LE CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES

Avis du contrôleur européen de la protection des données

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)

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 données[1],

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 données[2],

vu la demande d'avis présentée conformément à l'article 28, paragraphe 2, du règlement (CE) n° 45/2001,

A ADOPTÉ LE PRÉSENT AVIS:

I. INTRODUCTION

I.1. Consultation du CEPD

1. Le 28 février 2013, la Commission a adopté les propositions suivantes (ci-après «les propositions»):
   - proposition de règlement du Parlement européen et du Conseil portant création d'un système d'entrée/sortie (EES) pour l'enregistrement des entrées et sorties des ressortissants de pays tiers franchissant les frontières extérieures des États membres de l'Union européenne (ci-après la «proposition d'EES»)[3];
   - proposition de règlement du Parlement européen et du Conseil portant création d'un programme d'enregistrement des voyageurs (RTP) (ci-après la «proposition de RTP»)[4];

[1] JO L 281 du 23.11.95, p. 31.
[2] JO L 8 du 12.1.2001, p. 1.
[3] COM(2013) 95 final.
[4] COM(2013) 97 final.

Adresse postale: rue Wiertz 60 - B-1047 Bruxelles
Bureaux: rue Montoyer 30
E-mail : edps@edps.europa.eu – Site web: www.edps.europa.eu
Tel.: 02-283 19 00 - Fax : 02-283 19 50

- 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) (ci-après la «proposition de modification»)[5];

2. Le même jour, les propositions ont été envoyées au CEPD pour consultation. Avant l'adoption des propositions, le CEPD a eu la possibilité de formuler des commentaires informels à la Commission.

3. Le CEPD se réjouit qu'il soit fait référence à sa consultation au préambule de la proposition d'EES ainsi qu'à celui de la proposition de RTP.

I.2. Contexte

4. La communication de la Commission de 2008 intitulée «Préparer les prochaines évolutions de la gestion des frontières dans l'Union européenne» a proposé de nouveaux outils pour la future gestion des frontières européennes, notamment un système d'entrée/sortie (ci-après «EES») qui permettrait l'enregistrement électronique des dates d'entrée et de sortie des ressortissants de pays tiers ainsi qu'un programme d'enregistrement des voyageurs pour faciliter le franchissement des frontières pour les voyageurs de bonne foi (ci-après «RTP»). Elle envisageait également l'introduction d'un système d'autorisation électronique de voyage (ESTA) pour les ressortissants de pays tiers exemptés de l'obligation de visa.

5. Ces propositions ont été approuvées par le Conseil européen de décembre 2009 dans le programme de Stockholm[6]. Toutefois, dans sa communication de 2011 sur les frontières intelligentes, la Commission[7] a considéré que la mise en place d'un ESTA devait être écartée à ce stade car «sa contribution potentielle au renforcement de la sécurité des États membres ne justifierait pas la collecte de données à caractère personnel à pareille échelle ni son coût et son impact sur les relations internationales»[8]. Elle a également annoncé son intention de présenter des propositions relatives à l'EES et au RTP au cours du premier semestre de 2012.

6. Plus tard, le Conseil européen de juin 2011 a demandé que les travaux relatifs aux «frontières intelligentes» progressent rapidement et a réclamé l'introduction de l'EES et du RTP[9].

[5] COM(2013) 96 final.
[6] «Un Europe ouverte et sûre qui sert et protège les citoyens», Journal officiel de l'Union européenne du 4.5.2010, C 115/1.
[7] Communication de la Commission au Parlement européen, au Conseil, au Comité social et économique et au Comité des régions du 25 octobre 2011 – «Frontières intelligentes: options et pistes envisageables» [COM(2011) 680 final].
[8] Communication de la Commission sur les frontières intelligentes, précitée, p. 7.
[9] EUCO 23/11.

7. Le groupe de travail «Article 29» s'est prononcé sur la communication de la Commission relative aux frontières intelligentes, qui précédait les propositions, dans une lettre adressée le 12 juin 2012 à la commissaire Malmström[10]. Plus récemment, le 6 juin 2013, le groupe de travail a adopté un avis émettant des doutes sur la nécessité du paquet relatif aux frontières intelligentes[11].

8. Le présent avis se base sur ces positions, ainsi que sur un précédent avis du CEPD[12] relatif à la communication de la Commission de 2011 sur la migration[13] et sur les observations préliminaires formulées par le CEPD[14] sur trois communications relatives à la gestion des frontières (2008)[15]. Il se fonde également sur les informations fournies lors de la table ronde du CEPD sur le paquet relatif aux frontières intelligentes et ses implications sur la protection des données[16].

I.3. Objectif des propositions

9. L'article 4 de la proposition d'EES décrit sa finalité. La proposition a pour finalité d'améliorer la gestion des frontières extérieures de l'UE et la lutte contre l'immigration irrégulière, la mise en œuvre de la politique de gestion intégrée des frontières, la coopération entre les autorités douanières et celles compétentes en matière d'immigration ainsi que leur consultation mutuelle. Elle prévoit un système qui:

[10] Le groupe de travail «Article 29», institué conformément à la directive 95/46/CE, se compose d'un représentant de chaque autorité nationale de protection des données, du CEPD et d'un représentant de la Commission européenne. Il possède un caractère consultatif et indépendant. La lettre adressée le 12 juin 2012 par le groupe de travail à M[me] Cecilia Malmström au sujet des frontières intelligentes est disponible sur http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2012/20120612_letter_to_malmstrom_smart-borders_en.pdf.

[11] Groupe de travail «Article 29», avis n° 05/2013 sur les frontières intelligentes. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp206_en.pdf

[12] Avis du CEPD du 7 juillet 2011, consultable à l'adresse suivante: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2011/11-07-07_Migration_FR.pdf.

[13] Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions du 4 mai 2011 sur la migration [COM(2011) 248/3].

[14] Observations préliminaires du CEPD du 3 mars 2008, consultables à l'adresse suivante: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2008/08-03-03_Comments_border_package_EN.pdf.

[15] Communications de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions intitulées «Préparer les prochaines évolutions de la gestion des frontières dans l'Union européenne» [COM(2008) 69 final], «Examen de la création d'un système européen de surveillance des frontières (EUROSUR)» [COM(2008) 68 final] et «Rapport sur l'évaluation et le développement futur de l'agence FRONTEX», COM(2008) 67 final.

[16] Table ronde du CEPD sur le paquet relatif aux frontières intelligentes et ses implications sur la protection des données, Bruxelles, 10 avril 2013, lieu: locaux du CEPD, Rue Montoyer 30, Bruxelles. Voir résumé 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

a. renforcerait les vérifications aux points de passage des frontières extérieures et combattrait l'immigration clandestine;
b. calculerait et contrôlerait le calcul de la durée du séjour autorisé des ressortissants de pays tiers admis pour un court séjour;
c. aiderait à l'identification de toute personne qui ne remplit pas, ou ne remplit plus, les conditions d'entrée ou de séjour sur le territoire des États membres;
d. permettrait aux autorités nationales des États membres d'identifier les personnes ayant dépassé la durée de séjour autorisée et de prendre les mesures appropriées;
e. recueillerait des statistiques sur les entrées et sorties des ressortissants de pays tiers à des fins d'analyse.

10. Ce système devrait aider à contrôler la durée de séjour autorisée en fournissant des informations rapides et précises aux garde-frontières et aux voyageurs. Il remplacerait l'actuel système d'apposition manuelle des cachets sur les passeports, considéré comme lent et peu fiable, et améliorerait l'efficacité de la gestion des frontières[17].

11. Il devrait également faciliter, grâce au stockage des éléments biométriques, l'identification des personnes ne remplissant pas les conditions d'entrée ou de séjour dans l'UE, surtout en l'absence de documents d'identification. L'EES permettrait en outre de se faire une idée précise des flux de voyageurs et du nombre de personnes ayant dépassé la durée de séjour autorisée et d'élaborer ainsi des politiques fondées sur des faits, par exemple en ce qui concerne les obligations de visa. Les statistiques mentionnées à l'article 4 servent à réaliser ce dernier objectif.

12. L'EES servirait de base pour le RTP, qui, lui, a pour but de faciliter le passage des frontières pour les ressortissants de pays tiers voyageant fréquemment et ayant fait l'objet d'un contrôle de sûreté préalable. Les voyageurs enregistrés disposeraient d'un jeton contenant un numéro d'identification unique, à passer dans une barrière automatique à l'arrivée et au départ à la frontière. Les données du jeton, les empreintes digitales et, le cas échéant, le numéro de vignette-visa seraient comparés à ceux stockés dans le registre central et dans d'autres bases de données. Si toutes les vérifications concordent, le voyageur pourrait franchir la barrière automatique. Sinon, il serait aidé par un garde-frontière.

13. Enfin, la proposition de modification a pour objectif d'adapter le règlement (CE) n° 562/2006 établissant un code communautaire relatif au régime de franchissement des frontières par les personnes (ci-après «le code frontières Schengen») aux nouvelles propositions d'EES et de RTP.

[17] Voir l'exposé des motifs de la proposition d'EES.

I.4. Contexte et structure du présent avis

14. Le projet d'élaborer un système électronique destiné à contrôler les entrées et les sorties du territoire de l'UE n'est pas nouveau: plusieurs communications de la Commission susmentionnées ont déjà préparé le terrain pour les propositions actuellement examinées. Le paquet relatif aux frontières intelligentes doit dès lors être examiné en tenant compte de ces développements. Il convient en particulier de prendre en considération les éléments suivants.

15. Dans le programme de Stockholm, la Commission a adopté l'approche stratégique consistant à évaluer la nécessité de mettre au point un modèle européen en matière d'échange d'informations sur la base de l'évaluation des instruments actuels. Il sera notamment question de mettre en place un solide régime de protection des données ainsi qu'un système de collecte de données bien ciblé, et de procéder à la rationalisation des différents instruments, notamment en adoptant un plan de développement pour les systèmes d'information à grande échelle. Le programme de Stockholm rappelle la nécessité d'assurer la cohérence de la mise en œuvre et de la gestion des différents outils de gestion de l'information avec la stratégie de protection des données à caractère personnel et le plan de développement pour les systèmes d'information à grande échelle[18].

16. Une analyse globale est d'autant plus nécessaire compte tenu de l'existence et du développement et de la mise en œuvre de systèmes informatiques à grande échelle, tels qu'Eurodac[19], le VIS[20] et le SIS II[21]. Un système de frontières intelligentes représente un outil supplémentaire permettant de collecter de vastes quantités de données à caractère personnel dans le cadre du contrôle des frontières. Cette approche globale a été récemment confirmée par le Conseil JAI, qui a souligné la nécessité de tirer des enseignements de l'expérience du SIS, surtout en ce qui concerne l'escalade des coûts[22]. Le CEPD a également observé qu'«un

[18] Le programme de Stockholm — une Europe ouverte et sûre qui sert et protège les citoyens, JO 2010/C 115/01.

[19] Voir le règlement (UE) n° 603/2013 du Parlement européen et du Conseil du 26 juin 2013 relatif à la création d'Eurodac pour la comparaison des empreintes digitales aux fins de l'application efficace du règlement (UE) n° 604/2013 établissant les critères et mécanismes de détermination de l'État membre responsable de l'examen d'une demande de protection internationale introduite dans l'un des États membres par un ressortissant de pays tiers ou un apatride et relatif aux demandes de comparaison avec les données d'Eurodac présentées par les autorités répressives des États membres et Europol à des fins répressives, et modifiant le règlement (UE) n° 1077/2011 portant création d'une agence européenne pour la gestion opérationnelle des systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice, JO L 180 du 29.6.2013.

[20] Voir le règlement (CE) n° 767/2008 du Parlement européen et du Conseil du 9 juillet 2008 concernant le système d'information sur les visas (VIS) et l'échange de données entre les États membres sur les visas de court séjour (règlement VIS), JO L 218/60 du 13.8.2008.

[21] Voir le règlement (CE) n° 1987/2006 du Parlement européen et du Conseil du 20 décembre 2006 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen de deuxième génération
(SIS II), JO L 381/4 du 28.12.2006.

[22] Voir doc. du Conseil n° 8018/13, Note de la Présidence au Comité stratégique sur l'immigration, les frontières et l'asile/Comité mixte (UE-Islande/Liechtenstein/Norvège/Suisse) du 28 mars 2013 sur le paquet relatif aux frontières intelligentes.

modèle européen d'information ne peut être conçu sur la base de considérations techniques», compte tenu des possibilités quasiment illimitées offertes par les nouvelles technologies. Les informations doivent être traitées uniquement sur la base de besoins concrets en matière de sécurité[23].

17. L'analyse de l'EES et du RTP du point de vue de la protection de la vie privée et des données doit se faire à la lumière de la Charte des droits fondamentaux de l'Union européenne[24] (ci-après «la Charte»), et en particulier de ses articles 7 et 8. L'article 7, qui est similaire à l'article 8 de la Convention européenne des droits de l'homme (CEDH)[25], prévoit le droit général au respect de la vie privée et familiale et protège l'individu de l'ingérence des pouvoirs publics, tandis que l'article 8 de la Charte donne à chaque personne le droit à ce que ses données à caractère personnel ne soient traitées que dans certaines conditions particulières. Ces deux approches sont différentes et complémentaires. Le paquet relatif aux frontières intelligentes sera évalué en fonction de ces deux points de vue.

18. Le présent avis est particulièrement axé sur la proposition d'EES, qui est la plus pertinente en ce qui concerne la protection de la vie privée et des données. Il est structuré comme suit:

- la section II contient une évaluation générale du système d'entrée/sortie, axée sur le respect des articles 7 et 8 de la Charte;
- la section III présentera des commentaires sur les dispositions plus spécifiques de l'EES relatives au traitement des données biométriques et à l'accès des autorités répressives aux données;
- la section IV proposera des observations sur d'autres problèmes posés par l'EES;
- la section V traitera plus particulièrement du RTP;
- la section VI portera sur la nécessité d'inclure de nouvelles garanties en matière de sécurité des données;
- la section VII dressera la liste des conclusions.

http://www.statewatch.org/news/2013/apr/eu-council-smart-borders-8018-13.pdf

[23] Avis du CEPD du 10 juillet 2009 sur la communication de la Commission au Parlement européen et au Conseil intitulée «Un espace de liberté, de sécurité et de justice au service des citoyens», JO 2009/C 276/02.

[24] JO C 83 du 30.3.2010, p. 389.

[25] Conseil de l'Europe, STE n° 5, 4.11.1950.

II. ÉVALUATION GÉNÉRALE DE L'EES

II.1. Article 7 de la Charte: respect de la vie privée et familiale

19. Selon l'article 7 de la Charte, «[t]oute personne a droit au respect de sa vie privée et familiale, de son domicile et de ses communications». Toute limitation de ce droit (comme dans le cas de l'article 8) doit être conforme à l'article 52, paragraphe 1, de la Charte et doit donc être prévue par la loi, respecter le contenu essentiel des droits et libertés reconnus par la Charte, être nécessaire et proportionnée et «[répondre] effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et libertés d'autrui».

20. L'article 7 de la Charte doit être lu en combinaison avec l'article 8 de la CEDH, qui protège la vie privée et familiale de la même manière et ajoute qu'«[i]l ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire» à certaines fins[26].

21. Le principe de proportionnalité est étroitement lié au principe de nécessité. Selon la Cour européenne des droits de l'homme, l'ingérence dans un droit peut être considérée comme nécessaire si elle répond à un besoin social impérieux, si elle est proportionnée au but poursuivi et si les motifs invoqués par les autorités publiques pour la justifier apparaissent pertinents et suffisants[27]. La Cour de justice de l'Union européenne a en outre précisé qu'il convenait de démontrer que les mêmes objectifs ne pouvaient pas être atteints par d'autres moyens moins intrusifs[28].

L'EES constitue-t-il une ingérence? Dans quelle mesure?

22. Il est évident que le stockage habituel de données relatives aux individus et à leurs entrées et sorties du territoire de l'Union européenne révélera aussi souvent, et de nombreuses manières, des informations sur leur vie privée et familiale. La jurisprudence de la Cour européenne des droits de l'homme rappelle que «le simple fait de mémoriser des données relatives à la vie privée d'un individu constitue une ingérence au sens de l'article 8 CEDH»[29]. Pour évaluer le degré d'ingérence, plusieurs aspects peuvent être pris en considération, comme la nature des données, l'étendue de la collecte de données, l'utilisation qui sera faite de ces données ainsi que les éventuels changements de finalité (p.ex. la conservation de données de télécommunications à des fins commerciales et leur réutilisation par les autorités répressives), le transfert des données vers des pays tiers (p.ex. le transfert systématique des dossiers passagers) ou le caractère confidentiel

[26] «…à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui» (voir article 8, paragraphe 2, de la CEDH).
[27] Voir Cour européenne des droits de l'homme, Marper/Royaume-Uni, 4 décembre 2008, requêtes n° 30562/04 et 30566/04.
[28] Voir CJUE, affaires jointes C-92/09 et C-93/09, *Volker und Markus Schecke GbR/Land Hessen; Eifert/Land Hessen*, 9.11.2010.
[29] *Idem*, point 67.

de la collecte et du traitement (voir par exemple les conclusions de la Cour européenne des droits de l'homme dans les affaires Amann et Rotaru[30]).

23. La nature des données à caractère personnel, et en particulier leur caractère sensible, constitue un élément essentiel à prendre en considération. La collecte de données biométriques, par exemple, constitue une ingérence manifeste, comme l'indique la Cour européenne des droits de l'homme dans l'affaire Marper[31], qu'il convient de considérer isolément de la question générale des informations relatives à la vie privée et familiale d'une personne. Le fait que les informations collectées ne concernent pas des personnes soupçonnées d'être dans l'illégalité ou faisant l'objet d'une enquête constitue un autre élément d'ingérence.

24. En ce qui concerne l'EES, le CEPD note que le traitement est réalisé à vaste échelle, vu qu'il concerne tous les visiteurs de courte durée dans l'UE, qui sont des voyageurs non-suspects, et qu'il suppose la collecte de données d'identification, y compris des données biométriques (10 empreintes digitales) sur ces visiteurs. L'accès des autorités répressives aux données est également une possibilité envisagée et le système a été conçu pour le rendre envisageable. Il convient dès lors de conclure que les propositions impliquent une ingérence dans le droit au respect de la vie privée et familiale, avec des implications potentiellement importantes pour les personnes concernées.

L'ingérence est-elle justifiée par une base juridique claire?

25. Le libellé de la législation doit être suffisamment clair pour rendre les ingérences prévisibles. Les circonstances dans lesquelles le droit à la vie privée, à la vie familiale, à son domicile et à sa correspondance peut être limité doivent être explicitement indiquées dans la base juridique[32].

26. Tel est l'objectif de la proposition d'EES, qui vise à fournir un cadre clair pour la collecte, l'utilisation et la conservation de données relatives à des ressortissants d'États tiers, ainsi qu'au sujet de leurs droits à l'information, à l'accès et à la rectification de ces données. Il convient toutefois de définir plus précisément les finalités de la proposition et d'ajouter des garanties supplémentaires, comme nous l'expliquerons ci-après.

La mesure est-elle nécessaire et proportionnée dans une société démocratique pour l'une ou l'autre des finalités reprises à l'article 8, paragraphe 2, de la CEDH ou à l'article 52, paragraphe 1, de la Charte[33]?

27. Le point 9 de cet avis montre que la proposition présente des finalités différentes, qui ne sont pas clairement définies, mais qui sont en tout état

[30] Voir Cour européenne des droits de l'homme, Rotaru/Roumanie, 4 mai 2000, requête n° 28341/95, et Amann/Suisse, 16 février 2000, requête n° 27798/95.
[31] Op. cit.
[32] Voir Cour européenne des droits de l'homme, Kruslin/France, requête n° 11801/85, points 30-33.
[33] C'est-à-dire un intérêt général reconnu par l'Union/nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui.

de cause étroitement liées, avec une importance particulière accordée à la gestion des frontières et à la gestion plus efficace des séjours illégaux. L'évaluation effectuée au titre de l'article 7 devrait tenir compte de ces finalités.

28. Dans un premier temps, le CEPD estime qu'en principe, les bases de données à grande échelle sont créées dans le but de soutenir une politique de l'UE établie, spécifiée dans le droit de l'Union. Toutefois, dans le cas présent, il semblerait que la base de données ait été créée en l'absence d'une politique globale, et même dans le but de déterminer si une telle politique européenne doit être conçue et, si oui, de quelle manière. Cet élément est particulièrement préoccupant, étant donné que l'EES est créé dans le but d'identifier les voyageurs ayant dépassé la durée de séjour autorisée, mais sans qu'une politique européenne claire n'ait été mise au point en ce qui concerne la gestion de ces voyageurs.

29. La proposition indique que l'EES facilitera le calcul de la durée de séjour et, dès lors, l'identification des voyageurs ayant dépassé la durée de séjour autorisée (ce qui est déjà possible, bien que plus difficile, avec le système des tampons[34]). L'une des principales conséquences de l'identification des voyageurs ayant dépassé la durée de séjour autorisée est le refus d'un nouveau visa, lorsque la personne a fini par quitter le territoire de l'UE, puis y retourne. Si cette personne a été trouvée et identifiée sur le territoire de l'UE, le système faciliterait également son *retour* dans son pays d'origine. Toutefois, si l'EES peut faciliter *l'identification* des voyageurs ayant dépassé la durée de séjour autorisée, il ne permet pas de les *localiser* avec précision sur le territoire de l'UE, ni de déterminer les conditions de leur *retour* vers leur pays d'origine[35]. En outre, l'efficacité du système dans une zone entourée de frontières terrestres reste également floue[36]. Selon le CEPD, ces questions auraient dû être abordées comme condition préalable indispensable à l'élaboration de ce système de contrôle des frontières à grande échelle.

30. Dans un deuxième temps, une finalité distincte semble être la facilitation du calcul du dépassement de la durée de séjour et la création de statistiques. Cette finalité ne pourrait être reliée que de manière indirecte avec les finalités reprises à l'article 8, paragraphe 2, de la CEDH, et ne saurait justifier une ingérence dans le droit au respect de la vie privée. Le CEPD émet donc des doutes sur la nécessité et la proportionnalité des ingérences dans le droit au respect de la vie privée prévues par la proposition en ce qui concerne les finalités de l'amélioration du calcul et l'élaboration de statistiques.

[34] Un tampon est systématiquement apposé sur les documents de voyage des ressortissants de pays tiers à l'UE à l'entrée et à la sortie. Lorsqu'un document ne comporte pas de tampon d'entrée, on peut supposer que son titulaire ne remplit pas, ou plus, les conditions de séjour.

[35] Voir, au sujet de la question de savoir si la transmission des données d'identification au pays d'origine est la meilleure solution aux problèmes de rapatriement, surtout en l'absence de coopération du pays tiers, la note du comité Meijers du 3 mai 2013 sur les propositions relatives aux frontières intelligentes, p. 2.

[36] Voir l'analyse d'impact sur la proposition, pp. 14 et 15, également commentée dans l'avis du groupe de travail «Article 29», p. 6.

31. Le CEPD s'interroge dans ce contexte sur la nécessité que les informations permettent d'identifier la personne et pense que des données statistiques anonymes pourraient donner le même résultat[37] et même être encore plus rentables. Il peut être utile, à cette fin, d'examiner les possibilités offertes par le code frontières Schengen[38]. Cet objectif de gestion de la migration devrait également être concilié avec les politiques déjà mises en place en matière de migration, comme le fait remarquer à juste titre le groupe de travail «Article 29» en ce qui concerne «l'approche globale de la question des migrations et de la mobilité»[39].

32. Dans un troisième temps, il convient également d'analyser la question de la nécessité, dans le contexte plus large des systèmes informatiques à grande échelle. Plusieurs systèmes de la sorte ont été développés au cours des dernières années (Eurodac, le VIS et, plus récemment, le SIS II, remplaçant le SIS de première génération[40]), afin d'assurer un contrôle plus efficace des frontières extérieures, comme corollaire de la levée des frontières intérieures pour les personnes voyageant à l'intérieur du territoire de l'Union européenne. Ces systèmes d'information partagent des caractéristiques communes. Ils se composent généralement d'unités nationales et d'une unité centrale, et la supervision des traitements de données est partagée entre les autorités nationales de protection des données et le CEPD.

33. Comme mentionné ci-dessus, le CEPD a appuyé et commenté les conclusions du programme de Stockholm en invitant les parties intéressées à mener une réflexion en profondeur sur ces systèmes, à prendre dûment en considération à la fois les coûts pour la protection de la vie privée et des données, et l'efficacité pour le contrôle des frontières et la sécurité publique. Il a notamment souligné qu'«*il conviendra, dans les années à venir, d'être plus attentif à la mise en œuvre intégrale et efficace et à l'évaluation des instruments existants*»[41]. Dans le présent contexte, l'analyse devrait inclure les instruments proposés comme l'EES et le RTP, mais aussi ceux qui ont déjà été mis en œuvre.

---

[37] Voir CJUE, C-92/09, *op. cit.*

[38] Voir articles 11, paragraphe 2, et 13, paragraphe 5, du code frontières Schengen, invitant les États membres à s'informer mutuellement et à informer la Commission et le secrétariat général du Conseil au sujet de leurs pratiques nationales concernant la présomption de séjour illégal et le renversement de cette présomption au sens de l'article 11; les États membres sont également invités à établir un relevé statistique sur le nombre de personnes ayant fait l'objet d'une décision de refus d'entrée, les motifs du refus, la nationalité des personnes refusées et le type de frontière (terrestre, aérienne, maritime) auquel l'entrée leur a été refusée. Les États membres transmettent ces statistiques à la Commission une fois par an. La Commission publie tous les deux ans une compilation des statistiques communiquées par les États membres.

[39] Développée dans l'avis du groupe de travail «Article 29», p. 10. Voir COM(2011) 743 final.

40 Le système VIS a été lancé en partie en 2011 et se trouve en phase de déploiement dans plusieurs régions du monde. Le 9 avril 2013, le système d'information Schengen de deuxième génération (SIS II) est devenu opérationnel.

Le CEPD renvoie à ses conclusions relatives au contrôle du VIS effectué en 2011, dans lequel plusieurs des problèmes détectés représentaient des risques de sécurité importants dans le fonctionnement du VIS.

http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/VIS/12-06-01_VIS_security_audit_report_summ_EN.pdf

[41] Programme de Stockholm, point 1.2.2.

34. Le CEPD prend note de l'analyse effectuée par la Commission dans l'analyse d'impact de l'EES[42] en ce qui concerne la compatibilité de ce dernier avec les autres systèmes informatiques à grande échelle, et de sa conclusion selon laquelle aucun de ces systèmes ne répond aux exigences administratives visant à gérer le droit de séjour dans l'UE et à identifier et éviter l'immigration irrégulière, surtout en ce qui concerne les voyageurs dépassant la durée de séjour autorisée. Il reste néanmoins quelques zones d'ombre à éclaircir.

35. Si les systèmes existants ne répondent pas totalement aux objectifs du paquet relatif aux frontières intelligentes, ils peuvent tout de même permettre d'en atteindre quelques-uns, et peuvent également être développés pour en atteindre davantage à l'avenir. Par exemple, l'un des grands objectifs du règlement relatif au VIS[43] est d'aider à l'identification des personnes ne remplissant pas les conditions d'entrée, de séjour ou de résidence sur les territoires nationaux. Un signalement pourrait également être introduit, conformément à l'article 24 du règlement SIS II[44].

36. Le principal problème est la faible expérience du fonctionnement de ces systèmes, insuffisante pour pouvoir en tirer des conclusions utiles. L'expérience acquise avec le VIS et les autres systèmes actuels (Eurodac, SIS II) est limitée: le VIS[45], en particulier, n'est pas encore pleinement opérationnel, certains problèmes en matière de protection des données devant encore être gérés au niveau de l'unité centrale[46].

37. Le CEPD a par conséquent des doutes sur le moment choisi pour envisager un nouveau système de contrôle des frontières, avant qu'une évaluation complète des systèmes existants ne puisse effectivement être

[42] Voir pp. 20 et 69-76 de l'analyse d'impact de l'EES.

[43] Le VIS devrait avoir pour objet de faciliter la lutte contre la fraude et de faciliter les contrôles aux points de passage aux frontières extérieures et sur le territoire des États membres. Le VIS devrait également aider à l'identification de toute personne qui ne remplit pas ou ne remplit plus les conditions d'entrée, de présence ou de séjour applicables sur le territoire des États membres et faciliter l'application du règlement (CE) n° 343/2003 du Conseil du 18 février 2003 établissant les critères et mécanismes de détermination de l'État membre responsable de l'examen d'une demande d'asile présentée dans l'un des États membres par un ressortissant d'un pays tiers ainsi que contribuer à la prévention des menaces pesant sur la sécurité intérieure de l'un des États membres.

[44] Voir article 24, paragraphe 3, du règlement SIS II - Conditions auxquelles sont soumis les signalements introduits aux fins de non-admission ou d'interdiction de séjour
«Un 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».

[45] «À la fin de l'année 2011, les risques les plus critiques recensés étaient: a) consommation plus rapide que prévu de la capacité du système due au fait que certains États membres ont déployé le système dans d'autres régions en avance par rapport au déploiement progressif programmé; b) transfert du VIS central depuis le C.SIS vers l'agence européenne chargée de la gestion des systèmes d'information; et c) qualité des empreintes digitales pendant les opérations».
Voir p. 10 du rapport de la Commission au Parlement européen et au Conseil sur le développement du système d'information sur les visas (VIS) en 2011 (présenté conformément à l'article 6 de la décision 2004/512/CE du Conseil).

[46] Voir également note de bas de page 24.

réalisée afin d'assurer la cohérence et d'éviter de reproduire des difficultés déjà rencontrées par le passé.

38. En conclusion, même si *l'objectif* escompté pouvait être considéré comme étant légitime et nécessaire dans une société démocratique, les *mesures législatives* mises en œuvre ne répondent pas totalement aux exigences de l'article 8, paragraphe 2, de la CEDH en ce qui concerne la nécessité et la proportionnalité. Le CEPD considère dès lors que, sans nouvelle évaluation des législateurs,

    a. l'EES ne devrait pas être créé dans le but d'identifier les voyageurs ayant dépassé la durée de séjour autorisée, sans qu'une politique européenne claire n'ait été mise au point en ce qui concerne la gestion de ces voyageurs;

    b. la facilitation du calcul du dépassement de la durée de séjour et la création de statistiques ne sont pas des finalités qui devraient entraîner la création d'une base de données à grande échelle avec des données à caractère personnel;

    c. un EES ne devrait pas être créé avant qu'une évaluation complète des systèmes existants ne puisse effectivement être réalisée afin d'assurer la cohérence et d'éviter de reproduire des difficultés déjà rencontrées par le passé.

39. Dans un deuxième temps, le système devra satisfaire aux garanties spécifiques prévues par l'article 8 de la Charte.

II.2. Article 8 de la Charte: Protection des données à caractère personnel

40. Cette disposition prévoit que «[t]oute personne a droit à la protection des données à caractère personnel la concernant». Elle indique également que les données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi, et que toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification. Le respect de ces règles est soumis au contrôle d'une autorité indépendante. Telles sont les exigences fondamentales établies pour le traitement des données à caractère personnel, qui sont affinées dans les différents instruments juridiques pour la protection des données.

Traitement équitable

41. Les types de mesures devant contribuer à garantir un traitement équitable vont de la transparence générale à la limitation du nombre de données collectées, en passant par des mesures de prévention des discriminations. Le CEPD se félicite du fait que plusieurs dispositions de la proposition visant à garantir que les données collectées ne sont pas excessives (sans préjudice de l'évaluation de l'utilisation des données biométrique, qui fera l'objet d'un chapitre séparé ci-dessous) et du fait que des mesures de

sensibilisation soient prises, notamment en ce qui concerne le personnel chargé du traitement des données[47].

42. Le CEPD attire néanmoins l'attention sur les risques associés au calcul automatisé des dates et sur les décisions qui pourraient être prises à l'encontre de la personne concernée sur la base de ce traitement automatisé. Les conditions dans lesquelles la personne sera informée du fait qu'elle pourrait avoir été enregistrée (à tort) comme un voyageur ayant dépassé la durée de séjour autorisée ne sont toujours pas satisfaisantes, comme expliqué ci-dessous.

Finalité spécifique

43. La ou les finalités d'une mesure visant à traiter des données à caractère personnel doivent être suffisamment claires et précises pour garantir la transparence vis-à-vis des personnes concernées par la mesure. Le degré de spécification tiendra compte de l'étendue et de l'impact du traitement de données: plus celui-ci est intrusif, plus la finalité doit être claire. L'article 4 de la proposition énumère une série de finalités connexes ainsi que certains autres effets que le système cherche également à obtenir.

44. Ces finalités ont déjà été mentionnées plus haut dans le présent avis, mais peuvent être rappelées comme suit:

- les principales finalités, indiquées en termes généraux, sont l'amélioration de la gestion des frontières extérieures de l'UE et de la lutte contre l'immigration irrégulière, la mise en œuvre de la politique de gestion intégrée des frontières, la coopération entre les autorités douanières et celles compétentes en matière d'immigration ainsi que leur consultation mutuelle;
- les moyens disponibles pour réaliser ces finalités sont la fourniture d'un accès aux informations d'entrée et de sortie des ressortissants de pays tiers;
- les autres objectifs sont l'amélioration des vérifications aux frontières, le calcul et la surveillance de la durée de séjour, l'aide à l'identification des voyageurs ayant dépassé la durée de séjour autorisée et, par conséquent, à l'adoption des mesures appropriées, ainsi que la collecte de statistiques.

45. Le CEPD n'a pas d'autres observations à formuler sur les détails de ces finalités. Toutefois, le fait que des finalités doivent être spécifiées signifie également qu'aucun traitement de données ne devrait avoir lieu en dehors du cadre de ces finalités, ce qui pose un problème spécifique en ce qui concerne la réutilisation des données à des fins répressives. Ces finalités sont mentionnées en tant que possibilité ultérieure, après évaluation du système. Dans ses observations sur le programme de Stockholm, le CEPD a appelé à prêter une attention particulière à ce type de réutilisation de données à caractère personnel et a insisté sur l'importance d'une

[47] Voir en particulier l'article 8 relatif à l'utilisation de l'EES et à la prévention de la discrimination, les articles 11 et 12 relatifs à la liste des données à collecter, qui a été partiellement limitée afin de tenir compte de certaines observations du CEPD, l'article 25 relatif à la formation du personnel et l'article 33 relatif à l'information des personnes.

évaluation rigoureuse de la nécessité et de conditions strictes pour l'accès aux données. Cette question sera abordée plus en détail au chapitre III.

Fondement légitime

46. L'EES n'étant de toute évidence pas basé sur le consentement libre et éclairé des personnes concernées, la nécessité d'un fondement légitime établie par la loi porte essentiellement sur le respect ou non, par le système proposé, de l'article 7 de la Charte et de l'article 8 de la CEDH, comme déjà indiqué à la section II.1, les conclusions figurant au point 38. Il convient toutefois également d'insister sur le fait que les principes généraux de la protection des données exigent également que le traitement de données à caractère personnel soit nécessaire et proportionné aux finalités légitimes pouvant être concernées.

Droits de la personne

47. Le CEPD insiste sur la nécessité d'accorder une attention particulière aux conséquences juridiques pouvant découler du traitement automatisé de données à caractère personnel. Si la réalité des faits n'est pas suffisamment prise en considération, les conséquences pour les personnes concernées peuvent se révéler particulièrement négatives.

48. L'article 9 de la proposition d'EES, en particulier, mérite une attention spécifique, vu qu'il dispose qu'à l'expiration de la durée de séjour autorisée, afin de faciliter le calcul de la durée de séjour, le système déterminera automatiquement quelles données d'entrée ne sont pas accompagnées de données de sortie, et en informera les autorités compétentes. Cela soulève une question: comment éviter les erreurs causées par une décision automatisée? Celle-ci pourrait en effet omettre d'enregistrer certaines données de sortie pour diverses raisons (double statut du ressortissant de pays tiers – p.ex. entrée avec un passeport ordinaire et sortie avec un passeport diplomatique -, raisons médicales ou problèmes techniques du système).

49. Par ailleurs, les personnes doivent être pleinement informées, en temps utile, de toute décision prise, afin de pouvoir exercer correctement leurs droits. Cela est d'autant plus nécessaire compte tenu de la multiplication du nombre de bases de données dans le domaine de la gestion des frontières, qui pourrait compliquer de plus en plus la tâche des personnes cherchant à exercer leurs droits. Le CEPD estime que les dispositions suivantes pourraient être modifiées afin d'améliorer les droits des personnes dans ce contexte.

Droit à l'effacement (article 21, paragraphe 2)

50. Le CEPD se félicite de l'obligation imposée aux États membres d'effacer immédiatement les données à caractère personnel relatives à un ressortissant de pays tiers ayant dépassé la durée de séjour autorisée lorsque la personne concernée apporte la preuve qu'un événement grave et imprévisible l'a contrainte à dépasser la durée de séjour autorisée. Il considère néanmoins qu'il convient de préciser que les personnes

concernées devraient être informées de ce droit et devraient disposer de moyens de recours juridique lorsqu'il n'est pas respecté (voir recommandations ci-dessous).

Information de la personne concernée (article 33)

51. Le CEPD propose d'ajouter à l'article 33, paragraphe 1, une disposition selon laquelle les voyageurs dépassant la durée de séjour autorisée «*sont informés de ce qui suit par l'État membre responsable* ***de l'introduction de leurs données***». Sans cet ajout, les critères d'identification de l'État membre responsable resteraient flous.

52. Le CEPD suggère également d'inclure des informations sur:

- le traitement automatisé des données visant à calculer la durée de séjour;
- le fait qu'un séjour dépassant la durée autorisée entraînera la publication des données à caractère personnel de la personne sur une liste de voyageurs ayant dépassé la durée de séjour autorisée;
- les catégories de destinataires de cette liste;
- le droit d'obtenir l'effacement de ses données à caractère personnel lorsqu'il est prouvé que la durée de séjour autorisée a été dépassée en raison d'un événement grave et imprévisible;
- le droit de recevoir des informations sur les procédures à suivre pour exercer ses droits ainsi que sur les recours juridiques existants, y compris les dispositifs permettant à la personne concernée de faire entendre son point de vue, compte tenu du caractère automatisé du traitement des données.

53. Le CEPD note également avec satisfaction que les informations doivent être fournies par écrit (article 33, paragraphe 2), mais recommande d'ajouter: «sous une forme intelligible, en utilisant un langage simple et clair, adapté à la personne concernée», comme prévu à l'article 11, paragraphe 1, de la proposition de règlement sur la protection des données[48]. Des traductions de ces informations devraient être disponibles pour les ressortissants de pays tiers ne comprenant pas la langue de l'État membre responsable.

Voies de recours (article 36)

54. L'article 36 prévoit des modalités de recours en cas de refus du droit d'accès, de rectification et/ou d'effacement établi à l'article 35. Il est néanmoins difficile de savoir si cette disposition inclut la suppression de données visée à l'article 21, paragraphe 2. Le CEPD recommande par conséquent de modifier l'article 35 (ou l'article 36) afin de faire en sorte que les voies de recours judiciaire couvrent également la situation visée à l'article 21, paragraphe 2.

[48] Proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données), COM (2012) 11 final.

Surveillance par des autorités indépendantes (articles 37-39)

55. Le CEPD prend note avec satisfaction des dispositions relatives à la surveillance des opérations de traitement de données. Les responsabilités au niveau national et au niveau européen sont dûment prises en considération, et un système est établi afin d'assurer la coordination entre toutes les autorités concernées de protection des données, et ce sur la base de l'expérience acquise et de mécanismes existants, éprouvés et fiables. Le CEPD se tient prêt à assurer ses obligations en ce qui concerne l'EES (et le RTP).

56. Le CEPD prend note des responsabilités des différentes parties prenantes à l'intérieur du cadre des frontières intelligentes, à savoir la Commission, eu-Lisa et les États membres. Ces responsabilités engendrent parallèlement d'autres responsabilités pour les autorités de protection des données au niveau européen et national.

57. Cette répartition des compétences nécessite une coopération à plusieurs niveaux, entre responsables de traitements de données, entre autorités de protection des données ainsi qu'entre autorités et responsables de traitements, afin d'éviter d'éventuelles zones d'ombre.

58. Le CEPD se félicite du modèle de contrôle coordonné prévu à l'article 39 de la proposition en ce qui concerne la surveillance, de manière à garantir l'interprétation et l'application cohérentes du règlement. Il estime que cette approche devrait être complétée par une répartition claire des compétences au niveau national, afin de veiller à ce que les personnes concernées fassent valoir leurs droits auprès de l'autorité compétente. Il conviendrait à cet égard que l'identification de l'État membre responsable soit précisée et transparente pour le public, comme déjà indiqué au point 51.

III. OBSERVATIONS SPÉCIFIQUES SUR L'EES

III.1. Données biométriques

59. Les propositions se basent sur l'utilisation d'éléments biométriques (empreintes digitales). Le CEPD observe que conformément aux options d'action envisagées dans l'analyse d'impact[49], la Commission suppose que les empreintes digitales seront ajoutées automatiquement trois ans après la mise en service de l'EES.

60. Le CEPD souligne la nécessité de démontrer que l'utilisation de données biométriques dans ce contexte, qui constitue une nouvelle ingérence dans le droit au respect de la vie privée, est «nécessaire dans une société démocratique» et qu'aucune autre méthode moins intrusive n'est disponible. Dans l'affaire S. et Marper, la Cour européenne des droits de l'homme a considéré que les empreintes digitales et les photographies

[49] Voir pp. 26-39 de l'analyse d'impact de l'EES.

contenaient des informations uniques «susceptibles d'affecter la vie privée d'un individu» et que la conservation de ces informations sans le consentement de la personne concernée «ne saurait être considérée comme neutre ou insignifiante»[50]. Le traitement de ces informations devrait également être accompagné de garanties strictes et prendre en considération le risque d'erreur.

61. Le CEPD aurait dès lors préféré qu'une évaluation ex ante ait été effectuée, également sur l'introduction d'éventuelles garanties, au lieu d'adopter d'ores et déjà une décision définitive visant à introduire les données biométriques dans le système. Le CEPD recommande de modifier le texte de la proposition dans ce sens. Plus précisément, la Commission devrait entreprendre une analyse d'impact ciblée sur les données biométriques (empreintes digitales) au lieu de prévoir l'introduction automatique de celles-ci comme indiqué dans la proposition actuelle (article 12). Le CEPD suggère d'en faire une obligation incluse dans l'article 12, paragraphe 5, de la proposition d'EES.

62. À l'appui de cette recommandation, le CEPD prend note de ce qui se passe aux États-Unis, où un récent rapport préliminaire de l'Office gouvernemental des comptes mentionne les problèmes liés à la planification des infrastructures de sortie biométriques[51]. Il évoque des questions importantes telles que l'efficacité des actuels processus biographiques pour les départs aériens, les taux d'erreur de la collecte ou de la mise en correspondance de données, la valeur ajoutée qu'apporterait un système biométrique pour les départs aériens par rapport à l'actuel processus biographique pour les départs aériens, ainsi que la valeur et le coût globaux d'un dispositif biométrique pour les départs aériens. Ce projet d'élaboration d'un système biométrique pour les départs mis au point par les États-Unis est toujours en cours d'analyse.

63. Le CEPD voudrait également attirer l'attention sur la base de données australienne Movement Reconstruction, qui pourrait donner un autre exemple de système similaire fonctionnant uniquement à partir de données alphanumériques[52]. Ces «registres de mouvements» peuvent inclure le nom du voyageur, sa date de naissance, son sexe et son état civil, son pays de naissance, la date de son départ et/ou de son arrivée, le numéro et le pays de son document de voyage, le code de port et les informations sur son vol/navire, la sous-catégorie de visa et la date d'expiration de celui-ci, ainsi que le nombre de déplacements effectués.

---

[50] La Cour a également indiqué qu'une conservation générale et indifférenciée des «empreintes digitales, échantillons biologiques et profils ADN» de personnes non reconnues coupables d'infractions «ne traduisait pas un juste équilibre entre les intérêts publics et privés concurrents en jeu»; Cour européenne des droits de l'homme, S. et Marper/Royaume-Uni, *op. cit*, point 125.

[51] *Preliminary Observations on DHS's Overstay Enforcement Efforts*, disponible à l'adresse suivante: http://www.gao.gov/assets/660/654752.pdf.

[52] Plus d'informations à l'adresse suivante: http://www.immi.gov.au/managing-australias-borders/border-security/systems/movement-records.htm.

64. Par ailleurs, le CEPD a reconnu à plusieurs reprises les avantages apportés par l'utilisation des données biométriques, tout en soulignant que ces avantages dépendraient de l'application de garanties strictes.

65. Dans son avis sur le SIS II[53], le CEPD a proposé une liste non exhaustive d'obligations ou d'exigences communes devant être respectées lors de l'utilisation de données biométriques dans un système, notamment la réalisation d'une analyse d'impact ciblée, une importance spécifique accordée à la procédure d'enregistrement et au niveau de précision ainsi qu'une procédure de secours. Ces éléments contribueront à éviter que le ressortissant de pays tiers doive porter le poids des imperfections du système, comme les conséquences d'une erreur d'identification ou d'un échec d'enregistrement. Dans ce contexte, le CEPD se félicite de l'article 12, paragraphe 3, de la proposition d'EES, qui tient compte des personnes pour lesquelles le relevé des empreintes digitales est physiquement impossible.

66. En outre, le CEPD note que 10 empreintes digitales seront prélevées, au lieu de deux ou quatre, alors qu'à des fins de vérification, cela serait suffisant. Prélever d'emblée 10 empreintes digitales ne serait nécessaire qu'à condition de poursuivre un objectif différent, à savoir l'identification de traces dans un contexte répressif. Le CEPD considère qu'une collecte de données biométriques d'une telle ampleur ne devrait pas être prévue d'emblée, alors que l'évaluation d'un éventuel accès des autorités répressives à ces données ne devrait avoir lieu que deux ans après l'entrée en vigueur du système.

III.2. Accès des autorités répressives aux données

67. Le CEPD note que la proposition d'EES n'autorise pas en principe les autorités répressives à accéder à l'EES; cet accès n'est possible qu'à l'issue d'une période d'évaluation. La proposition prévoit que la première évaluation de l'EES traitera spécifiquement de la question de l'accès aux données à des fins répressives, notamment des conditions de cet accès, de la période de conservation et de l'accès des autorités de pays tiers.

68. L'accès à l'EES s'inscrirait non seulement dans une tendance générale visant à accorder aux services répressifs l'accès à de nombreux systèmes d'information et d'identification à grande échelle (voir par exemple l'accès à Eurodac[54]), mais constituerait également un pas supplémentaire

[53] Avis du 19 octobre 2005 sur trois propositions relatives au système d'information Schengen de deuxième génération (SIS II) [COM(2005) 230 final, COM(2005) 236 final et COM(2005) 237 final] (JO C 91 du 19.4.2006, p. 38).

[54] Voir le règlement (UE) n° 603/2013 du Parlement européen et du Conseil du 26 juin 2013 relatif à la création d'Eurodac pour la comparaison des empreintes digitales aux fins de l'application efficace du règlement (UE) n° 604/2013 établissant les critères et mécanismes de détermination de l'État membre responsable de l'examen d'une demande de protection internationale introduite dans l'un des États membres par un ressortissant de pays tiers ou un apatride et relatif aux demandes de comparaison avec les données d'Eurodac présentées par les autorités répressives des États membres et Europol à des fins répressives, et modifiant le règlement (UE) n° 1077/2011 portant création d'une agence européenne pour la gestion opérationnelle des systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice (refonte), JO L 180/1 du 29.6.2013.

dans une tendance visant à accorder à ces services l'accès à des données sur des personnes qui en principe ne sont soupçonnées d'aucune infraction.

69. Le CEPD estime que l'introduction de la possibilité pour les autorités répressives d'accéder à l'EES - ce qui constituerait une nouvelle ingérence dans le droit au respect de la vie privée ainsi qu'une violation du principe essentiel de limitation de la finalité établi par la législation sur la protection des données - devrait être basée sur une évaluation en bonne et due forme démontrant clairement la nécessité de cet accès. En particulier, la valeur ajoutée précise de cet accès par rapport à l'accès aux bases de données biométriques existantes devrait être établie, et il convient également de prouver que la nécessité passe outre à l'intrusion dans la vie privée des individus. Le CEPD rappelle que les personnes dont les données sont conservées dans l'EES ne sont en principe soupçonnées d'aucune infraction et ne devraient pas être traitées comme telles, étant donné que le système a été conçu principalement comme un outil de calcul de la durée de séjour des ressortissants de pays tiers.

70. Si l'accès s'avérait nécessaire, il conviendrait d'instaurer des conditions strictes en exigeant, par exemple, que les données soient proportionnées, étroitement ciblées et fondées sur des suspicions concernant des personnes déterminées.

III.3. Transfert de données à destination de pays tiers

71. Selon le CEPD, les raisons pour lesquelles le transfert de données de l'EES vers des pays tiers est nécessaire au retour des ressortissants de ces pays devraient être davantage explicitées.

72. Le CEPD se félicite que le transfert soit en principe interdit, et que l'article 27, paragraphe 2, contienne un certain nombre de conditions, dans le cas où une dérogation s'appliquerait. Toutefois, selon lui, le transfert de données à caractère personnel conservées dans l'EES à destination de pays tiers, d'organisations internationales ou de parties privées[55] aux fins de prouver l'identité de ressortissants de pays tiers et aux fins du retour est formulé de manière trop large. Le CEPD comprend la nécessité d'échanger certaines données avec un pays tiers lorsque le retour de la personne concernée l'exige, mais la proposition n'indique pas clairement dans quelles conditions et pour quelles finalités les pays tiers seront autorisés à demander des preuves de l'identité d'un ressortissant de pays tiers.

73. Une disposition similaire figurant dans le règlement VIS[56], le CEPD recommanderait également au législateur européen d'attendre des éléments expliquant comment la disposition du VIS est concrètement

[55] Voir article 27, paragraphe 2.
[56] Voir article 30, paragraphe 2, du règlement (CE) n° 767/2008 du Parlement européen et du Conseil du 9 juillet 2008 concernant le système d'information sur les visas (VIS) et l'échange de données entre les États membres sur les visas de court séjour (règlement VIS).

appliquée, puis d'étudier la possibilité d'appliquer également à l'EES les exceptions figurant actuellement à l'article 27, paragraphe 2.

IV. AUTRES OBSERVATIONS SUR L'EES

Définition de personne ayant dépassé la durée de séjour autorisée

74. L'article 5, paragraphe 13, définit la notion de «personne ayant dépassé la durée de séjour autorisée» comme se rapportant à 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. Il n'est pas évident de déterminer si la définition est censée couvrir uniquement le cas de figure dans lequel un ressortissant de pays tiers est entré légalement sur le territoire de l'UE, mais a dépassé la durée de séjour autorisée, ou également le cas de figure dans lequel le ressortissant de pays tiers n'a pas respecté les conditions de séjour établies dans le code frontières Schengen (visa et documents de voyage valides, moyens de subsistance suffisants, etc.)[57]. Cela pourrait avoir des conséquences juridiques différentes pour les personnes qui ont dépassé leur période légale de séjour dans l'UE et pour celles qui n'ont pas respecté les conditions établies pour entrer légalement sur le territoire de l'UE, mais n'ont pas dépassé la période légale de 90 jours sur une quelconque période de 180 jours. Le CEPD suggère que la Commission clarifie cette définition.

Vérification de l'identité

75. L'article 18, paragraphe 1, permet l'accès aux données afin de vérifier l'identité du ressortissant de pays tiers et/ou si les conditions d'entrée ou de séjour sur le territoire des États membres sont remplies. Le libellé de cette disposition est trop large. En particulier, l'utilisation du mot «ou» pourrait indiquer que les données à caractère personnel peuvent être utilisées à des fins de vérification de l'identité indépendamment de la vérification des conditions relatives à la durée de séjour. Afin d'éviter tout risque d'accès aux données par des autorités non spécifiquement compétentes en matière d'immigration et pour des finalités sans rapport, le CEPD recommande au législateur européen de supprimer le mot «ou» et de garder associées les deux conditions (vérification de l'identité et des conditions de séjour).

Conservation des données relatives aux personnes ayant dépassé la durée de séjour autorisée

76. Le CEPD se félicite, comme établi à l'article 20, qu'une période maximale de six mois pour la conservation des données dans l'EES soit fixée. En ce qui concerne la période de conservation de cinq ans prévue pour les données relatives aux voyageurs ayant dépassé la durée de séjour autorisée, ni l'analyse d'impact, ni la proposition n'explique la raison

[57] Voir l'article 5, paragraphe 1, du règlement (CE) n° 562/2006 du Parlement européen et du Conseil du 15 mars 2006 établissant un code communautaire relatif au régime de franchissement des frontières par les personnes (code frontières Schengen), JO L 105/1 du 13.4.2006.

justifiant cette période, qui semble disproportionnée par rapport à l'objectif recherché. Le CEPD recommande au législateur de l'UE de mieux justifier, dans un considérant, la nécessité de conserver pendant si longtemps les données relatives aux voyageurs ayant dépassé la durée de séjour autorisée ou de limiter sensiblement cette période.

Statistiques anonymes

77. L'article 40 permet aux autorités compétentes d'accéder à certaines catégories de données à des fins de notification et d'établissement de statistiques «sans permettre l'identification». L'utilisation de l'expression «sans permettre l'identification» engendre de la confusion, étant donné que certaines des catégories de données auxquelles l'accès est accordé permettront – du moins indirectement, surtout lorsque les données sont associées – l'identification des personnes concernées. En outre, l'objectif de «notification» mentionné à l'article 40 devrait être clarifié (qu'est-ce qui doit être notifié, par qui, à qui, et à quelle fréquence). Le CEPD recommande par conséquent au législateur de l'UE d'indiquer le texte suivant: «à des fins de notification et d'établissement de statistiques *anonymes*», ainsi que de définir le sens de la «notification» dans un considérant.

V. OBSERVATIONS SUR LA PROPOSITION DE RTP

Objectif de la proposition et rôle du consentement

78. Le RTP a été conçu pour accélérer le franchissement des frontières pour les voyageurs qui ont déjà fait l'objet d'un contrôle de sûreté. Le système est basé sur des contrôles d'identité et des barrières de passage aux frontières automatisés, dans le but de réduire ou d'éliminer la nécessité pour les gardes-frontières de vérifier les documents de voyage. Selon la proposition de RTP, le système doit être établi sur une base volontaire: les voyageurs effectuant de fréquents déplacements se verront offrir la possibilité de demander un franchissement plus rapide des frontières[58].

79. Le consentement du voyageur est présenté comme le motif légitimant le traitement de données à caractère personnel. Pour être valide, ce consentement doit être «libre, spécifique et informé»[59]. Comme indiqué dans l'avis 15/2011 du groupe de travail «Article 29»[60], le consentement ne peut être valable que si la personne concernée est véritablement en mesure d'exercer un choix et s'il n'y a pas de risque de coercition ou de conséquences négatives importantes si elle ne donne pas son consentement. Si les conséquences du consentement sapent la liberté de choix des personnes, le consentement n'est pas libre.

[58] Ibid, p. 5.
[59] Voir article 2, point h), de la directive 95/46/CE.
[60] Groupe de travail «Article 29», avis n° 15/2011 sur la définition du consentement, adopté le 13 juillet 2011. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf

80. La mise en place de l'EES et la mise en œuvre complète du VIS[61] sont susceptibles d'augmenter le temps consacré aux vérifications aux frontières, ce qui amènerait les voyageurs fréquents à privilégier le RTP. Dans ce contexte, il convient de faire en sorte que le consentement puisse effectivement être considéré comme une base juridique valide pour le traitement. En outre, le fait que le système soit de nature volontaire ne préjuge pas de l'évaluation de sa nécessité et de sa proportionnalité, ni du fait que son développement et son fonctionnement ne dépendent d'un autre système, à savoir l'EES.

81. Il semblerait également que le RTP impose des charges administratives demandant beaucoup de temps aux voyageurs fréquents, du moins au moment de l'enregistrement, vu qu'ils devront donner une fois de plus leurs empreintes digitales à une autre fin et fournir une fois de plus les documents administratifs requis par l'article 9 de la proposition de RTP. En outre, leurs données alphanumériques et biométriques resteront 5 ans dans le système afin de permettre de vérifier l'historique de voyage en utilisant une approche centrée sur la personne. Le niveau d'efficacité du fonctionnement pratique du RTP n'est toujours pas évident.

Le RTP et les risques éventuels de discrimination

82. Le RTP nécessite que tous les participants aient fait l'objet d'un contrôle documentaire et d'un contrôle de sûreté préalables. Les critères de contrôle sont dès lors essentiels. comme le souligne également l'exposé des motifs, qui indique que «*le paragraphe 2 (de l'article 12) est crucial car il établit les critères d'examen des voyageurs enregistrés*»[62]. L'examen des documents justificatifs devant être présentés par le demandeur et des conditions que doivent évaluer les autorités chargées des visas ou des frontières semble indiquer que les critères de contrôle pour le RTP ont été alignés sur ceux utilisés pour l'examen des demandes de visas à entrées multiples[63]. Le CEPD se dit satisfait que les critères des deux instruments aient été alignés.

83. Toutefois, la finalité de la proposition, comme indiqué à son article 2, est de «faciliter le franchissement des frontières extérieures de l'Union européenne par les ressortissants de pays tiers voyageant fréquemment et ayant fait l'objet d'un contrôle de sûreté préalable». Un risque de discrimination peut exister[64], vu que seuls les voyageurs passant des étapes spécifiques, en se soumettant à un enregistrement ad hoc et en

[61] Ibid., p. 16.
[62] p. 10.
[63] Voir articles 14, 21 et 24 du code des visas.
[64] Voir également les observations préliminaires du CEPD sur trois communications de la Commission sur la gestion des frontières [COM (2008) 69, COM (2008)68 et COM (2008)67], 3 mars 2008, http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2008/08-03-03_Comments_border_package_EN.pdf;
et l'avis du 7 juillet 2011 sur la communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions sur la migration, JO C 34/02 du 8.2.2012, p. 18;
http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2011/11-07-07_Migration_FR.pdf

présentant des informations détaillées, seraient considérés comme des voyageurs «à faible risque», tandis que le grand nombre de voyageurs qui ne voyagent pas suffisamment souvent pour se soumettre à un enregistrement, ou dont les empreintes digitales sont illisibles[65], seraient donc implicitement placés de fait dans la catégorie des voyageurs «à risque plus élevé».

84. L'analyse d'impact indique que le problème potentiel de la discrimination se pose surtout si le contrôle de sûreté est trop strict. Cette question devrait dès lors être intégrée au programme de formation aux droits fondamentaux organisé par Frontex pour les gardes-frontières. Il convient d'indiquer clairement, comme indiqué dans l'analyse d'impact, que les personnes n'utilisant pas le contrôle automatisé aux frontières ne sont pas considérées comme des voyageurs présentant un risque[66]. Afin de sensibiliser le grand public, cette question devrait également être abordée lors de la campagne d'information organisée avant que le RTP ne devienne opérationnel. Les brochures et affiches devraient clairement indiquer que les voyageurs sont libres de choisir d'introduire ou non une demande pour le RTP et d'utiliser ou non le contrôle automatisé aux frontières. Le CEPD estime que dans une certaine mesure, ces initiatives pourraient aider à éviter le risque de stigmatisation.

Critères subjectifs d'évaluation

85. Les articles 5 et 9 mentionnent tous deux le critère d'«intégrité et de fiabilité» pour le demandeur. Afin de garantir la sécurité juridique et l'égalité de traitement, les critères subjectifs tels que «s'il est connu desdites autorités pour son intégrité et sa fiabilité» devraient être supprimés ou remplacés par des critères plus objectifs permettant une application cohérente dans toute l'UE.

Catégories de données à collecter

86. La proposition mentionne, aux articles 12 et 15, l'obligation, pour les autorités chargées des visas ou des frontières, de vérifier que le demandeur n'est pas considéré comme constituant une menace pour l'ordre public, la sécurité intérieure ou la santé publique, ou pour les relations internationales de l'un des États membres, et, en particulier, qu'il ne fait pas l'objet, pour ces mêmes motifs, d'un signalement dans les bases de données nationales des États membres [articles 12, paragraphe 2, point h), et 15, paragraphe 1, point d)]. Le CEPD recommande de préciser les modalités de cette vérification, les types d'informations que les autorités chargées des visas ou des frontières doivent prendre en considération, avec ou sans interconnexion des bases de données, ainsi que les incidences de ces traitements.

87. La proposition devrait également prévoir un mécanisme permettant de traiter les demandes et requêtes des personnes, dans le but d'éviter qu'un

[65] Voir l'article 8 et l'exposé des motifs de la proposition n'autorisant aucune exemption à la collecte de données biométriques.
[66] Voir p. 39 de l'analyse d'impact.

individu n'introduise des demandes simultanées dans différents États membres, avec éventuellement des réponses différentes. Le registre central, censé être utilisé pour les demandes selon l'article 24, pourrait être vérifié afin d'éviter ces traitements multiples de demandes.

Interdiction des transferts internationaux

88. Le CEPD accueille avec satisfaction l'article 42, lequel dispose explicitement qu'en toute circonstance, il est interdit de communiquer à des pays tiers ou organisations internationales ou de mettre à leur disposition des données traitées dans le registre central ou pendant l'examen des demandes.

VI. RECOMMANDATIONS DE SÉCURITÉ POUR L'EES ET LE RTP

89. Conformément à l'article 23 de la proposition d'EES et à l'article 37 de la proposition de RTP, la Commission sera tenue d'adopter les mesures nécessaires à l'élaboration et à la mise en œuvre technique des systèmes requis. EU-Lisa, l'agence chargée des systèmes d'information à grande échelle, sera responsable du reste des travaux de mise en place de ces systèmes.

90. La mise en place de systèmes comme l'EES ou le RTP est souvent complexe et nécessite l'adoption d'une méthodologie adéquate afin de garantir un résultat de haute qualité. Généralement, avant de concevoir ou de mettre en œuvre l'une ou l'autre composante de ces systèmes, les méthodologies de développement efficaces commencent par analyser les besoins afin de pouvoir gérer toutes les exigences. Ces méthodologies peuvent être liées à des besoins fonctionnels, à des besoins en matière de protection des données, à des besoins de sécurité ou à d'autres besoins, et doivent être définies, soigneusement décrites et documentées de manière à pouvoir être mises en œuvre en utilisant l'approche coûts/bénéfices la plus efficace possible. Par ailleurs, la phase d'analyse constitue une étape essentielle au cours de laquelle les notions de «respect de la vie privée dès la conception»[67] et de «respect de la vie privée par défaut»[68] doivent être prises en considération. En outre, une analyse adéquate permettra de comprendre comment les exigences s'adaptent mutuellement et de faire en sorte que les différentes exigences n'aient pas des conséquences négatives significatives les unes sur les autres.

91. Le CEPD recommande de veiller à ce que les propositions incluent l'exécution d'une véritable analyse des besoins avant la conception ou la mise en œuvre d'une quelconque partie du système. Cette analyse devrait être réalisée conjointement par la Commission et l'Agence de manière à garantir que toutes les exigences sont bien gérées et qu'elles n'entrent pas mutuellement en conflit.

[67] Intégrer le respect de la vie privée à tous les éléments, dès le début du déploiement d'un système.
[68] Élaborer par défaut les activités de la manière la plus respectueuse de la vie privée possible.

Développement et gestion opérationnelle

92. L'article 24 de la proposition d'EES et l'article 38 de la proposition de RTP disposent que l'Agence sera responsable du développement des différentes parties de chaque système. Le développement est défini aux articles 24, paragraphe 1, du règlement EES et 38, paragraphe 1, du règlement RTP comme étant «l'élaboration et la mise en œuvre des spécifications techniques, en la réalisation d'essais et en la coordination générale du projet».

93. Pendant les phases d'essai du développement d'un système, et afin de détecter les erreurs de développement, des données (appelées «données d'essai») doivent être utilisées afin de vérifier si le logiciel nouvellement développé se comporte ou non comme attendu. Les données d'essai devraient par conséquent présenter les mêmes caractéristiques que les données «réelles» (données à caractère personnel provenant de personnes qui seront traitées par l'EES). On y parvient généralement en examinant les «vraies» données et en constituant un ensemble de données d'essai qui y ressemblent sans divulguer la moindre donnée à caractère personnel.

94. Toutefois, l'article 24, paragraphe 1, du règlement EES et l'article 38, paragraphe 1, du règlement RTP ne précisent pas ce que l'Agence peut faire ou non avec les «vraies» données dans le cadre de la mise en place du système, p.ex. lors des essais, de la vérification, de la validation ou de la migration test vers les nouvelles versions du système. Il conviendrait d'indiquer clairement dans ces dispositions que les données à caractère personnel ne doivent pas être utilisées à de telles fins.

95. Les articles 24, paragraphe 2, du règlement EES et 38, paragraphe 2, du règlement RTP fixent la disponibilité de la plateforme à 24 heures par jour, sept jours par semaine, ce qui prouve que ces systèmes revêtent une importance critique et ne doivent en aucun cas arrêter de fonctionner. La création d'un système nécessite un plan de maintien des activités expliquant comment l'organisation doit réagir en cas d'incident afin de garantir que les opérations restent sous contrôle même dans les cas de perturbations les plus graves. La nécessité d'un plan de maintien des activités devrait dès lors être incluse à l'article 24, paragraphe 2, du règlement EES ainsi qu'à l'article 38, paragraphe 2, du règlement RTP, et une base juridique devrait être établie pour la mise en œuvre des mesures contenant les modalités de ce plan.

Responsabilités nationales

96. Les suggestions formulées ci-dessus sont également applicables aux États membres lorsqu'ils élaborent leur système national. Les données à caractère personnel ne devraient pas être utilisées pour les essais, la vérification, la validation ou la migration test vers de nouvelles versions de leur système national, comme devrait l'indiquer l'article 25 du règlement EES et l'article 39 du règlement RTP.

Sécurité des données

97. Le CEPD est satisfait que l'article 28 du règlement EES et l'article 43 du règlement RTP visent à garantir un niveau de sécurité suffisant pour protéger les données de l'EES et du RTP contre les menaces. Toutefois, l'élaboration des mesures devrait être basée sur un processus continu de gestion et de surveillance des risques liés aux informations. Ce processus continu – souvent appelé «gestion des risques pour la sécurité des informations» – vise à recenser, évaluer et hiérarchiser les risques pour les informations de l'organisation et à définir et mettre en œuvre des mesures de sécurité afin de ramener les risques à un niveau adapté aux besoins et acceptable pour l'Agence et les États membres. La gestion des risques pour la sécurité des informations permet également que le contexte dans lequel les données sont traitées et les systèmes sont utilisés soit clairement compris (également en ce qui concerne les besoins en matière de protection des données); ainsi, une série de contrôles de sécurité rentables peuvent être sélectionnés et mis en œuvre afin de parvenir au niveau de sécurité adéquat.

98. Le CEPD recommande par conséquent de préciser à l'article 28 du règlement EES, ainsi qu'à l'article 43 du règlement RTP, que les pratiques en matière de gestion des risques pour la sécurité des informations doivent être utilisées afin de définir les mesures techniques et organisationnelles appropriées pour protéger l'ensemble des données pertinentes, en tenant compte de tous les besoins en matière de protection des données. Il convient d'inclure une obligation visant à garantir la sécurité grâce à l'adoption de pratiques adéquates en matière de gestion des risques pour la sécurité des informations basées sur

- des normes internationales reconnues;
- des contrôles réguliers de toutes les analyses effectuées dans ce contexte;
- le contrôle et le suivi de toutes les mesures techniques et organisationnelles mises en œuvre dans ce contexte; et
- une intense collaboration entre l'Agence et les États membres, afin de gérer les risques pour la sécurité au-delà des frontières des systèmes d'information.

99. Par ailleurs, en ce qui concerne les mesures spécifiques reprises à l'article 28 du règlement EES et à l'article 43 du règlement RTP:

- à l'article 28, paragraphe 2, point a), du règlement EES, et à l'article 43, paragraphe 2, point a), du règlement RTP, «critiques» devrait être remplacé par «pertinentes»;
- à l'article 28, paragraphe 2, point f), du règlement EES, et à l'article 43, paragraphe 2, point f), du règlement RTP, l'expression «uniquement […] grâce à des modes d'accès confidentiels» devrait être explicitée;
- à l'article 28, paragraphe 2, point g), du règlement EES, et à l'article 43, paragraphe 2, point g), du règlement RTP, il convient d'ajouter: «rendre disponibles leurs profils ainsi que toute autre information pertinente nécessaire aux autorités aux fins de l'exercice du contrôle»;

- à l'article 28, paragraphe 2, point i), du règlement EES, et à l'article 43, paragraphe 2, point i), du règlement RTP, il convient de veiller à ce que les fichiers journaux, ainsi que les données auxquelles ils font référence, soient protégés;
- afin de garantir le contrôle de l'efficacité des mesures de sécurité, l'article 28, paragraphe 2, point k), du règlement EES et l'article 43, paragraphe 2, point k), du règlement RTP devraient inclure non seulement l'audit (qui consiste à donner une image de la situation à un moment précis), mais aussi l'observation en temps réel du système au moyen d'outils spécialisés; ces deux dispositions devraient être reformulées afin d'établir une différence nette entre ces deux concepts et de les appliquer correctement;
- l'article 28, paragraphe 3, du règlement EES et l'article 43, paragraphe 3, du RTP devraient également inclure des mesures à adopter par l'Agence afin de garantir la disponibilité du système, comme indiqué à l'article 24 du règlement EES et à l'article 38 du règlement RTP, ainsi que ses sauvegardes;
- l'article 28, paragraphe 3, du règlement EES et l'article 43, paragraphe 3, du règlement RTP devraient également mentionner le plan de maintien des activités (voir ci-dessus).

100. En ce qui concerne les incidents de sécurité, l'article 28 du règlement EES et l'article 43 du règlement RTP devraient également inclure:

- la nécessité pour l'Agence et les États membres de se mettre d'accord sur un mécanisme commun d'évaluation pour les incidents de sécurité;
- la nécessité pour l'Agence et les États membres de gérer les incidents de sécurité, en suivant un processus documenté, ainsi qu'en gardant un historique de tous les incidents de sécurité et de leur résolution;
- la nécessité que les États membres informent leurs autorités de surveillance nationales ainsi que l'Agence des incidents graves de sécurité détectés sur leur système;
- la nécessité que toutes les parties collaborent en cas d'incident de sécurité;
- la nécessité que l'Agence informe les États membres concernés, la ou les autorités de surveillance nationales correspondantes et le CEPD en cas d'incident grave de sécurité.

Établissement de relevés

101. En ce qui concerne l'article 30, paragraphe 2, du règlement EES et l'article 45 du règlement RTP, il convient de noter que i) les fichiers-journaux utilisés pour la sécurité des données et ii) ceux utilisés pour effectuer la surveillance et l'audit, ainsi que pour vérifier que les données à caractère personnel ont bien été traitées conformément aux règles sont différents. Le CEPD recommande de scinder ces registres en deux ensembles (l'un pouvant être un sous-ensemble de l'autre), afin d'éviter de divulguer au personnel de sécurité des données à caractère personnel figurant dans le système. Ces registres devraient par ailleurs être protégés contre tout accès non autorisé et contre toute modification non autorisée.

VII. CONCLUSIONS

102. Le paquet relatif aux frontières intelligentes vise à créer un nouveau système informatique à grande échelle afin de compléter les mécanismes de contrôle des frontières existants. La licéité de ce système doit être évaluée sur la base des principes de la Charte, en particulier de son article 7 relatif au droit au respect de la vie privée et familiale et de son article 8 relatif à la protection des données à caractère personnel, et ce dans le but d'évaluer non seulement les ingérences du nouveau système dans les droits fondamentaux, mais aussi les garanties incluses dans les propositions en matière de protection des données.

103. De ce point de vue, le CEPD confirme que le système d'EES proposé constitue une ingérence dans le droit au respect de la vie privée et familiale. S'il est satisfait des garanties apportées dans les propositions et reconnaît les efforts déployés dans ce sens par la Commission, il conclut néanmoins que la nécessité reste la question centrale: le rapport coûts/bénéfices du système est en jeu, non seulement du point de vue financier, mais aussi du point de vue des droits fondamentaux considérés dans le contexte global des dispositifs et des politiques relatives aux frontières qui existent actuellement.

104. En ce qui concerne l'EES, le CEPD émet les recommandations suivantes:

- conformément à l'article 7 de la Charte, la nécessité et la proportionnalité du système ne pourront être positivement démontrées qu'après l'adoption d'une politique européenne claire sur la gestion des personnes ayant dépassé la durée de séjour autorisée et l'évaluation du système dans le contexte plus global des systèmes informatiques à grande échelle existants;

- conformément à l'article 8, les principes en matière de protection des données devraient être améliorés comme suit:

  - les finalités devraient être limitées et la conception du système ne devrait pas préjuger de la future évaluation de tout éventuel accès aux données de l'EES par les autorités répressives;
  - les droits des personnes concernées devraient être renforcés, surtout en ce qui concerne le droit à l'information et les possibilités de recours, en tenant compte de la nécessité d'apporter des garanties spécifiques au niveau des décisions automatisées prises au sujet du calcul de la durée de séjour;
  - la surveillance devrait être complétée par un aperçu clair de la répartition des compétences au niveau national, afin de veiller à ce que les personnes concernées fassent valoir leurs droits auprès de l'autorité compétente;
  - l'utilisation de données biométriques devrait faire l'objet d'une analyse d'impact ciblée et, si jugé nécessaire, le traitement de ces données devrait être soumis à des garanties spécifiques relatives au processus d'enregistrement, au niveau de précision et à la nécessité

d'une procédure de secours. En outre, le CEPD s'interroge fortement sur la collecte de 10 empreintes digitales alors qu'à des fins de vérification, il suffirait d'en recueillir deux ou quatre;
- les raisons pour lesquelles le transfert de données de l'EES vers des pays tiers est nécessaire au rapatriement des ressortissants de ces pays devraient être explicitées.

105. Si le RTP ne soulève pas les mêmes questions substantielles que l'EES en ce qui concerne son ingérence dans les droits fondamentaux, le CEPD attire néanmoins l'attention du législateur sur les aspects suivants:

- la base volontaire de ce système est reconnue, mais le consentement ne doit être considéré comme une base juridique valide pour le traitement qu'à condition qu'il soit librement donné, ce qui signifie que le RTP ne devrait pas devenir la seule solution disponible pour éviter les longues files et les charges administratives;
- il convient de prévenir les risques de discrimination: le grand nombre de voyageurs qui ne voyagent pas assez souvent pour se soumettre à un enregistrement, ou dont les empreintes digitales sont illisibles, ne devraient pas être placés de fait dans la catégorie des voyageurs «à risque plus élevé»;
- le processus de vérification précédant l'enregistrement devrait être basé sur un accès sélectif à des bases de données clairement identifiées.

106. En ce qui concerne les aspects relatifs à la sécurité, le CEPD estime que, pour l'EES comme pour le RTP et afin d'évaluer et de hiérarchiser les risques, il convient d'élaborer un plan de maintien des activités ainsi que des pratiques de gestion des risques pour la sécurité des informations. Une solide collaboration devrait en outre être prévue entre l'Agence et les États membres.

Fait à Bruxelles, le 18 juillet 2013.

(signé)

Peter HUSTINX
Contrôleur européen de la protection des données