu'elles sont décrites aux articles 14 à 18. Le CEPD se réjouit de ce que la proposition réduit le volume global des données à caractère personnel de 36 à 26 éléments de données par individu et le nombre d'empreintes digitales⁵⁰ traitées de dix à quatre pour les ressortissants de pays tiers exemptés de l'obligation de visa (article 15, paragraphe 1). Pour les ressortissants de pays tiers soumis à l'obligation de visa, l'image faciale sera le seul élément d'identification biométrique enregistré dans l'EES (article 14, paragraphe 1), étant donné que leurs dix empreintes digitales sont déjà stockées dans le VIS. Le relevé des dix empreintes digitales est habituellement lié à la poursuite de finalités répressives.

35. Le CEPD doute cependant de la nécessité de stocker dans l'EES les images faciales des ressortissants de pays tiers soumis à l'obligation de visa, alors qu'elles le sont déjà dans le VIS. Le CEPD prend note de l'observation figurant dans l'analyse d'impact selon laquelle, à l'heure actuelle, *«le titulaire d'un visa ne peut être recherché dans le VIS à partir de son image»*, mais s'interroge sur la raison pour laquelle le VIS ne pourrait pas être pleinement utilisé à la fois pour les fonctions de l'EES et pour celles du VIS⁵¹. **Le CEPD demande de justifier la nécessité de stocker, dans l'EES, les images faciales des ressortissants de pays tiers soumis à l'obligation de visa. Cette obligation aura comme conséquence que les ressortissants de pays tiers soumis à l'obligation de visa verront leur image faciale enregistrée deux fois dans deux bases de données différentes, qui seront reliées entre elles. En l'absence d'une justification convaincante pour stocker les images faciales dans deux bases de données différentes, le CEPD recommande de retirer l'image faciale de l'article 14, paragraphe 1, de la proposition de telle sorte que l'EES repose à la fois sur les empreintes digitales et les images faciales déjà stockées dans le VIS pour les ressortissants de pays tiers soumis à l'obligation de visa, afin d'éviter la reproduction inutile de données biométriques dans les systèmes informatiques de l'UE et de limiter au strict nécessaire la collecte et le stockage de données dans l'EES.**

36. Enfin, l'article 15 de la proposition de 2016 relative à l'EES envisage plusieurs cas dans lesquels il serait impossible de relever les empreintes digitales des ressortissants de pays tiers pour des raisons juridiques (par exemple, l'individu a moins de 12 ans) ou factuelles (par exemple, il lui manque une main ou des doigts ou l'extrémité de ses doigts est endommagée). L'article 15, paragraphe 3, décrit la situation dans laquelle il est physiquement impossible de relever les empreintes digitales d'un ressortissant d'un pays tiers. Certaines de ces situations peuvent être de nature temporaire et sont habituellement liées à une affection médicale. La procédure décrite à l'article 15, paragraphe 3, autorise les autorités frontalières à demander des précisions sur les motifs de l'impossibilité temporaire de relever les empreintes digitales. Toutefois, aucune autre explication n'est apportée sur le sort réservé aux données collectées, ni sur l'endroit, les modalités et la durée de leur conservation, ni encore sur la manière dont elles

peuvent être utilisées et dont elles sont sécurisées. **Le CEPD recommande de modifier l'article 15, paragraphe 3, de manière à préciser les données pouvant être collectées, stockées et utilisées par les autorités frontalières.**

III.3 Recommandations supplémentaires sur les propositions

a) Données biométriques

37. La proposition de 2016 relative à l'EES prévoit la collecte, le stockage et l'utilisation des données biométriques des ressortissants de pays tiers: l'image faciale uniquement pour les voyageurs soumis à l'obligation de visa (article 14, paragraphe 1) et une combinaison de quatre empreintes digitales et de l'image faciale pour les voyageurs qui en sont exemptés (article 15, paragraphe 1). Le CEPD se réjouit de voir figurer la justification de l'usage particulier des données biométriques au considérant 10 de la proposition de 2016 relative à l'EES ainsi que d'un bout à l'autre de l'analyse d'impact accompagnant la proposition⁵². Le CEPD a reconnu à plusieurs reprises les avantages apportés par l'utilisation des données biométriques, tout en soulignant que, de par leur nature même, ces avantages dépendraient de l'application de garanties plus strictes⁵³. Toute erreur du système pourrait avoir d'importantes conséquences néfastes⁵⁴ pour les ressortissants de pays tiers dont les données se trouveront dans le système.

38. Toute proposition d'un système impliquant le traitement de données biométriques devrait s'accompagner de garanties et de sauvegardes suffisantes afin d'assurer la protection effective des données stockées face au risque d'abus, d'erreur, d'accès non autorisé et d'utilisation de ces données. Ces garanties et sauvegardes font pencher la balance vers une plus grande proportionnalité. Le CEPD a déjà recommandé la mise en œuvre d'une liste non exhaustive de sauvegardes pour le traitement automatique des données biométriques dans l'EES afin d'éviter que les ressortissants de pays tiers subissent les imperfections du système, par exemple en cas d'enregistrement impossible ou d'erreur du système lors de l'utilisation de données biométriques⁵⁵.

39. Le CEPD salue l'analyse d'impact sur les droits fondamentaux effectuée par la Commission⁵⁶, qui se concentre sur les incidences du futur EES sur les articles 7 et 8 de la Charte et aborde la question de la pertinence des données biométriques dans ce contexte et les raisons pour lesquelles les éléments d'identification biométriques ont été retenus dans la proposition. Le CEPD regrette néanmoins que ce document ne comprenne pas une analyse des conséquences des erreurs et des échecs de la technologie d'établissement de correspondances biométriques pour les ressortissants de pays tiers.

40. L'article 33 de la proposition de 2016 relative à l'EES établit à juste titre la nécessité de disposer d'empreintes digitales de haute qualité. La question de la qualité des images faciales qui ne sont pas tirées du document de voyage électronique lisible à la machine (eMRTD) (c'est-à-dire du passeport) n'est pas abordée, alors qu'elle revêt une importance capitale. **Le CEPD recommande donc d'ajouter à l'article 14 une disposition prévoyant un niveau de qualité minimal pour les images faciales prises en direct. En outre, l'article 33 devrait préciser que la Commission fournira, par voie de mesure d'exécution, des informations détaillées sur la manière d'atteindre ce niveau de qualité nécessaire pour les images faciales prises en direct.**

41. Le CEPD se réjouit également de ce que l'article 19 de la proposition de 2016 prévoit des procédures de secours en cas d'impossibilité technique d'introduire des données dans le système central ou en cas d'échec.

b) Sécurité du système

42. La sécurité d'un système tel que décrit à l'article 6 de la proposition relative à l'EES, qui s'étend sur de multiples entités [une unité centrale hébergée par l'eu-LISA et une interface uniforme nationale (IUN) dans chaque État membre] ne peut être réalisée que si une vision globale du système est adoptée. Autrement dit, il s'agit de ne pas se limiter à la sécurité de l'unité centrale, mais de tenir compte également de tous les autres composants du système et de tous ses utilisateurs. La sécurité du système proposé sera en outre affectée par celle d'autres systèmes reliés entre eux, comme les infrastructures frontalières nationales de chaque État membre.

43. Les mesures prises pour assurer la sécurité du système (unité centrale et IUN), qui comprennent les obligations des utilisateurs dans les États membres, doivent être harmonisées étant donné qu'un affaiblissement de la sécurité au niveau d'un élément du système affecterait la sécurité du système dans son ensemble. Par exemple, un incident de sécurité touchant un élément des infrastructures frontalières nationales reliées à une IUN pourrait affecter la sécurité de l'unité centrale de l'EES.

44. Bien que l'article 39 de la proposition de 2016 relative à l'EES établisse les responsabilités de l'eu-LISA et des États membres en matière de sécurité, il n'est fait aucune mention de la nécessité de veiller à cette harmonisation systématique des efforts dans le domaine de la sécurité. **Le CEPD recommande que l'article 39 souligne la nécessité de cette coordination entre l'eu-LISA et les États membres dans le domaine de la sécurité. Cette harmonisation de la sécurité devrait reposer sur un processus adéquat de gestion des risques dans le domaine de la sécurité des informations qui couvre l'ensemble des éléments du nouveau système, y compris les éléments relevant de la responsabilité des États membres.**

45. L'article 6, point c), mentionne la nécessité de disposer d'un «*canal de communication sécurisé entre le système central de l'EES et le système central du VIS*», mais son point d) ne fait pas explicitement mention de la sécurité dans le cas de l'«*infrastructure de communication entre le système central et les interfaces uniformes nationales*». **Le CEPD recommande de modifier le texte de l'article 6, point d), de la manière suivante: «une infrastructure de communication sécurisée entre le système central et les interfaces uniformes nationales».**

46. L'article 34 décrit les responsabilités en matière de développement et de gestion opérationnelle du système central, des interfaces uniformes nationales, de l'infrastructure de communication et du canal de communication sécurisé entre le système central de l'EES et le système central du VIS. Il n'aborde toutefois pas la question de la sécurité ni celle du respect de la vie privée. Le CEPD fait observer que tout nouveau système, et toute modification majeure d'un système existant (en l'occurrence, du VIS), ne sauraient être réalisés professionnellement que dans le respect:

- d'une procédure de sécurité adéquate comprenant une analyse détaillée des risques; et
- des principes de protection de la vie privée dès la conception et par défaut

47. Le CEPD recommande d'ajouter les exigences suivantes à l'article 34:

- la réalisation d'une analyse des risques dans le cadre du développement de ce nouveau système;
- le respect des principes de protection de la vie privée dès la conception et par défaut tout au long du développement du système;
- l'actualisation de l'analyse des risques concernant le VIS afin de tenir compte de la nouvelle connexion avec l'EES à venir et le suivi assuré par l'adoption des mesures de sécurité supplémentaires mises en évidence par l'analyse des risques actualisée.

c) Sécurité du site web

48. Le CEPD comprend la nécessité de fournir des informations aux ressortissants de pays tiers afin de «*vérifier à tout moment la durée de séjour autorisée restante*». Il comprend également que les transporteurs auront besoin de «*vérifier si des ressortissants de pays tiers titulaires d'un visa à entrée unique ou à double entrée ont déjà utilisé ou non leur visa*». D'après l'article 12 de la proposition de 2016 relative à l'EES, ces exigences seront satisfaites par un «*accès internet sécurisé à un service web hébergé par l'eu-LISA*». Toutefois, sous l'angle de la sécurité, la proposition de 2016 relative à l'EES ne contient pas d'informations suffisamment détaillées sur les mesures spécifiques pour garantir la sécurité des données à caractère personnel dans le cadre de ce service web et sur la répartition précise des responsabilités pour assurer cette sécurité, y compris lorsque les données à caractère personnel ont été extraites et stockées par les transporteurs.

49. Le CEPD comprend que l'eu-LISA sera responsable de la sécurité du service web et des données à caractère personnel qu'il contient ainsi que de la procédure de transfert de ces données du système central vers le service web. Il convient par conséquent de considérer l'eu-LISA comme le responsable du traitement pour ces aspects. Le CEPD recommande de préciser clairement ces responsabilités dans la proposition de 2016 relative à l'EES. Les besoins spécifiques en matière de sécurité devraient découler d'une analyse des risques dans le domaine de la sécurité des informations réalisée par l'eu-LISA. Cette analyse devrait être régulièrement mise à jour. L'eu-LISA devrait également être responsable de la mise en œuvre adéquate et du suivi des contrôles de sécurité définis à l'issue de l'analyse des risques.

50. Le CEPD nourrit en outre des inquiétudes quant à la sécurité des données à caractère personnel lorsque les transporteurs les auront extraites du service web, étant donné que rien n'indique qu'ils seront responsables de la sécurité de ces données. L'article 33, paragraphe 1, point g), fait référence aux mesures d'exécution que la Commission devra adopter avant le développement du nouveau système en ce qui concerne ce service web. Ces mesures pourraient être l'occasion d'imposer que les données à caractère personnel bénéficient d'un certain niveau de sécurité lorsqu'elles sont extraites par les transporteurs.

51. Un autre problème de sécurité posé par ce service web se rapporte à la manière dont les ressortissants de pays tiers et les transporteurs s'authentifieront auprès du service web afin de

demander des informations. L'authentification auprès du service web aurait lieu de la manière suivante:

- les ressortissants de pays tiers entreraient les données requises par l'article 14, paragraphe 1, point b), à savoir le type et le numéro du ou des documents de voyage, et le code en trois lettres du pays de délivrance (article 12, paragraphe 1);
- les transporteurs fourniraient les données énumérées à l'article 14, paragraphe 1, point d), à savoir le numéro de la vignette-visa de court séjour, y compris le code en trois lettres de l'État membre de délivrance, le type de visa, la date de fin de la durée maximale de séjour autorisée par le visa, qui doit être actualisée à chaque entrée, et la date d'expiration du visa, le cas échéant (article 12, paragraphe 2).

52. En ce qui concerne les ressortissants de pays tiers, l'authentification auprès du service web (uniquement à partir du type et du numéro du ou des documents de voyage, et du code en trois lettres du pays de délivrance) est peut-être faible; un tiers pourrait tenter d'entrer des données formatées adéquatement dans le service web dans l'espoir de confirmer le lien entre le ressortissant d'un pays tiers qui l'intéresse et les données de son document de voyage, pour ensuite obtenir des informations sur la durée de séjour autorisée de ce ressortissant. Des informations supplémentaires devraient être demandées au ressortissant d'un pays tiers qui utilise le service web afin de rendre plus difficile ce type d'attaque contre le service web et d'accroître l'assurance que la demande de consultation d'une série spécifique de données émane bien de lui. Une telle information pourrait être par exemple la date de naissance, qui serait demandée en plus du type et du numéro du ou des documents de voyage, et du code en trois lettres du pays de délivrance. La détermination du type exact d'informations supplémentaires devant être demandées pour une authentification en bonne et due forme des ressortissants de pays tiers devrait toutefois découler de l'analyse des risques recommandée au point 49 ci-dessus.

53. Comme les transporteurs pourraient consulter les données d'un grand nombre de ressortissants de pays tiers, il est nécessaire de s'assurer que seuls les membres de leur personnel habilités à cet effet ont accès au service web. Il convient par conséquent de mettre en place un système d'authentification adéquat qui ne soit pas lié aux données des ressortissants de pays tiers (par exemple, utilisation d'un identifiant et d'un mot de passe ou d'un jeton d'authentification). Le niveau approprié d'authentification devrait être défini sur la base de l'analyse des risques mentionnée précédemment. En outre, une traçabilité adéquate des demandes adressées au service web par les transporteurs devrait être assurée (journalisation) de manière à ce qu'ils puissent être tenus responsables si une utilisation abusive du service web est détectée.

d) Interopérabilité entre l'EES et le VIS

54. La proposition de 2016 relative à l'EES instaure dès le départ une «interopérabilité» entre l'EES et le VIS, ou plutôt une «interconnexion» des deux systèmes. La Commission considère l'interconnexion des systèmes d'information comme une dimension de l'interopérabilité et la définit comme le fait que «différents systèmes ou bases de données sont techniquement capables de communiquer les uns avec les autres»⁵⁷. L'interconnexion entre le futur EES et le VIS existant est une première étape vers un objectif à long terme de la Commission, annoncé dans la communication intitulée «Des systèmes d'information plus robustes et plus intelligents

au service des frontières et de la sécurité» et inclus dans le deuxième train de mesures «Frontières intelligentes»: l'amélioration de l'interopérabilité entre les systèmes d'information existants et futurs de l'UE pour la gestion des frontières et la sécurité.

55. La proposition de 2016 relative à l'EES charge l'eu-LISA d'établir un canal de communication direct entre les systèmes centraux des deux bases de données afin de permettre la consultation directe entre ces deux systèmes (article 7). L'EES et le VIS partageront les mêmes caractéristiques techniques et un système commun d'établissement de correspondances biométriques. Par conséquent, les autorités frontalières utilisant l'EES pourront également consulter le VIS aux fins spécifiques définies à l'article 7, paragraphe 2, de la proposition de 2016 relative à l'EES, tandis que les autorités chargées des visas utilisant le VIS pourront consulter l'EES aux fins spécifiques définies à l'article 7, paragraphe 3. L'article 55 de la proposition de 2016 relative à l'EES modifie aussi le règlement VIS afin d'assurer l'interopérabilité des deux systèmes.

56. La Commission déclare que «[c]ela permettra de réduire les doublons et donc les opérations inutiles de traitement de données à caractère personnel conformément au principe de "respect de la vie privée assuré dès la conception"»⁵⁸. Concrètement, les empreintes digitales des titulaires de visa déjà stockées dans le VIS ne le seront plus à nouveau dans l'EES, mais l'EES réutilisera les empreintes digitales du VIS pour ses besoins propres de manière à éviter que les empreintes digitales des titulaires de visa soient stockées à deux reprises, une fois dans chaque système. Le CEPD se demande pourquoi il ne saurait en être de même des images faciales des ressortissants de pays tiers soumis à l'obligation de visa, qui sont déjà stockées dans le VIS⁵⁹.

57. A priori, le CEPD ne s'oppose pas à l'interopérabilité des systèmes informatiques européens à grande échelle pour autant que le respect intégral des droits fondamentaux soit assuré. Il insiste cependant sur le fait qu'un tel choix est susceptible d'accroître les risques de violation des principes de protection des données, et en particulier le principe de limitation de la finalité. Pour ce qui est de l'EES et du VIS, la compatibilité de la réutilisation des données collectées dans le contexte du VIS pour chaque finalité de l'EES devrait être appréciée, et vice versa. Le CEPD considère que les finalités premières des deux systèmes sont étroitement liées et que les données concernées sont dans une certaine mesure identiques. Cela devrait limiter les risques d'abus.

58. Au-delà de la proposition spécifique de 2016 relative à l'EES, le CEPD analysera plus en détail à une autre occasion les implications de l'objectif général d'une plus grande interopérabilité poursuivi par la Commission.

e) Programmes nationaux d'allègement des formalités

59. La Commission a décidé de retirer sa proposition de 2013 relative au RTP du deuxième train de mesures «Frontières intelligentes», mais a présenté une proposition révisée de modification du code frontières Schengen. L'un des principaux changements introduits par la proposition de 2016 modifiant le code frontières Schengen réside dans un nouvel article 8 *sexies*, qui permet aux États membres d'établir des programmes nationaux d'allègement des formalités pour les ressortissants de pays tiers qui franchissent les frontières extérieures et peuvent bénéficier, lors de leur entrée, de dérogations aux vérifications approfondies. Les États membres qui choisissent volontairement cette option seront tenus de

soumettre à un contrôle de sûreté préalable les ressortissants de pays tiers demandant à participer à leurs programmes.

60. Le nouvel article 8 *sexies* impose aussi à la Commission d'effectuer une évaluation de sa mise en œuvre avant la fin de la troisième année de son application. Sur la base de cette évaluation, le Parlement européen ou le Conseil pourra inviter la Commission à proposer l'établissement d'un «*programme de l'Union pour les ressortissants de pays tiers qui voyagent fréquemment et ont fait l'objet d'un contrôle de sûreté préalable*». Le CEPD suivra de près ces développements.

61. Les programmes nationaux d'allègement des formalités ne nécessiteront pas le développement d'un nouveau système. Ils utiliseront les données conservées dans l'EES. L'article 23 de la proposition de 2016 relative à l'EES autorise par conséquent les autorités visées à l'article 8 *sexies* à accéder aux données de l'EES aux fins de l'examen des demandes d'accès aux programmes nationaux d'allègement des formalités. Dans un souci de cohérence, le CEPD recommande d'inclure cette finalité dans la liste de finalités spécifiques visée à l'article 5 de la proposition de 2016 relative à l'EES.

62. Par ailleurs, le nouvel article 8 *sexies* ne décrit aucune mesure de sécurité, et le besoin de sécurité n'y est même pas mentionné. **Le CEPD recommande de clarifier les responsabilités en matière de sécurité à toutes les étapes du processus, y compris en cas d'interconnexion entre les programmes volontaires des différents États membres et l'EES. Le CEPD recommande également de préciser dans le nouvel article 8 *sexies* du code frontières Schengen que la sécurité doit être garantie à la suite d'une analyse adéquate des risques dans le domaine de la sécurité des informations.**

f) Droits des personnes concernées

63. Le CEPD se réjouit des articles 44 et 46 de la proposition de 2016 relative à l'EES, qui prévoient le droit à l'information des ressortissants de pays tiers et leurs droits d'accès, de rectification et d'effacement de leurs données à caractère personnel.

64. Le CEPD nourrit tout d'abord certaines inquiétudes quant à l'article 46, paragraphe 6, de la proposition, qui conditionne les demandes d'accès, de rectification et d'effacement de données à caractère personnel présentées par *toute* personne concernée à la fourniture des empreintes digitales de l'intéressé. Le CEPD comprend la nécessité de joindre à ces demandes les données à caractère personnel permettant d'identifier certains ressortissants de pays tiers comme étant les personnes légitimes concernées. Toutefois, une telle condition pourrait constituer un obstacle de taille à l'exercice effectif du droit d'accès, qui est une garantie importante pour la personne concernée, et qui a même été inscrit à l'article 8, paragraphe 2, de la Charte. **Le CEPD conseille au législateur de l'UE de reconsidérer cette condition à l'exercice du droit d'accès, par exemple en limitant l'utilisation des empreintes digitales aux cas où de sérieux doutes planent sur l'identité du demandeur.**

65. En ce qui concerne le droit à l'information, le CEPD se réjouit de ce que la proposition de 2016 relative à l'EES prévoit désormais une brochure commune et un site web disponible en plusieurs langues, éventuellement complétés par des informations spécifiques émanant des États membres, en plus des informations déjà fournies aux ressortissants de pays tiers au

moment de la création de leur dossier individuel. **Le CEPD recommande néanmoins d'ajouter les éléments suivants aux informations énumérées à l'article 44, paragraphe 1:**

- 1) une explication du fait que les données de l'EES seront consultées aux fins de la gestion des frontières et de l'allègement des formalités. Cette explication précisera que le dépassement de la durée de séjour autorisée entraînera automatiquement l'ajout des données de l'individu à une liste⁶⁰ et indiquera les conséquences possibles de ce dépassement;
- 2) la durée de conservation des données fixée pour les fiches d'entrée/sortie et pour les dossiers individuels; et
- 3) le droit des personnes ayant dépassé la durée de séjour autorisée de voir leurs données à caractère personnel effacées si elles apportent la preuve que ce dépassement est dû à un événement grave et imprévisible⁶¹.

66. En ce qui concerne le droit d'accès, **le CEPD recommande que le délai de réponse aux demandes d'accès visées à l'article 46, paragraphe 1, soit rigoureux et harmonisé et qu'il ne dépasse pas quelques mois**⁶². Le respect du droit d'accès, tel qu'il est garanti par l'article 8 de la Charte, et le suivi des demandes d'accès revêtent une importance capitale dans la mesure où l'exercice de ce droit permet aux personnes concernées de contrôler le traitement de leurs données à caractère personnel et de découvrir éventuellement des erreurs et un accès illicite à ces données. En outre, l'article 48 concernant les voies de recours donne aux personnes concernées la possibilité de former un recours ou de déposer une plainte lorsque les droits d'accès, de rectification et d'effacement leur ont été refusés. Pour que ces droits soient effectifs, la même disposition devrait s'appliquer lorsque le responsable du traitement n'a pas répondu aux demandes d'exercice de ces droits ou lorsqu'il ne les a jamais traitées.

67. Le CEPD salue aussi l'article 9, paragraphe 2, qui explique que l'utilisation de l'EES ne peut avoir pour effet de soumettre les ressortissants de pays tiers à des discriminations fondées sur le sexe, la race ou l'origine ethnique, la religion ou les convictions, un handicap, l'âge ou l'orientation sexuelle. Le CEPD se félicite en outre de ce qu'une attention particulière a été accordée aux enfants et aux personnes âgées ou handicapées. La proposition omet toutefois de préciser les sauvegardes supplémentaires qui seraient mises en œuvre pour garantir que cette attention particulière à l'égard des enfants et des personnes âgées ou handicapées est dûment respectée. **Le CEPD recommande de modifier l'article 9, paragraphe 2, en décrivant clairement les sauvegardes qui garantiraient qu'une attention adéquate est accordée aux données ayant trait aux enfants et aux personnes âgées ou handicapées.**

g) Statistiques

68. Le CEPD comprend que le personnel dûment autorisé des autorités compétentes des États membres, de la Commission, de l'eu-LISA et de Frontex doivent élaborer des rapports et produire des statistiques sur les données contenues dans l'EES. Toutefois, le volume de données pouvant être consultées est susceptible de permettre l'identification d'individus, contrairement à ce qui est affirmé à l'article 57, paragraphes 1 et 2. Par exemple, la combinaison de la nationalité, du sexe et de la date de naissance d'un ressortissant d'un pays tiers peut donner lieu à son identification.

69. En outre, étant donné que l'eu-LISA devra extraire ces données et les transférer dans un fichier central, les risques de fuites de données augmentent significativement si des mesures de sécurité adéquates ne sont pas élaborées.

70. Le CEPD recommande par conséquent de reformuler l'article 57 relatif à l'utilisation des données à des fins de notification et d'établissement de statistiques en reconnaissant que les données énumérées à l'article 57, paragraphe 1, points a) à i), peuvent entraîner l'identification d'individus et qu'elles doivent dès lors être protégées de la même manière que le fichier central de l'EES. Cette protection implique de procéder à une analyse adéquate des risques dans le domaine de la sécurité des informations et de mettre en œuvre des mesures de sécurité appropriées avant de créer ce fichier central supplémentaire. Le CEPD met vivement en garde contre le fait que la solution proposée actuellement par l'article 57 imposera une lourde charge à l'eu-LISA, qui devra gérer et sécuriser de manière appropriée un deuxième fichier, mais aussi au CEPD, qui devra le contrôler. **Le CEPD serait favorable à une solution qui, au lieu de rendre nécessaire un fichier central supplémentaire, imposerait à l'eu-LISA de développer des fonctions permettant aux États membres, à la Commission, à l'eu-LISA et à Frontex d'extraire automatiquement et directement les statistiques demandées du système central de l'EES, sans qu'un fichier supplémentaire soit nécessaire.**

h) Le CEPD en tant que contrôleur

71. L'article 50 de la proposition de 2016 relative à l'EES établit les responsabilités du CEPD en tant que contrôleur du futur EES, l'une d'entre elles étant de veiller à ce qu'un audit des activités de traitement des données à caractère personnel menées par l'eu-LISA dans le cadre de ce nouveau système soit réalisé tous les quatre ans au minimum.

72. Toutefois, la proposition de 2016 relative à l'EES omet de fournir au CEPD les informations adéquates qui lui permettraient d'assumer ces nouvelles responsabilités de manière efficace et efficiente. De même, l'eu-LISA devrait informer le CEPD de tous les rapports qu'il devra présenter à la Commission, au Conseil ou au Parlement en vertu de la proposition. **Le CEPD recommande dès lors ce qui suit:**

- à l'article 36, paragraphe 3, que le CEPD soit informé des mesures prises par l'eu-LISA en vertu de l'article 36, paragraphe 2, non seulement lors de la mise en service de l'EES, mais aussi tout au long de la durée de vie de l'EES et de ses données;
- à l'article 64, paragraphe 2, que le CEPD soit informé des rapports concernant l'état d'avancement du développement du système central, des interfaces uniformes et de l'infrastructure de communication entre le système central et les interfaces uniformes;
- à l'article 64, paragraphe 4, que le CEPD reçoive le rapport sur le fonctionnement technique de l'EES tous les deux ans après la mise en service du système;
- à l'article 65, paragraphe 5, que le CEPD reçoive les rapports de la Commission concernant l'évaluation globale de l'EES.

73. En outre, **le CEPD recommande d'ajouter à l'article 50 une disposition similaire à celle de l'article 49, paragraphe 3, de manière à ce que les ressources nécessaires soient**

allouées au CEPD pour lui permettre d'assurer une surveillance adéquate de ce nouveau système.

IV. Accès des autorités répressives

74. La proposition de 2016 relative à l'EES prévoit que les autorités répressives des États membres et Europol auront accès aux données de l'EES dès sa mise en service⁶³. L'EES sera utilisé comme un outil d'identification afin d'identifier des suspects, des auteurs ou des victimes inconnus, et comme un outil de renseignement pour consulter l'historique des déplacements de suspects connus.

75. Le CEPD reconnaît qu'il est important que les autorités répressives aient à leur disposition les meilleurs outils possible pour trouver les auteurs d'infractions terroristes ou d'autres infractions pénales graves. Il rappelle⁶⁴ cependant que l'accès aux données de l'EES accordé aux autorités répressives devra respecter séparément les droits des ressortissants de pays tiers au respect de la vie privée et à la protection des données et qu'il déclenchera la même évaluation préalable de la nécessité et de la proportionnalité.

76. Le CEPD rappelle⁶⁵ que l'accès aux données de l'EES accordé aux autorités répressives s'inscrit dans une tendance croissante visant à octroyer à ces autorités l'accès aux données à caractère personnel de ressortissants de pays tiers qui franchissent les frontières de l'UE⁶⁶, bien qu'en principe, ces voyageurs ne soient pas soupçonnés d'un comportement illicite ou qu'ils ne fassent pas l'objet d'une enquête.

IV.1 Répression en tant qu'objectif secondaire

77. Comme expliqué ci-dessus⁶⁷, le CEPD comprend que la base de données de l'EES sera créée en premier lieu aux fins de la gestion des frontières et que l'accès au système pourrait ensuite être accordé aux autorités répressives sous réserve de conditions et de sauvegardes strictes. **Le CEPD considère qu'il serait inacceptable de créer l'EES décrit directement et principalement à des fins répressives et que l'EES devrait rester un outil de gestion des frontières uniquement conçu à cet effet.**

78. L'article 5 de la proposition de 2016 relative à l'EES énumère cependant douze finalités de la *collecte* et de la *conservation* des données de l'EES ainsi que de l'accès à ces données; les finalités j), k) et l) se rapportent aux finalités répressives secondaires du système. **Le CEPD recommande de modifier l'article 5 afin de bien faire ressortir que l'EES a des finalités principales et secondaires et d'inclure les finalités propres à la répression dans une disposition distincte, en tant que finalités secondaires, de manière à ce qu'elles ne semblent pas placées sur le même pied que les autres finalités liées à la gestion des frontières et à l'allègement des formalités.**

IV.2 Nécessité de l'accès des autorités répressives

79. Le CEPD souligne que le seul fait que les données de l'EES ont été principalement collectées à des fins spécifiques – et qu'elles sont donc disponibles – ne saurait justifier en soi le besoin d'accéder à ces données et de les utiliser à d'autres fins telles que la répression⁶⁸. À

cet égard, le CEPD a recommandé à plusieurs reprises d'apporter des preuves solides du besoin d'accéder aux données de l'EES à des fins répressives⁶⁹.

80. Le considérant 16 de la proposition actuelle affirme qu'*«il est essentiel que les autorités répressives disposent des informations les plus récentes pour pouvoir exécuter leurs tâches»* et que la possibilité existante qu'ont les autorités répressives d'accéder aux données du VIS *«a déjà prouvé son efficacité»*.

⁷⁰ Le CEPD fait observer que ce qui est considéré comme utile ne saurait être forcément tenu pour nécessaire en tant que tel pour la protection des données⁷¹ et que les allégations concernant la nécessité doivent être étayées par des preuves évidentes.

81. L'analyse d'impact accompagnant la proposition indique également que le VIS est effectivement consulté par des autorités répressives (soit 14 000 consultations/mois au cours des huit premiers mois de 2015) et que *«ces consultations permettent d'élucider de graves infractions pénales»* sans donner d'autres indications⁷². Le CEPD observe cependant que, d'après la communication de la Commission intitulée «Des systèmes d'information plus robustes et plus intelligents au service des frontières et de la sécurité», les autorités répressives des États membres utilisent de manière inégale la possibilité d'accéder au VIS et ont signalé des problèmes pratiques dans les procédures⁷³. De plus, bien qu'Europol ait la possibilité *légitime* d'accéder au VIS depuis la fin 2013, l'agence n'est en réalité pas connectée à la base de données et ne met pas encore en œuvre cette possibilité.

82. Le CEPD invite la Commission à fournir de plus amples informations, par exemple les rapports ou les statistiques disponibles qui tiennent compte de l'expérience déjà acquise avec le VIS (ainsi qu'avec le SIS et Eurodac), afin d'étayer ces allégations et de fournir des éléments objectifs supplémentaires prouvant que les autorités répressives, y compris Europol, doivent avoir accès aux données de l'EES.

IV.3 Conditions d'accès et sauvegardes

83. Dans l'éventualité où la nécessité d'un tel accès devait être établie, il conviendrait de démontrer que ce traitement supplémentaire respecte l'exigence de proportionnalité énoncée à l'article 52, paragraphe 1, de la Charte. Pour satisfaire à cette exigence, la CJUE a fourni des orientations dans l'arrêt DRI⁷⁴ et précisé qu'un tel accès doit être proportionné, étroitement ciblé et fondé sur des soupçons à l'encontre d'une personne déterminée. Cet accès doit être soumis à des conditions strictes le limitant à des cas spécifiques et être accompagné de sauvegardes appropriées.

84. Le CEPD se félicite que l'article 29 de la proposition de 2016 relative à l'EES définisse les conditions devant être remplies pour que les autorités répressives aient accès aux données de l'EES au moyen d'une demande électronique motivée ainsi que les conditions supplémentaires, énoncées à l'article 29, paragraphe 2, aux fins de l'identification d'un suspect ou d'un auteur inconnu ou d'une victime supposée d'une infraction terroriste ou d'une autre infraction pénale grave.

85. L'article 29, paragraphe 2, prévoit que ces recherches préalables ne sont pas obligatoires s'il existe des motifs raisonnables de croire qu'une comparaison avec les systèmes des autres États membres ne permettrait pas de vérifier l'identité de la personne concernée. Le CEPD ne voit pas comment une autorité désignée pourrait savoir à l'avance, sans effectuer de recherches

dans les systèmes des autres États membres, si des données pertinentes s'y trouvent. **Le CEPD invite la Commission à clarifier l'article 29, paragraphe 2.**

86. En outre, le CEPD considère que le mécanisme de vérification du respect de ces conditions d'accès aux données de l'EES constitue une sauvegarde essentielle pour empêcher tout accès illicite. L'article 26, paragraphe 3, de la proposition relative à l'EES charge les points d'accès centraux désignés de vérifier que les conditions de l'accès des autorités répressives nationales sont remplies. Toutefois, les autorités nationales désignées qui demandent l'accès aux données de l'EES et les autorités chargées de la vérification qui accordent celui-ci peuvent faire partie des mêmes autorités. En effet, l'article 26, paragraphe 3, prévoit que *«[l]’autorité désignée et le point d'accès central peuvent appartenir à la même organisation si le droit national le permet, mais le point d'accès central agit en toute indépendance quand il accomplit sa mission au titre du présent règlement»* et ajoute que *«[l]e point d'accès central est distinct des autorités désignées et ne reçoit d'elles aucune instruction concernant le résultat de ses vérifications»*. **Le CEPD recommande de modifier cette disposition afin d'empêcher que les autorités désignées et l'autorité chargée de la vérification appartiennent à la même organisation.** La même recommandation s'applique à l'unité spécialisée composée d'agents d'Europol qui sera désignée par l'agence en qualité de point d'accès central en application de l'article 27, paragraphe 2. Étant donné les spécificités d'Europol, un mécanisme efficace devrait être trouvé afin de soumettre l'autorisation préalable d'accéder aux données de l'EES au contrôle d'un organe qui soit suffisamment indépendant de l'autorité désignée⁷⁵.

87. Le CEPD insiste sur le fait que l'autorité chargée de la vérification doit être réellement indépendante de l'autorité désignée afin de garantir une vérification en bonne et due forme du respect des conditions. À cet égard, la CJUE a également jugé dans l'arrêt DRI que l'accès des autorités nationales compétentes devrait être *«subordonné à un contrôle préalable effectué soit par une juridiction, soit par une entité administrative»* indépendante *«dont la décision vise à limiter l'accès aux données et leur utilisation à ce qui est strictement nécessaire aux fins d'atteindre l'objectif poursuivi»*⁷⁶.

88. Par ailleurs, l'article 28, paragraphe 2, prévoit des cas d'urgence exceptionnels pour lesquels le respect de l'ensemble des conditions fixées à l'article 29 pourrait faire l'objet d'une vérification a posteriori. Le CEPD considère que les exceptions devraient être réglementées de la manière la plus précise possible. La proposition prévoit que la vérification a posteriori doit avoir lieu *«sans retard indu»* après le traitement de la demande. **Le CEPD recommande de fixer un délai strict pour l'exécution de cette vérification, qui commencerait à courir dès que la demande a été traitée.**

89. Enfin, le CEPD se réjouit de ce qu'une attention particulière a été attachée au droit de la personne concernée d'être informée de l'accès à des fins répressives. En effet, d'après l'article 44, paragraphe 1, point a), une explication, dans un langage clair, relative au fait que les États membres et Europol peuvent avoir accès aux données de l'EES à des fins répressives sera communiquée aux ressortissants de pays tiers.

4. CONCLUSION

90. Le CEPD salue les efforts réalisés par la Commission dans la proposition de 2016 relative à l'EES pour répondre aux préoccupations en matière de protection des données soulevées à l'égard du train de mesures «Frontières intelligentes» de 2013. Certaines des recommandations

et des observations formulées par le CEPD dans son avis précédent sur le train de mesures ont été dûment prises en considération, par exemple en ce qui concerne l'introduction de procédures de secours en cas d'impossibilité technique ou de dysfonctionnement du système.

91. Le CEPD salue les efforts de la Commission pour justifier la nécessité de la création de l'EES, mais souhaite formuler d'importantes recommandations directement liées à sa proportionnalité afin de garantir que l'EES respecte pleinement la condition essentielle prévue à l'article 52, paragraphe 1, à savoir qu'il doit être à la fois nécessaire et proportionné. Il fait observer que la nécessité et la proportionnalité de l'EES doivent être appréciées aussi bien de manière globale, compte tenu des systèmes informatiques à grande échelle qui existent déjà au sein de l'UE, que de manière spécifique, dans le cas particulier des ressortissants de pays tiers qui se rendent légalement dans l'UE. Il considère qu'une durée de conservation de cinq ans pour l'ensemble des données à caractère personnel stockées dans l'EES devrait être pleinement justifiée. Il souligne également que les aspects suivants de la proposition de 2016 relative à l'EES devraient être mieux justifiés et étayés par des preuves convaincantes: la capture de l'image faciale des voyageurs soumis à l'obligation de visa, la durée de conservation fixée à cinq ans pour les personnes ayant dépassé la durée de séjour autorisée et la nécessité de l'accès des autorités répressives aux données de l'EES. Dans le cas contraire, le législateur de l'UE devrait reconsidérer ces aspects.

92. En outre, étant donné que l'ingérence de l'EES dans les droits fondamentaux des ressortissants de pays tiers au respect de la vie privée et à la protection des données est de vaste ampleur, le CEPD considère que l'EES devrait rester un outil de gestion des frontières conçu à cet effet. Par conséquent, la différence entre les objectifs déclarés de l'EES, à savoir les objectifs principaux de gestion des frontières et d'allègement des formalités et l'objectif secondaire de répression, devrait être introduite clairement dans la proposition de 2016 relative à l'EES et mise en évidence tout au long du texte, en particulier en lien avec les articles 1^{er} et 5.

93. En outre, le CEPD nourrit des inquiétudes quant au fait que l'ensemble des personnes concernées seront tenues de fournir dans tous les cas leurs empreintes digitales lorsqu'elles introduisent une demande d'accès, de rectification ou d'effacement de leurs données à caractère personnel. Cela pourrait constituer un obstacle de taille à l'exercice effectif du droit d'accès, qui est une garantie importante pour la personne concernée, inscrite à l'article 8, paragraphe 2, de la Charte.

94. Les autres recommandations formulées par le CEPD dans le présent avis concernant les aspects et articles suivants:

- l'article 14 devrait être détaillé de manière à ce qu'un niveau de qualité minimal soit atteint pour les images faciales prises en direct. L'article 33 devrait préciser que la Commission fournira des informations détaillées sur la manière d'atteindre ce niveau de qualité nécessaire pour les images faciales prises en direct;
- l'article 15, paragraphe 3, devrait être modifié de manière à préciser les données pouvant être collectées, stockées et utilisées par les autorités frontalières lorsqu'elles demandent des précisions sur les motifs de l'impossibilité temporaire de relever les empreintes digitales;

- l'article 39 devrait souligner la nécessité d'une coordination entre l'eu-LISA et les États membres pour garantir la sécurité de l'EES;
- les responsabilités en matière de sécurité devraient être clairement établies dans la proposition en cas d'interconnexion entre les programmes nationaux d'allègement des formalités des États membres et l'EES. Le nouvel article 8 *sexies* du code frontières Schengen devrait préciser que la sécurité doit être garantie à la suite d'une analyse adéquate des risques dans le domaine de la sécurité des informations et décrire les mesures nécessaires;
- la proposition devrait indiquer clairement que l'eu-LISA est responsable de la sécurité du service web et des données à caractère personnel qu'il contient ainsi que de la procédure de transfert de ces données du système central vers le service web;
- l'article 44, paragraphe 1, devrait être modifié afin de comprendre l'information communiquée aux personnes concernées: la durée de conservation appliquée à leurs données, le droit des personnes ayant dépassé la durée de séjour autorisée de voir leurs données à caractère personnel effacées si elles apportent la preuve que ce dépassement est dû à un événement grave et imprévisible et une explication du fait que les données de l'EES seront consultées aux fins de la gestion des frontières et de l'allègement des formalités;
- l'article 46, paragraphe 1, devrait fixer un délai de réponse aux demandes d'accès qui soit rigoureux et harmonisé;
- l'article 9, paragraphe 2, devrait être modifié de manière à décrire clairement les sauvegardes qui garantiraient qu'une attention adéquate est accordée aux données ayant trait aux enfants et aux personnes âgées ou handicapées;
- l'article 57 devrait être modifié de manière à imposer à l'eu-LISA de développer des fonctions permettant aux États membres, à la Commission, à l'eu-LISA et à Frontex d'extraire automatiquement et directement les statistiques demandées du système central de l'EES, sans qu'un fichier supplémentaire soit nécessaire;
- la proposition devrait fournir au CEPD les informations et les ressources adéquates qui lui permettraient d'assumer ses nouvelles responsabilités de contrôleur du futur EES de manière efficace et efficiente;
- l'article 28, paragraphe 2, devrait fixer un délai strict dans lequel les autorités chargées de la vérification seront tenues d'exécuter la vérification a posteriori des conditions d'accès aux données de l'EES à des fins répressives en cas d'urgence;
- l'article 28, paragraphe 3, devrait être modifié afin d'empêcher que les autorités désignées et l'autorité chargée de la vérification appartiennent à la même organisation.

95. Le CEPD insiste sur la nécessité de traiter ces questions globalement. Il encourage le législateur à poursuivre ses activités visant à cartographier les différentes bases de données dans le contexte des frontières et des migrations, à mieux coordonner les différents systèmes

et à éviter les chevauchements entre eux, tout en respectant pleinement les normes en matière de protection des données et ses relations avec les pays tiers.

Bruxelles, le 21 septembre 2016

(signature)

Giovanni BUTTARELLI
Contrôleur européen de la protection des données

NOTES

¹ JO L 281 du 23.11.1995, p. 31.

² JO L 8 du 12.1.2001, p. 1.

³ JO L 350 du 30.12.2008, p. 60.

⁴ Communication de la Commission du 13 février 2008 intitulée «Préparer les prochaines évolutions de la gestion des frontières dans l'Union européenne», COM(2008) 69 final.

⁵ Observations préliminaires du CEPD du 3 mars 2008 sur trois communications relatives à la gestion des frontières.

⁶ Avis du CEPD du 7 juillet 2011 sur la communication sur la migration.

⁷ Communication de la Commission du 25 octobre 2011 intitulée «Frontières intelligentes: options et pistes envisageables», COM(2011) 680 final.

⁸ Le groupe de travail «Article 29» a commenté la communication de la Commission relative aux frontières intelligentes dans une lettre adressée à la commissaire Malmström le 12 juin 2012.

⁹ Table ronde du CEPD sur le train de mesures «Frontières intelligentes» et ses conséquences pour la protection des données, Bruxelles, 10 avril 2013. Voir le résumé disponible à l'adresse suivante: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/Events/2013/13-04-10_Summary_smart_borders_final_EN.pdf

¹⁰ Proposition de règlement du Parlement européen et du Conseil portant création d'un système d'entrée/sortie pour l'enregistrement des entrées et sorties des ressortissants de pays tiers franchissant les frontières extérieures des États membres de l'Union européenne, COM(2013) 95 final.

¹¹ Proposition de règlement du Parlement européen et du Conseil portant création d'un programme d'enregistrement des voyageurs, COM(2013) 97 final.

¹² Proposition de règlement du Parlement européen et du Conseil modifiant le règlement (CE) n° 562/2006 en ce qui concerne l'utilisation du système d'entrée/sortie (EES) et le programme d'enregistrement des voyageurs (RTP), COM(2013) 96 final.

¹³ Avis du CEPD du 18 juillet 2013 sur les propositions de règlement portant création d'un système d'entrée/sortie (EES) et de règlement portant création d'un programme d'enregistrement des voyageurs (RTP).

¹⁴ Avis 05/2013 du groupe de travail «Article 29» du 6 juin 2013 sur les frontières intelligentes.

¹⁵ Étude technique sur les frontières intelligentes – rapport final, octobre 2014, disponible à l'adresse suivante: http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/smart-borders/docs/smart_borders_technical_study_en.pdf

¹⁶ Étude technique sur les frontières intelligentes – analyse des coûts, octobre 2014, disponible à l'adresse suivante: http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/smart-borders/docs/smart_borders_costs_study_en.pdf

¹⁷ Rapport final de l'eu-LISA sur le projet pilote relatif aux frontières intelligentes, décembre 2015, disponible à l'adresse suivante: http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/smart-borders/index_en.htm

¹⁸ Consultation publique de la Commission sur les frontières intelligentes, disponible à l'adresse suivante: http://ec.europa.eu/dgs/home-affairs/what-is-new/public-consultation/2015/consulting_0030_en.htm

¹⁹ Observations formelles du CEPD du 3 novembre 2015 sur la consultation publique de la Commission sur les frontières intelligentes.

²⁰ Voir le communiqué de presse disponible à l'adresse suivante: http://europa.eu/rapid/press-release_IP-16-1247_fr.htm

²¹ Communication de la Commission du 6 avril 2016 intitulée «Des systèmes d'information plus robustes et plus intelligents au service des frontières et de la sécurité», COM(2016) 205 final.

²² COM (2016) 194 final.

²³ Règlement (UE) 2016/399 du Parlement européen et du Conseil du 9 mars 2016 concernant un code de l'Union relatif au régime de franchissement des frontières par les personnes (code frontières Schengen) (texte codifié), JO L 77 du 23.3.2016, p. 1.

²⁴ COM (2016) 196 final.

²⁵ Document de travail des services de la Commission du 6 avril 2016 intitulé «Analyse d'impact sur la création d'un système d'entrée/sortie de l'UE accompagnant la proposition de 2016 relative à l'EES et la proposition de 2016 modifiant le code frontières Schengen», SWD(2016) 115 final (ci-après l'«analyse d'impact»).

²⁶ <http://data.consilium.europa.eu/doc/document/ST-8485-2016-INIT/en/pdf>

²⁷ La DG HOME et le CEPD ont organisé en 2015 deux ateliers sur certains aspects des frontières intelligentes: le premier, qui a eu lieu le 20 mars, portait plus particulièrement sur l'élaboration des propositions relatives aux frontières intelligentes; le second, interactif, s'est tenu le 21 septembre 2015 et concernait la problématique de la protection des données et du respect de la vie privée dans les politiques relatives aux migrations et aux affaires intérieures. Ce second atelier a également abordé les propositions de 2013 relatives aux frontières intelligentes. Voir le compte rendu de l'atelier du 20 mars 2015 à l'annexe 16 de l'analyse d'impact.

²⁸ Le terme de «personne ayant dépassé la durée de séjour autorisée» est défini comme suit à l'article 3, paragraphe 1, point 18, de la proposition de 2016 relative à l'EES: «*tout ressortissant d'un pays tiers qui ne remplit pas, ou ne remplit plus, les conditions tenant à la durée d'un court séjour sur le territoire des États membres*».

²⁹ La proposition de 2016 relative à l'EES exclut de son champ d'application les ressortissants de pays tiers qui bénéficient des dispositions de la directive 2004/38/CE et sont titulaires de la carte de séjour adéquate, les titulaires d'un titre de séjour au sens de l'article 2, paragraphe 16, du texte codifié du code frontières Schengen, les titulaires d'un visa de long séjour, les ressortissants des principautés d'Andorre et de Monaco, de la république de Saint-Marin, et les personnes ou catégories de personnes exemptées de vérifications aux frontières ou bénéficiant de mesures facilitant le franchissement des frontières, conformément au code frontières Schengen (article 2, paragraphe 3).

³⁰ Voir page 5 de l'analyse d'impact.

³¹ Les articles 14 à 18 de la proposition relative à l'EES dressent une liste exhaustive des données à caractère personnel qui seront collectées et stockées dans l'EES, tant pour les ressortissants de pays tiers soumis à l'obligation de visa que pour ceux qui en sont exemptés.

³² Voir page 34 de l'analyse d'impact selon laquelle, par exemple, le nom de naissance et le lieu de naissance ne devraient plus figurer dans l'EES à venir.

³³ Avis 03/2012 du groupe de travail «Article 29» du 27 avril 2012 sur l'évolution des technologies biométriques; arrêt de la CEDH du 4 décembre 2008 dans l'affaire S. et Marper/Royaume-Uni, requêtes n^{os} 30562/04 et 30566/04, points 84-85, dans lequel la Cour européenne des droits de l'homme a considéré que les empreintes digitales «*contiennent objectivement des informations uniques sur l'individu concerné et permettent une identification précise dans un grand nombre de circonstances*» et que la conservation de ces données peut donner lieu à des préoccupations importantes concernant le respect de la vie privée.

³⁴ Voir pages 2 et 3 de l'exposé des motifs de la proposition de 2016 relative à l'EES.

³⁵ Voir pages 58 à 65 de l'analyse d'impact; la gestion des frontières et l'allègement des formalités sont aussi décrits comme «*la finalité première de l'EES*» à la page 65 du document. En outre, l'annexe 13 de l'analyse d'impact relative aux incidences sur les droits fondamentaux parle elle aussi d'un «*objectif principal*».

³⁶ Voir page 37 de l'analyse d'impact; la répression est également présentée comme la «*finalité secondaire*» aux pages 38 et 65 du document. En outre, l'annexe 13 de l'analyse d'impact relative aux incidences sur les droits fondamentaux parle également d'un «*objectif secondaire*».

³⁷ Voir points 28, 35 et 82 ci-dessous

³⁸ Voir section I ci-dessus sur les incidences de l'EES sur le respect de la vie privée et la protection des données.

³⁹ Affaires jointes C-293/12 et C-594/12, Digital Rights Ireland (C-293/12) et Seitlinger (C-594/12), EU:C:2014:238 (ci-après l'«*arrêt DRI*»).

⁴⁰ Voir annexe 13 de l'analyse d'impact relative aux incidences sur les droits fondamentaux, p. 127.

⁴¹ La proposition de 2013 relative à l'EES prévoyait une conservation des données d'une durée maximale de 180 jours (article 20).

⁴² La proposition opère une nette distinction entre les «*dossiers individuels*», qui comprendront les «*éléments d'identification*» (par exemple, le nom, la date de naissance, etc.), les données du passeport et les données biométriques, et les fiches d'entrée/sortie ou les fiches de refus d'entrée, qui correspondent à la date et au lieu d'entrée/sortie ou de refus d'entrée.

⁴³ Arrêt DRI, point 64.

⁴⁴ Voir page 37 de l'analyse d'impact.

⁴⁵ Par exemple, lorsque le ressortissant d'un pays tiers épouse un citoyen de l'UE.

⁴⁶ Voir article 20, paragraphe 3, de la proposition de 2013 relative à l'EES.

⁴⁷ Le considérant 27 de la proposition de 2016 relative à l'EES considère que le choix de la durée de cinq ans est nécessaire «*afin de faciliter l'identification et le processus de retour*».

⁴⁸ Avis du CEPD du 18 juillet 2013, point 76; observations formelles du CEPD du 3 novembre 2015, p. 9.

⁴⁹ Voir page 6 de l'exposé des motifs de la proposition de 2016 relative à l'EES et l'article 24, paragraphe 3, du règlement SIS II qui dispose qu'«*[u]n signalement peut également être introduit lorsque la décision visée au paragraphe 1 est fondée sur le fait que le ressortissant d'un pays tiers a fait l'objet d'une mesure d'éloignement, de renvoi ou d'expulsion qui n'a pas été abrogée ni suspendue, et qui comporte ou est assortie d'une interdiction d'entrée, ou, le cas échéant, de séjour, fondée sur le non-respect des réglementations nationales relatives à l'entrée ou au séjour des ressortissants de pays tiers*».

⁵⁰ Voir articles 10 et 11 de la proposition de 2013 relative à l'EES.

-
- ⁵¹ Voir page 30 de l'analyse d'impact.
- ⁵² Voir annexe 13 de l'analyse d'impact relative aux incidences sur les droits fondamentaux, p. 125.
- ⁵³ Avis du CEPD du 18 juillet 2013, point 64; observations formelles du CEPD du 3 novembre 2015, p. 6.
- ⁵⁴ Les conséquences d'une identification en tant que personne ayant dépassé la durée de séjour autorisée dans l'UE pourraient être, par exemple, le refus ultérieur d'un nouveau visa, lorsque l'individu souhaitera revenir sur le territoire de l'UE après l'avoir quitté. Il s'agit également d'un motif de renvoi du ressortissant d'un pays tiers dans son pays d'origine.
- ⁵⁵ Avis du CEPD du 7 juillet 2011, point 31; observations formelles du CEPD du 3 novembre 2015, p. 6; et avis du CEPD du 19 octobre 2005 sur trois propositions concernant le système d'information Schengen de deuxième génération (SIS II), section 4.1. sur les données biométriques.
- ⁵⁶ Annexe 13 de l'analyse d'impact relative aux incidences sur les droits fondamentaux.
- ⁵⁷ Communication de la Commission du 6 avril 2016 intitulée «Des systèmes d'information plus robustes et plus intelligents au service des frontières et de la sécurité», COM(2016) 205 final, p. 16.
- ⁵⁸ Voir page 5 de l'exposé des motifs de la proposition de 2016 relative à l'EES.
- ⁵⁹ Voir point 35 ci-dessus.
- ⁶⁰ Voir article 11 de la proposition de 2016 relative à l'EES.
- ⁶¹ Voir article 32, paragraphe 5, de la proposition de 2016 relative à l'EES.
- ⁶² Article 12 de la directive 95/46/CE.
- ⁶³ La proposition de 2013 relative à l'EES avait envisagé un tel accès en tant qu'option possible pouvant être mise en œuvre sur la base d'une évaluation du système réalisée deux ans après son entrée en service (article 46, paragraphe 5).
- ⁶⁴ Annexe 16 de l'analyse d'impact sur les travaux préparatoires avec le Contrôleur européen de la protection des données, p. 142.
- ⁶⁵ Avis du CEPD du 18 juillet 2013, point 68; observations formelles du CEPD du 3 novembre 2015, p. 5.
- ⁶⁶ Une telle tendance a été observée ces dernières années, et elle devrait prendre de l'ampleur dans un proche avenir, eu égard à la proposition de règlement sur le système européen d'information sur les casiers judiciaires (ECRIS), qui étend le système actuel aux casiers judiciaires des ressortissants de pays tiers, et à la proposition de 2016 relative à la refonte du règlement Eurodac, qui étendra les finalités du système et, partant, le volume des données auxquelles les autorités répressives nationales sont autorisées à accéder.
- ⁶⁷ Voir ci-dessus, point 20.
- ⁶⁸ Avis 03/2013 du groupe de travail «Article 29» du 2 avril 2013 sur la limitation des finalités.
- ⁶⁹ Avis du CEPD du 18 juillet 2013, point 69; observations formelles du CEPD du 3 novembre 2015, pp. 4 et 10.
- ⁷⁰ Considérant 16 de la proposition de 2016 relative à l'EES.
- ⁷¹ La CEDH a jugé que la notion de nécessité n'avait pas la souplesse de termes tels qu'«*admissible*», «*normal*» ou «*utile*», mais qu'il impliquait un «*besoin social impérieux*»; voir arrêt de la CEDH du 7 décembre 1976 dans l'affaire Handyside/Royaume-Uni, requête n° 5493/72, point 48.
- ⁷² Voir page 67 de l'analyse d'impact.
- ⁷³ Communication de la Commission du 6 avril 2016 intitulée «Des systèmes d'information plus robustes et plus intelligents au service des frontières et de la sécurité», COM(2016) 205 final, pp. 8 et 9.
- ⁷⁴ Arrêt DRI, points 58 à 68.
- ⁷⁵ Pour le même raisonnement, voir point 58 de l'avis 7/2016 du CEPD du 21 septembre 2016 sur le premier paquet de mesures pour une réforme du régime d'asile européen commun.
- ⁷⁶ Arrêt DRI, point 62.