Avis du Contrôleur européen de la protection des données sur la proposition modifiée de règlement du Parlement européen et du Conseil relatif à la création du système «EURODAC» pour la comparaison des empreintes digitales aux fins de l'application efficace du règlement (UE) n° […/…] […] (Refonte)

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 décision-cadre 2008/977/JAI du Conseil du 27 novembre 2008[3] relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale,

A ADOPTÉ LE PRÉSENT AVIS:

1. 1. INTRODUCTION

1.1. Consultation du CEPD

1. Le 30 mai 2012, la Commission a adopté une proposition concernant une refonte du règlement du Parlement européen et du Conseil relatif à la création du système «EURODAC» pour la comparaison des empreintes digitales aux fins de

[1] JO L 281 du 23.11.1995, p. 31.
[2] JO L 8 du 12.01.2001, p. 1.
[3] JO L 350 du 30.12.2008, p. 60.

Adresse postale: rue Wiertz 60 - B-1047 Bruxelles
Bureaux: rue Montoyer 63
Courrier électronique: edps@edps.europa.eu – Site web: www.edps.europa.eu
Tél.: 02-283 19 00 - Fax: 02-283 19 50

l'application efficace du règlement (UE) n° […/…] (établissant les critères et mécanismes de détermination de l'État membre responsable de l'examen d'une demande de protection internationale présentée dans l'un des États membres par un ressortissant de pays tiers ou un apatride) et pour les demandes de comparaison avec les données d'EURODAC présentées par les services répressifs 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 (ci-après, la «proposition»)[4].

2. La proposition a été envoyée par la Commission au CEPD pour consultation le 5 juin 2012, conformément à l'article 28, paragraphe 2, du règlement (CE) n° 45/2001. Le CEPD recommande de faire référence à la présente consultation dans le préambule de la proposition.

3. Le CEPD regrette que les services de la Commission ne lui aient pas demandé de formuler des observations informelles à l'intention de la Commission avant l'adoption de la proposition, conformément à la procédure convenue en rapport avec les documents de la Commission relatifs au traitement de données à caractère personnel[5].

4. La proposition a été présentée aux ministres de l'Intérieur lors du Conseil «Justice et affaires intérieures» des 7 et 8 juin 2012 et est actuellement examinée au sein du Conseil et du Parlement européen en vue de l'adoption d'un règlement selon la procédure législative ordinaire d'ici à la fin 2012. Le présent avis du CEPD vise à contribuer à cette procédure.

1.2. Contexte

5. EURODAC a été créé en 2000 par le règlement (CE) n° 2725/2000 du 11 décembre 2000 concernant la création du système «Eurodac» pour la comparaison des empreintes digitales aux fins de l'application efficace de la convention de Dublin[6]. La Commission a présenté des propositions de modification de ce règlement en 2008[7] et en 2009[8]. La proposition de la Commission de 2008 visait à garantir un degré plus élevé d'harmonisation et de meilleures normes de protection pour le régime d'asile européen commun (RAEC), tandis que la proposition de la Commission de 2009 avait pour objet l'utilisation des empreintes digitales des demandeurs d'asile à des fins répressives.

6. Le CEPD a rendu des avis sur ces deux propositions de la Commission, celle de 2008[9] et celle de 2009[10]. Il s'est montré très critique, en particulier dans ce deuxième avis.

---

[4] COM(2012)254 final.
[5] Le CEPD a été consulté de manière informelle par la Commission sur une modification du règlement EURODAC pour la dernière fois en 2008.
[6] JO L 316 du 15.12.2000, p. 1.
[7] COM(2008)825 final.
[8] COM(2009)342 final et COM(2009)344 final.
[9] Avis du contrôleur européen de la protection des données sur la proposition de règlement du Parlement européen et du Conseil concernant la création du système «Eurodac» pour la comparaison des empreintes digitales aux fins de l'application efficace du règlement (CE) n° […/…] (établissant les

7. À la suite de l'entrée en vigueur du traité sur le fonctionnement de l'Union européenne (TFUE) et de l'abolition de la structure en piliers, la Commission a adopté une nouvelle proposition en 2010, qui remplace les propositions précédentes[11]. Afin de faire progresser les négociations sur le paquet de mesures concernant l'asile et favoriser la conclusion d'un accord sur EURODAC, la proposition de la Commission de 2010 ne contenait plus de dispositions sur l'accès à EURODAC à des fins répressives.

8. La proposition actuelle retire et remplace la proposition de la Commission de 2010, suivant la procédure de la refonte, afin de:
   - tenir compte d'une résolution du Parlement européen et du résultat des négociations au sein du Conseil[12];
   - permettre aux services répressifs des États membres et à Europol d'accéder à la base de données centrale d'EURODAC aux fins de prévenir, détecter et enquêter sur les infractions terroristes et d'autres infractions pénales graves;
   - apporter les modifications nécessaires au règlement (UE) n° 1077/2011 du Parlement européen et du Conseil du 25 octobre 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[13].

9. D'après l'exposé des motifs de la proposition, il est devenu évident que l'accès à EURODAC à des fins répressives «doit être pris en compte dans le cadre d'un accord équilibré sur les négociations du paquet relatif au régime d'asile européen commun»[14]. La proposition actuelle n'a fait l'objet d'aucune nouvelle consultation ou analyse d'impact étant donné que, d'après l'exposé des motifs, les analyses d'impact de 2008 et de 2009[15] seraient toujours valides. C'est apparemment pour les mêmes raisons que le CEPD n'a pas eu la possibilité de formuler des observations informelles, comme indiqué au point 3 ci-dessus.

1.3. Motifs et structure du présent avis du CEPD

10. Dans le présent avis, le CEPD souhaite mettre en exergue les principaux problèmes suivants:
    - la procédure suivie ne tient pas compte de la nature fondamentale de la proposition; une nouvelle analyse d'impact aurait dû être réalisée;
    - la nécessité et la proportionnalité de l'accès aux données d'EURODAC à des fins répressives ne sont pas suffisamment démontrées;

---

critères et mécanismes de détermination de l'État membre responsable de l'examen d'une demande de protection internationale présentée dans l'un des États membres par un ressortissant de pays tiers ou un apatride) (COM(2008)825), JO C 229 du 23.9.2009, p. 6.

[10] Avis du CEPD du 7 octobre 2009 sur les propositions concernant l'accès à EURODAC à des fins répressives, JO C 92 du 10.4.2010, p. 1.

[11] COM(2010)555 final.

[12] Voir l'exposé des motifs, p. 3.

[13] JO L 286 du 1.11.2011, p. 1.

[14] Voir l'exposé des motifs, p. 3.

[15] SEC(2008)2981 et SEC(2009)936.

- la proposition n'examine pas suffisamment les conséquences de l'utilisation des données d'EURODAC à des fins répressives en ce qui concerne les aspects liés à la législation en vigueur en matière de protection des données, et ne prend pas davantage en considération la nouvelle base juridique de la protection des données depuis l'entrée en vigueur du traité de Lisbonne, ni la réforme en cours de la protection des données.

11. L'avis est structuré comme suit:
    - la section 2 formule des observations critiques sur la procédure suivie par la Commission;
    - la section 3 se focalise sur les problèmes généraux liés à l'accès aux données d'EURODAC à des fins répressives;
    - la section 4 contient des observations sur la législation en matière de protection des données applicable à la collecte et au traitement des données d'EURODAC dans une perspective répressive;
    - la section 5 contient des observations sur des dispositions plus spécifiques de la proposition concernant l'accès à EURODAC à des fins répressives;
    - la section 6 émet certaines observations sur d'autres dispositions de la proposition;
    - la section 7 énonce les conclusions.

12. L'avis s'appuie sur les points de vue exprimés dans des avis précédents concernant la révision d'EURODAC (voir le point 5), ainsi que sur d'autres avis rendus dans des domaines pertinents. Il tient également compte des expériences du groupe de coordination de contrôle d'EURODAC, créé afin de faciliter le contrôle prévu par l'article 20 du règlement EURODAC actuel[16].

2. PROCÉDURE SUIVIE PAR LA COMMISSION

13. Il semble que la Commission considère la proposition en question comme un exercice technique. Il ressort de l'exposé des motifs qu'elle vise essentiellement à relancer son ancienne proposition, adoptée en 2009. Or, au cours des trois dernières années, d'importants changements institutionnels et de fond ont eu lieu, par exemple à la suite de l'entrée en vigueur du traité de Lisbonne. En outre, le fait qu'il a été décidé en 2010 de retirer les dispositions sur l'accès à des fins répressives afin de faciliter les négociations au sein du Conseil et du Parlement indique clairement que la proposition actuelle – qui compte l'accès à des fins répressives parmi ses principaux objectifs – n'est pas de nature principalement technique.

14. D'après la Commission, la proposition reprend les dispositions de la proposition d'une décision du Conseil de 2009, désormais caduque. Aucun des éléments introduits n'est considéré comme nouveau, et tous ont été évalués dans le cadre des analyses d'impact précédentes de 2008[17] et de 2009[18]. Par conséquent, au lieu

[16] Sur ce groupe, voir http://www.edps.europa.eu/EDPSWEB/edps/cache/off/Supervision/Eurodac.
[17] SEC(2008) 2981, 3.12.2008.
[18] SEC(2009) 936, 10.9.2009.

de joindre une nouvelle analyse d'impact, la Commission utilise celles de 2008 et de 2009 pour justifier l'adoption de la présente proposition. Le CEPD n'est pas d'accord avec cette approche et estime qu'une nouvelle analyse d'impact reste nécessaire.

15. D'après le CEPD, deux raisons expliquent pourquoi les deux analyses d'impact effectuées il y a trois et quatre ans ne suffisent pas à démontrer la nécessité et la cohérence réelles de la présente proposition.

16. La première raison est que les résultats des premières analyses d'impact n'étaient pas pertinents ou convaincants. L'analyse d'impact de 2008 n'est pas pertinente étant donné qu'elle n'évalue pas l'introduction de l'accès à EURODAC à des fins répressives. Quant à l'analyse d'impact de 2009, si elle évalue effectivement la possibilité d'utiliser les données d'EURODAC à des fins répressives, elle n'est pas suffisamment détaillée[19].

17. L'analyse d'impact de 2009 envisageait quatre options politiques pour réglementer l'accès aux données des demandeurs d'asile à des fins répressives[20]. La première option (le maintien du statu quo) a été écartée sans explication. Deux des trois autres options ont consisté à analyser les raisons pour lesquelles l'accès à la base de données d'EURODAC serait essentiel pour identifier des criminels présumés et pour prévenir un crime, lutter contre celui-ci et enquêter à son sujet. L'analyse a toutefois omis de fournir ne fût-ce que des exemples spécifiques justifiant la nécessité réelle d'un tel accès[21]. Qui plus est, elle n'a pas tenu compte du fait que les demandeurs d'asile forment un groupe de personnes vulnérables et que la nécessité d'une protection supplémentaire devrait donc être appréciée.

18. La quatrième option politique concernait la possibilité de créer un réseau décentralisé permettant à chaque État membre de consulter d'une manière automatisée les bases de données nationales de demandeurs d'asile de tous les autres États membres. Cette option suggérait que le nouveau réseau n'utiliserait que des instruments existants, comme le mécanisme prévu par la décision 2008/615/JAI du Conseil du 23 juin 2008 relative à l'approfondissement de la coopération transfrontalière, notamment en vue de lutter contre le terrorisme et la criminalité transfrontalière (ci-après, la «décision Prüm»)[22]. Cette option a été écartée au motif qu'elle serait compliquée et coûteuse.

19. L'analyse d'impact de 2009 affirme en plusieurs endroits que les instruments répressifs actuels sont insuffisants et qu'ils ne sont pas pratiques pour comparer les empreintes digitales aux fins d'enquête criminelle. Elle fait notamment remarquer que la recherche d'empreintes digitales dans les fichiers automatisés

[19] Pour de plus amples détails, voir les avis du CEPD de 2008 et 2009; voir également l'avis du CEPD du 15 décembre 2010 sur la création d'EURODAC pour la comparaison des empreintes digitales, JO C 101 du 1.4.2011, p. 14.
[20] SEC(2009)936, pp. 17-19.
[21] Les exemples donnés aux pages 11 et 12 de l'analyse d'impact sont trop généraux et vagues. Ils ne reposent pas sur des cas réels et spécifiques, mais plutôt sur des situations hypothétiques dans lesquelles la comparaison des empreintes digitales des demandeurs d'asile pourrait s'avérer utile à des fins répressives. Voir également l'avis du CEPD de 2009, points 46-48.
[22] JO L 210 du 6.8.2008, pp. 1-11.

nationaux d'empreintes digitales (ci-après, les «FAED»)[23] d'autres États membres appliquant la décision Prüm n'était pas totalement fiable dans la mesure où certains États membres étaient susceptibles de ne pas enregistrer les empreintes digitales de demandeurs d'asile dans leurs FAED nationaux si celles-ci n'étaient pas liées à un crime[24]. En outre, l'analyse d'impact souligne que la décision-cadre 2006/960/JAI du Conseil relative à la simplification de l'échange d'informations et de renseignements entre les services répressifs[25] peut être utilisée pour collecter des données sur les demandeurs d'asile uniquement si des raisons factuelles donnent lieu de croire qu'un État membre particulier détient effectivement l'information[26]. Enfin, l'analyse d'impact note que l'assistance juridique mutuelle implique qu'une demande doit être adressée à l'ensemble des États membres censés disposer de l'information pertinente, ce qui prend du temps[27].

20. D'après le CEPD, il convient de démontrer que la combinaison de ces trois instruments et leur utilisation simultanée ne couvriraient pas l'ensemble des situations possibles dans lesquelles l'identité des demandeurs d'asile est requise à des fins répressives. En outre, dans tous les exemples fournis par l'analyse d'impact de 2009, la décision Prüm ainsi que d'autres instruments ont été écartés car jugés insuffisants parce que tous les demandeurs d'asile n'ont pas leurs empreintes digitales enregistrées dans d'autres systèmes. L'analyse d'impact omet cependant d'avancer des arguments cohérents et justifiés en faveur d'un instrument supplémentaire centré spécifiquement sur les demandeurs d'asile[28], alors que des instruments comparables ne sont pas prévus et qu'ils ne sont vraisemblablement pas nécessaires pour d'autres groupes d'individus.

21. La deuxième raison pour laquelle une nouvelle analyse d'impact est nécessaire est que les deux études d'impact précédentes sont obsolètes. Elles ont été réalisées dans un contexte où la décision Prüm et la décision concernant la mise en œuvre de la décision Prüm n'étaient appliquées que partiellement dans les États membres. Le CEPD est d'avis que les progrès réalisés depuis 2009 dans l'application de ces décisions doivent être pris en compte dans l'évaluation visant à déterminer si un accès à EURODAC à des fins répressives est effectivement nécessaire.

22. En outre, la proposition ne comprend pas l'analyse d'impact sur les droits fondamentaux prévue par la communication de la Commission de 2010 intitulée «Stratégie pour la mise en œuvre effective de la Charte des droits fondamentaux par l'Union européenne». Cette communication a été adoptée dans le contexte de l'entrée en vigueur du traité de Lisbonne, qui a conféré à la Charte des droits fondamentaux le statut de droit primaire de l'UE[29]. L'analyse d'impact doit

[23] Voir la décision 2008/616/JAI du Conseil du 23 juin 2008 concernant la mise en œuvre de la décision 2008/615/JAI relative à l'approfondissement de la coopération transfrontalière, notamment en vue de lutter contre le terrorisme et la criminalité transfrontalière, JO L 210 du 6.8.2008, p. 12 (ci-après, la «décision concernant la mise en œuvre de la décision Prüm»).
[24] SEC(2009)936, p. 9.
[25] JO L 386 du 29.12.2006, p. 89.
[26] SEC(2009)936, p. 9.
[27] *Ibidem*, pp. 9-10.
[28] Voir l'exposé plus détaillé aux points 31-32.
[29] COM (2010)573.

examiner l'incidence de la proposition sur les droits en utilisant la liste de contrôle fournie dans cette communication[30].

23. Cette liste de contrôle prévoit que des réponses soient apportées à des questions fondamentales – par exemple, s'agit-il d'impacts positifs (promotion des droits fondamentaux) ou négatifs (limitations des droits fondamentaux)? Les limitations apportées aux droits fondamentaux seraient-elles nécessaires pour réaliser un objectif d'intérêt général ou pour protéger les droits et libertés d'autrui? La mesure serait-elle proportionnée à l'objectif poursuivi, et respecterait-elle le contenu essentiel des droits fondamentaux concernés?

24. Eu égard à ce qui précède, le CEPD recommande vivement à la Commission de réaliser une nouvelle analyse d'impact dans laquelle les quatre options politiques seraient examinées, qui fournirait des preuves solides et des données statistiques fiables et qui comprendrait une analyse d'impact sur les droits fondamentaux. En outre, elle devrait dûment tenir compte de l'évolution des pratiques et du droit observée depuis 2009.

3. ACCÈS AUX DONNÉES D'EURODAC À DES FINS RÉPRESSIVES

3.1. Limitation des finalités et risque de détournement d'usage

25. Lorsque le règlement créant EURODAC a été adopté, il n'envisageait pas l'accès des forces de police à la base de données, devenue opérationnelle en 2003. Les empreintes digitales sont collectées et traitées aux fins de la détermination de l'État membre responsable de l'examen d'une demande d'asile, afin d'empêcher les demandes d'asile multiples au sein de l'UE et, de manière plus générale, de faciliter l'application du règlement de Dublin[31]. Des garanties spécifiques sont prévues pour faire en sorte que la base de données d'EURODAC ne soit *pas* utilisée à d'autres fins.

26. La proposition suggère un nouveau régime juridique, dans lequel les données continueront d'être collectées aux fins de l'examen des demandes d'asile, mais pourront – dans certaines circonstances – être utilisées à d'autres fins, par exemple la répression en dehors du contexte de l'asile et de la migration. Cela constitue ce qu'il est convenu d'appeler un «détournement de finalité», à savoir un élargissement progressif de l'usage d'un système ou d'une base de données au-delà de la finalité pour laquelle ils ont été initialement conçus.

27. En général, le CEPD a de fortes réserves à l'égard de cette tendance. Il appelle à une approche prudente face à des initiatives pouvant entraîner l'utilisation de données ou de systèmes pour d'autres finalités sans rapport avec les finalités

[30] Voir également les «Orientations opérationnelles sur la prise en compte des droits fondamentaux dans les analyses d'impact de la Commission», SEC(2011)567 du 6.5.2011.

[31] La convention de Dublin a été remplacée en 2003 par le 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, JO L 50 du 25.2.2003, p. 1 (ci-après, le «règlement de Dublin»).

initiales. Il ne faut pas accepter facilement que, puisque les données sont déjà collectées, elles peuvent tout aussi bien être utilisées pour d'autres finalités, qui sont susceptibles d'avoir une incidence plus grande sur la vie des individus. L'évaluation de la nécessité et de la proportionnalité de la création d'EURODAC aurait été totalement différente si l'accès à des fins répressives avait été envisagé d'entrée de jeu.

28. En outre, cet élargissement de l'usage d'un système existant est difficile à concilier avec le principe de limitation des finalités, un des principes clés de la législation relative à la protection des données[32]. Les exceptions à ce principe sont possibles, mais uniquement à de strictes conditions. Avant toute chose, le traitement des données pour l'autre finalité doit être nécessaire et proportionné.

29. Le CEPD n'est pas convaincu que la nécessité et la proportionnalité qui pourraient justifier une exception au principe de la limitation des finalités ont été suffisamment démontrées. Une meilleure justification est nécessaire, comme exposé dans les sections suivantes.

3.2. Nécessité de l'accès à des finalités répressives

30. La proposition soulève certaines questions relatives à la nécessité d'accorder l'accès à EURODAC à des fins répressives, puisque, comme précédemment indiqué, il existe déjà un certain nombre d'instruments juridiques permettant à un État membre de consulter les empreintes digitales et d'autres données en matière répressive détenues par un autre État membre[33].

31. Premièrement, les États membres peuvent avoir recours à la décision Prüm, qui vise à renforcer la coopération transfrontalière entre les pays de l'UE en matière pénale, notamment en mettant en réseau les bases de données nationales des États membres[34]. Aux termes de l'article 8 de la décision Prüm, les États membres veillent à la disponibilité des données indexées provenant des FAED nationaux créés en vue de la prévention des infractions pénales et de la réalisation d'enquêtes en la matière. Ces données de référence consistent uniquement en un numéro de référence et des données dactyloscopiques (à savoir, «les images d'empreintes digitales, images d'empreintes digitales latentes, d'empreintes de paumes de mains, d'empreintes de paumes de mains latentes, ainsi que des modèles de telles images [points caractéristiques codés], lorsqu'ils sont stockés et traités dans une base de données automatisée»[35]).

32. Deuxièmement, d'autres instruments pourraient être appliqués. La décision-cadre 2006/960/JAI pourrait être utilisée pour les consultations d'empreintes digitales. Les mesures prévues dans cet instrument peuvent être mises en œuvre moyennant certaines conditions telles que la nécessité de donner des raisons

[32] Le principe est énoncé à l'article 5, point b), de la convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, STCE n° 108, 28.1.1981 (ci-après, la «convention 108»), à l'article 6, paragraphe 1, point b), de la directive 95/46/CE et à l'article 3 de la décision-cadre 2008/977/JAI.

[33] Pour de plus amples informations, voir également l'avis du CEPD du 7 octobre 2009.

[34] Voir l'article 1er et le considérant 13 de la décision Prüm.

[35] Article 2, point i), de la décision concernant la mise en œuvre de la décision Prüm.

factuelles de croire qu'un autre État membre détient l'information, ainsi que la nécessité d'une autorisation préalable d'une autorité judiciaire. En outre, la convention européenne d'entraide judiciaire en matière pénale[36] pourrait également être utilisée par les autorités judiciaires des États membres pour demander l'accès aux bases d'empreintes digitales recueillies ou non en rapport avec des activités criminelles, y compris à celles des demandeurs d'asile. Enfin, si un ressortissant d'un pays tiers a demandé un visa Schengen, ses empreintes digitales seront déjà saisies dans le système d'information sur les visas en tant que demandeur de visa[37]; et si le ressortissant du pays tiers est recherché en vue d'une arrestation ou s'il est signalé aux fins de non-admission, il se retrouvera dans le système d'information Schengen[38].

33. Par conséquent, le CEPD suggère de procéder à une évaluation exhaustive et actualisée avant de créer un nouvel instrument donnant aux services répressifs l'accès aux données des demandeurs d'asile, afin de déterminer si une mise en œuvre intégrale des instruments existants ne pourrait pas suffire. D'après le CEPD, il y a des raisons suffisantes de croire que les instruments existants peuvent déjà être efficaces et suffisants.

34. La situation actuelle de la décision Prüm et de la décision concernant la mise en œuvre de la décision Prüm a récemment été examinée par le Conseil, qui, observant que certaines difficultés de mise en œuvre subsistaient[39], a appelé en décembre 2011 les États membres à achever leurs procédures nationales de mise en œuvre juridique et technique afin d'appliquer pleinement les décisions Prüm[40]. Le Conseil a également invité les États membres à préparer l'évaluation de l'efficacité et de l'efficience des décisions Prüm en tant qu'outil d'échange d'informations[41], conformément au programme de Stockholm, qui souligne 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*»[42].

35. Par ailleurs, le CEPD nourrit à cet égard un vif intérêt pour la communication de la Commission sur le modèle européen d'échange d'informations, qui a été annoncé pour 2012 et qui reposera, entre autres, sur les résultats de l'exercice de cartographie de l'information lancé par la Commission en 2010[43]. L'objectif de ce dernier était d'analyser les systèmes et canaux d'informations actuels afin de déterminer la nécessité éventuelle de nouveaux instruments ou mesures. Tant que la mise en œuvre des instruments actuels n'est pas pleinement opérante et analysée de manière plus approfondie, le CEPD considère qu'il serait prématuré d'accorder l'accès aux données d'EURODAC à des fins répressives.

---

[36] Convention européenne d'entraide judiciaire en matière pénale, STCE n° 030, 20.4.1959.
[37] Sur la base de l'article 8 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), JO L 218 du 13.8.2008, p. 60.
[38] Sur la base des articles 95 et 96 de la convention de Schengen.
[39] Conseil des ministres, 18676/11, 20.12.2011.
[40] Conseil des ministres, 17762/11, 5.12.2011.
[41] *Ibidem*.
[42] Programme de Stockholm, point 1.2.2.
[43] À la page:
http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/police-cooperation/eixm/index_en.htm.

3.3. Proportionnalité de l'accès à des fins répressives

36. Le CEPD nourrit également des doutes quant au fait que l'accès des services répressifs aux données d'EURODAC serait conforme à l'exigence de proportionnalité.

37. Il convient de souligner que les demandeurs d'asile constituent un groupe de personnes vulnérables et que, par conséquent, leur position précaire doit être prise en considération lors de l'évaluation de la nécessité et de la proportionnalité de la mesure proposée[44]. La proposition n'en tient pas compte.

38. Le résultat net des changements qu'il est proposé d'apporter au système actuel réside dans le fait qu'un demandeur d'asile peut être identifié si ses empreintes digitales sont trouvées sur une scène de crime, ce qui n'est pas le cas d'autres individus parce que ces données ne sont pas disponibles pour tous les groupes sociaux. La Commission n'a justifié d'aucune manière la différence de traitement entre les demandeurs d'asile et les autres individus à cet égard. Le traitement des données d'EURODAC à des fins répressives pourrait par conséquent donner lieu à une discrimination potentielle des demandeurs d'asile, qui, en l'absence de justification, ne saurait être considérée comme une mesure proportionnée.

39. Il convient de souligner que la Cour de justice de l'UE et la Cour européenne des droits de l'homme (ci-après, la «CEDH») ont condamné des bases de données qui conduisaient à une inégalité de traitement injustifiée entre les personnes[45]. Dans l'affaire *S. et Marper*, la CEDH a évoqué à cet égard les risques de stigmatisation[46].

40. La proportionnalité implique également que, si la nécessité de l'accès était démontrée et la mise en balance des droits et des intérêts respectée, l'accès à des fins répressives devrait être soumis à des conditions strictes, comme le neuvième considérant de la proposition le souligne également, notamment la condition qu'il existe de bonnes raisons de croire que l'auteur d'une infraction terroriste ou d'une autre infraction pénale grave a demandé l'asile (voir également le point 56 ci-dessous).

4. LÉGISLATION APPLICABLE EN MATIÈRE DE PROTECTION DES DONNÉES

41. Actuellement, la directive 95/46/CE s'applique à tous les traitements de données effectués par les États membres dans le cadre du système EURODAC. Toutefois, le fait d'accorder aux services répressifs l'accès aux données d'EURODAC entraîne l'application du cadre juridique compliqué adopté sur la base de l'ancien troisième pilier. Le traitement de données à caractère personnel par les autorités

[44] Voir également l'avis du CEPD de 2009, point 29.
[45] Voir l'arrêt de la CJUE du 16 décembre 2008 dans l'affaire C-524/06, *Huber*, Rec. 2008, I-09705, et l'arrêt de la CEDH du 4 décembre 2008 dans les affaires 30562/04 et 30566/04, *S. et Marper contre Royaume-Uni*.
[46] *Ibidem*, point 122.

nationales compétentes est régi par les dispositions de 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 pénale[47] dans la mesure où il relève de son champ d'application. Le traitement de données à caractère personnel par Europol est régi par la décision 2009/371/JAI du Conseil portant création de l'Office européen de police (Europol)[48].

42. La proposition contient plusieurs dispositions énonçant certains droits et obligations liés à la protection des données. D'après le trente-deuxième considérant de la proposition, elles complètent ou clarifient la directive 95/46/CE. On ne comprend toutefois pas très bien en quoi ces spécifications ont trait à la décision-cadre 2008/977/JAI ou à la décision 2009/371/JAI du Conseil[49]. L'article 33, qui énonce que ces deux décisions s'appliquent au traitement des données d'EURODAC par les services répressifs et Europol, respectivement, n'apporte aucune clarté sur ce point, laissant ainsi ouverte la question de savoir s'il y a lieu de considérer que certaines dispositions de la proposition complètent ou clarifient également ces deux décisions.

43. Le principal exemple est l'article 35, qui interdit explicitement le partage de données à caractère personnel avec des pays tiers, des organisations internationales ou des entités privées. Le lien n'est pas précisé entre cette interdiction et la possibilité de transférer des données à caractère personnel en vertu de la décision-cadre 2008/977/JAI. À cet égard, il est pertinent de souligner que la décision-cadre 2006/960/JAI ne porte pas d'interdiction de transférer des données vers des pays tiers[50]. Le CEPD est d'avis que le transfert de données d'EURODAC est effectivement interdit, y compris en cas d'utilisation de ces données à des fins répressives, et recommande au législateur de le préciser à l'article 35 de la proposition.

44. L'article 35 contient une exception à l'interdiction. Les États membres ont le droit de transférer des données à caractère personnel vers les pays tiers auxquels le règlement de Dublin s'applique. D'après le CEPD, il faudrait préciser dans les considérants ou dans une disposition de fond que cette exception ne saurait s'appliquer aux données traitées à des fins répressives. .

45. Un autre exemple concerne l'article 29 de la proposition, qui définit les droits de la personne concernée. Si l'article 29 venait effectivement compléter ou clarifier la décision-cadre 2008/977/JAI ou la décision 2009/371/JAI du Conseil, il devrait attacher une attention particulière aux droits des personnes concernées dans le contexte de l'accès à des fins répressives et de l'utilisation ultérieure des données. Par exemple, en vertu de l'article 29, paragraphe 1, point b), la personne concernée a le droit d'être informée des finalités pour lesquelles ses données seront traitées. Or, cette disposition indique uniquement qu'une description des objectifs du règlement de Dublin sera incluse. Si l'on devait décider d'accorder

[47] JO L 350 du 30.12.2008, p. 60.
[48] JO L 121 du 15.5.2009, p. 37.
[49] Décision 2009/371/JAI du Conseil du 6 avril 2009 portant création de l'Office de police européen («EUROPOL»), JO L 121 du 15.5.2009, p. 37.
[50] JO L 386 du 29.12.2006, pp. 89-100.

l'accès à EURODAC à des fins répressives, cela devrait être ajouté à l'information communiquée à la personne concernée.

46. La nécessité de préciser le lien que les dispositions de la proposition entretiennent avec la décision-cadre 2008/977/JAI ainsi que la décision 2009/371/JAI du Conseil est d'autant plus forte que les propositions pour un nouveau cadre de protection des données du 25 janvier 2012 prévoient de conserver la distinction entre un instrument général de protection des données et un instrument autonome à des fins répressives[51]. En outre, les nouvelles règles proposées n'affectent pas les règles relatives à la protection des données applicables aux institutions, organes et agences de l'UE telles que fixées par le règlement (CE) n° 45/2001, ni les règles spécifiques en la matière telles que celles applicables à Europol ou les dispositions de la décision Prüm[52].

5. DISPOSITIONS SPÉCIFIQUES DE LA PROPOSITION CONCERNANT L'ACCÈS À DES FINS RÉPRESSIVES

47. Comme exposé ci-dessus, il y a lieu tout d'abord de démontrer que l'accès à EURODAC à des fins répressives est véritablement nécessaire et proportionné. Les conditions dans lesquelles cet accès pourrait être accordé relèvent d'une autre analyse, qui ne devrait être effectuée que si la nécessité et la proportionnalité sont démontrées de manière suffisante. Il conviendrait alors de tenir compte des observations qui suivent.

5.1. Autorités désignées et autorités chargées de la vérification

48. Les États membres déterminent des «autorités désignées» (article 5 de la proposition) ainsi que des «autorités chargées de la vérification» (articles 6 et 7 de la proposition). Ces deux types d'autorités doivent être responsables de la prévention et de la détection des infractions terroristes et des autres infractions pénales graves, ainsi que des enquêtes en la matière. Leurs responsabilités sont cependant très différentes.

49. Aux termes de l'article 5, les autorités désignées sont autorisées à consulter les données d'EURODAC en vertu du règlement proposé. Pour garantir sans équivoque que cet accès est limité aux finalités répressives, le CEPD recommande

[51] COM(2012)11 final et COM(2012)10 final.

[52] Voir l'avis du CEPD du 7 mars 2012 sur le paquet de mesures pour une réforme de la protection des données, point 26, disponible à la page suivante: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-03-07_EDPS_Reform_package_FR.pdf. Les demandeurs d'asile sont également protégés par deux autres textes législatifs: premièrement, la directive 2011/95/CE (JO L 337 du 20.12.2011, p. 9) consacre le principe de confidentialité (article 37) et protège la collecte, le traitement et la diffusion d'informations relatives aux mineurs non accompagnés (article 31, paragraphe 5); deuxièmement, le règlement (CE) n° 343/2003 du Conseil (JO L 50 du 25.2.2003, p. 1) établit que les demandes de données à caractère personnel formulées par les États membres sont adéquates, pertinentes et raisonnables pour l'examen de la demande d'asile (article 21, paragraphe 1), que les informations échangées ne peuvent être utilisées qu'aux fins de la détermination de l'État membre responsable de l'examen de la demande d'asile (article 21, paragraphe 7), et que le demandeur d'asile a le droit d'être informé, conformément à la directive 95/46/CE (article 21, paragraphe 9).

d'ajouter à l'article 5, paragraphe 1, les termes «pour les finalités visées à l'article 1er, paragraphe 2».

50. L'autorité chargée de la vérification visée à l'article 6 vérifie la licéité des demandes d'accès aux données d'EURODAC formulées par les autorités désignées. Elle examine et confirme[53] que les conditions de cet accès sont bien remplies. Le CEPD considère le mécanisme de contrôle comme une garantie essentielle contre tout accès illicite. Il souligne que, du point de vue des droits fondamentaux, l'option privilégiée serait d'exiger une autorisation judiciaire préalable, qui offre des garanties adéquates et solides d'indépendance et d'impartialité. En l'absence d'une telle exigence, il est essentiel de veiller à ce que l'autorité chargée de la vérification soit effectivement indépendante de l'autorité désignée afin de garantir un contrôle réel et approprié et de créer un système adéquat de contrôles et d'équilibres.

51. Par conséquent, le CEPD recommande d'ajouter au moins à l'article 6 de la proposition que l'autorité chargée de la vérification remplit ses fonctions et ses tâches en toute indépendance et qu'elle ne reçoit pas d'instructions sur l'exercice de la vérification.

52. Il en va de même de l'article 7 de la proposition concernant l'accès aux données d'EURODAC par Europol.

5.2. Procédure et conditions de comparaison et de transfert de données à des fins répressives

53. Aux termes de l'article 19 de la proposition, une demande d'accès aux données d'EURODAC à des fins répressives est soumise au contrôle préalable de l'autorité chargée de la vérification, qui examine si les conditions d'accès sont remplies. Le paragraphe 3 prévoit une exception à ce contrôle préalable «dans des cas d'urgence exceptionnels». Dans ces cas, une vérification a posteriori est effectuée sans retard excessif après le traitement de la demande. Toutefois, aucune ligne directrice n'est fournie sur ce qui constitue un cas d'urgence exceptionnel. Cette absence de clarté pourrait entraîner des interprétations divergentes et une insécurité quant à la portée de l'exception. Le CEPD recommande d'ajouter à l'article 19 le critère de la nécessité d'empêcher un danger imminent lié à une infraction terroriste ou à une autre infraction pénale grave[54].

54. Par ailleurs, l'article 19, paragraphe 3, énonce que la vérification a posteriori est effectuée «sans retard excessif» après le traitement de la demande. Le CEPD considère que cette expression est trop vague et recommande d'introduire un délai concret.

[53] Voir l'article 19, paragraphe 2, de la proposition.

[54] On pourrait également envisager d'autres formulations plus spécifiques, comme celles mentionnées au vingt-sixième considérant de la proposition, en particulier: «un danger spécifique et concret en rapport avec une infraction terroriste ou une autre infraction pénale grave, ou à des personnes spécifiques à l'égard desquelles il existe de raisons sérieuses de croire qu'elles ont commis ou commettront des infractions terroristes ou d'autres infractions pénales graves».

55. Conformément à l'article 20, les autorités désignées ne peuvent demander la comparaison d'empreintes digitales avec celles conservées dans la base de données centrale EURODAC à des fins répressives que si la comparaison avec les bases nationales de données dactyloscopiques et les systèmes automatisés nationaux d'identification par empreintes digitales d'autres États membres en application de la décision Prüm n'a donné aucun résultat positif et si:

    - la comparaison est nécessaire aux fins de la prévention et de la détection des infractions terroristes et autres infractions pénales graves, et aux fins d'enquêtes en la matière (article 20, paragraphe 1, point a));

    - la comparaison est nécessaire dans un cas précis; des comparaisons systématiques ne peuvent être effectuées (article 20, paragraphe 1, point b)); et si

    - il existe des motifs raisonnables de penser que la comparaison avec les données d'EURODAC contribuera à la prévention ou à la détection des infractions pénales en question ou aux enquêtes en la matière (article 20, paragraphe 1, point c)).

56. Le CEPD salue l'exigence d'une consultation préalable des bases de données nationales et de celles d'autres États membres à travers le mécanisme mis en place par la décision Prüm. Il considère néanmoins qu'un contrôle préalable du système d'information sur les visas doit également être obligatoire. Il note en outre que la liste des conditions ne comprend pas l'exigence visée au neuvième considérant de la proposition et dans l'exposé des motifs selon laquelle il doit exister de bonnes raisons de croire que l'auteur d'une infraction terroriste ou d'une autre infraction pénale grave a demandé l'asile[55]. À la lumière des observations précédentes sur la proportionnalité de l'accès aux données d'EURODAC, le CEPD considère cette condition comme particulièrement importante et recommande vivement au législateur de l'ajouter à la liste figurant à l'article 20 de la proposition. La référence au neuvième considérant ne suffit pas à garantir le respect de cette exigence.

57. Le CEPD considère que l'utilisation des termes «contribuera à», figurant à l'article 20, paragraphe 1, point c), est trop large. Comme indiqué dans l'exposé des motifs, la comparaison des données doit contribuer «considérablement» à la prévention ou à la détection des infractions pénales en question ou aux enquêtes en la matière[56]. Le CEPD suggère de modifier l'article 20, paragraphe 1, point c), en conséquence. Toujours en rapport avec cette disposition, il recommande de clarifier ce qu'il y a lieu d'entendre par «motifs raisonnables»[57].

58. En ce qui concerne Europol, ni l'exposé des motifs, ni les considérants n'expliquent la nécessité d'accorder l'accès aux données d'EURODAC à Europol. Le dixième considérant énonce seulement que «dans le cadre de la coopération entre les autorités des États membres, lors d'enquêtes sur des activités criminelles transfrontalières, Europol joue un rôle clé de soutien dans la prévention de la criminalité, ainsi que pour l'analyse et les enquêtes criminelles à l'échelle de l'Union» pour justifier son accès aux données d'EURODAC dans le cadre de ses missions. En outre, l'analyse d'impact de 2009 n'est pas très diserte sur la

[55] Voir en particulier le neuvième considérant et la p. 7 de l'exposé des motifs.
[56] Voir la page 7 de l'exposé des motifs.
[57] Voir également l'avis du CEPD de 2010, point 49.

nécessité concrète d'un accès direct d'Europol[58]. Dans la pratique, avant d'envoyer des empreintes digitales à Europol, un service répressif national peut les comparer, s'il y a lieu, aux données d'EURODAC, et il est très probable qu'il le fasse. Le CEPD recommande par conséquent d'au moins décrire dans un considérant le genre de situations justifiant un accès *direct* d'Europol à la base de données centrale d'EURODAC.

59. En outre, le CEPD note que les critères stricts relatifs à l'accès des autorités désignées aux données d'EURODAC ne s'appliquent pas à l'accès d'Europol à ces mêmes données. Les demandes de comparaison formulées par Europol sont autorisées aux fins d'une analyse spécifique ou d'une analyse de portée générale et de type stratégique. Le CEPD se demande comment les larges facilités accordées à Europol sont compatibles avec le raisonnement avancé par la Commission, à savoir que l'accès n'est nécessaire que dans un cas précis et dans des circonstances bien définies. En l'absence de toute explication spécifique, le CEPD recommande d'aligner l'article 21 sur l'article 20.

5.3. Comparaison avec des empreintes digitales latentes

60. Actuellement, en comparant les empreintes digitales d'une personne avec les données d'EURODAC, les pays de l'UE peuvent déterminer si un demandeur d'asile ou un ressortissant étranger en séjour illégal dans un pays de l'UE a déjà demandé l'asile dans un autre pays de l'UE ou si un demandeur d'asile est entré illégalement sur le territoire de l'Union. Ces situations requièrent la présence physique de la personne concernée (au moins à un moment donné) pour permettre aux autorités nationales compétentes de prélever ses empreintes digitales afin de les comparer avec les données d'EURODAC. La réalisation de comparaisons à des fins répressives est différente dans son approche puisque les empreintes digitales peuvent être prélevées sur une scène de crime ou dans un autre environnement en l'absence de la personne concernée. Cela suscite de nouvelles préoccupations quant aux effets néfastes potentiels sur les personnes innocentes.

61. Le CEPD nourrit des doutes sérieux sur la possibilité de rechercher des empreintes digitales latentes dans le système EURODAC à des fins répressives, comme le douzième considérant l'envisage. Toute recherche dans EURODAC basée sur une empreinte digitale latente, en particulier si elle a été trouvée dans un lieu public, est susceptible de déboucher sur un nombre élevé de résultats possibles étant donné le nombre plus grand de corrélations possibles avec des empreintes partielles ou fragmentaires. Les conséquences d'une fausse concordance peuvent être graves car celle-ci risque d'entraîner l'implication injuste d'innocents dans des enquêtes pénales. Le taux d'erreur peut être influencé par la qualité des empreintes digitales latentes, qui sont souvent déformées, ce qui ajoute à la

[58] On peut lire dans l'analyse d'impact de 2009 que: «(...) Europol est censé fournir aux services répressifs nationaux les outils nécessaires pour échanger des informations entre eux, comme pour l'échange d'informations utilisant les unités nationales Europol. Il ressort des réponses qu'Europol et les États membres ont apportées au questionnaire que l'échange d'informations entre ces unités serait facilité si les informations échangées en rapport avec les empreintes digitales de demandeurs d'asile faisaient partie des informations échangées entre eux par l'intermédiaire d'Europol dans le cadre d'un fichier concret lié au crime organisé transfrontalier. Comme Europol ne peut avoir actuellement accès aux informations sur les demandeurs d'asile, il ne peut garantir que ces informations font partie de ses missions d'analyse et d'enquête».

difficulté de faire correspondre ces empreintes digitales à celles saisies dans EURODAC, qui sont prélevées dans de meilleures conditions.

62. La comparaison d'empreintes digitales à des fins répressives doit en tout cas être soumise au moins aux mêmes garanties que celles déjà prévues, notamment à l'article 25, paragraphe 4, de la proposition.

5.4. Accès aux données à caractère personnel et conservation de celles-ci à des fins répressives

63. L'article 33, paragraphe 4, prévoit que «[les] données à caractère personnel qu'un État membre ou Europol obtient d'EURODAC en vertu du présent règlement sont effacées des dossiers nationaux et de ceux d'Europol après un mois, si ces données ne sont pas nécessaires à la poursuite d'une enquête pénale spécifique menée par cet État membre ou Europol». Le CEPD accueille favorablement la période de conservation des données extraites d'EURODAC à des fins répressives, mais il demande de clarifier l'exigence relative à l'absence d'une enquête pénale spécifique pour supprimer les données. L'accès aux données d'EURODAC ne doit être autorisé qu'en cas d'enquête pénale spécifique. Le CEPD recommande dès lors de préciser plus clairement le cadre de cette exception ou de la supprimer.

5.5. Nature des données consultées à des fins répressives

64. L'article 9, paragraphe 5, l'article 15, paragraphe 2, et l'article 17, paragraphe 4 – qui concernent l'accès à EURODAC dans le contexte de l'application du règlement de Dublin –, prévoient qu'en cas de résultat positif (c'est-à-dire, lorsqu'une ou plusieurs correspondances résultent de la comparaison entre les empreintes digitales saisies dans le système central et celles transmises par un État membre), le système central transmet, pour tous les ensembles de données correspondant au résultat positif, les données visées à l'article 11[59], accompagnées, le cas échéant, de la marque visée à l'article 18, paragraphe 1. La proposition ne contient cependant pas de disposition similaire lorsque la comparaison des empreintes digitales est requise à des fins répressives.

65. L'exposé des motifs (p. 7) indique que «[la] comparaison avec EURODAC à des fins répressives donnera un résultat positif ou négatif («hit/no hit»), ce qui signifie qu'elle indiquera seulement si un autre État membre possède des données relatives à un demandeur d'asile. La proposition ne prévoit pas de nouvelles possibilités de traiter des informations à caractère personnel supplémentaires dans le cadre du suivi d'un «hit» (réponse positive)». Le CEPD se demande dans quelle mesure il serait efficace, pour les services répressifs, de ne recevoir que des informations de type «hit/no hit», c'est-à-dire portant sur l'existence ou l'absence d'une correspondance. On peut raisonnablement imaginer que les services répressifs devront savoir quel État membre détient les données relatives au demandeur d'asile auquel les empreintes digitales appartiennent.

[59] La proposition fait référence aux données mentionnées à l'article 8, point a). Cet article concerne cependant les statistiques établies par l'Agence IT. Le CEPD déduit du règlement EURODAC que la disposition pertinente est en fait l'article 11 de la proposition, qui énumère les données saisies dans le système central.

66. Cette nécessité éventuelle d'informations supplémentaires doit être clarifiée. Dans le cas où la communication d'informations complétant le «résultat positif» (par exemple, l'identification de l'État membre détenant les données) serait envisagée, le CEPD rappelle qu'en vertu des principes de nécessité et de proportionnalité, l'information à transmettre doit être limitée au strict minimum nécessaire à la finalité pour laquelle l'accès a été accordé.

5.6. Agence IT et modifications au règlement (UE) n° 1077/2011

67. Le CEPD se demande pourquoi les règles relatives au secret professionnel contenues dans l'article 17, paragraphe 5, point g), du règlement (UE) n° 1077//2011[60] ont été retirées (voir l'article 38, paragraphe 4, point a), de la proposition) et recommande de les rétablir.

68. L'article 38, paragraphe 2, de la proposition introduit à l'article 12, paragraphe 1, point t), l'obligation, pour le conseil d'administration, de demander des comparaisons aves les données d'EURODAC par les autorités répressives des États membres à des fins répressives. La proposition n'apporte pas d'autres précisions sur cette obligation. Le CEPD comprend qu'elle est liée aux rapports et aux données statistiques que l'Agence IT doit fournir. Il recommande dès lors de préciser à l'article 38, paragraphe 2, de la proposition modifiant l'article 12, paragraphe 1, point t), du règlement (UE) n° 1077/2011 les finalités précises de ce genre de demande, ainsi que l'anonymisation des données par les services répressifs avant leur transmission au conseil d'administration.

6. AUTRES DISPOSITIONS SPÉCIFIQUES DE LA PROPOSITION

69. Le CEPD a commenté d'autres dispositions de la proposition dans ses avis de 2008 et 2009, mentionnés au point 6 ci-dessus. Ces observations ne seront pas répétées ici dans leur intégralité. La présente section mettra en évidence les principales préoccupations et abordera les nouvelles modifications. Le cas échéant, il sera fait référence à l'analyse plus approfondie des avis précédents du CEPD.

6.1. Article 4: gestion opérationnelle

70. Le CEPD salue l'obligation de veiller à ce que le système central utilise à tout moment la meilleure technologie disponible, moyennant une analyse coût-bénéfice (article 4, paragraphe 1). Il recommande toutefois de remplacer l'expression «meilleure technologie disponible» par l'expression «meilleures techniques disponibles», qui comprend tant la technologie utilisée que la manière dont l'installation est conçue, construite, entretenue et exploitée. Ce point est important car le concept de «meilleures techniques disponibles» est plus large et couvre divers aspects contribuant à l'application de la «protection des données dès

[60] Règlement (UE) n° 1077/2011 du Parlement européen et du Conseil du 25 octobre 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 286 du 1.11.2011, p. 1.

la conception», qui est considérée comme un principe clé dans la révision du cadre légal de l'UE relatif à la protection des données[61].

71. À l'article 3, paragraphe 1, un système de maintien des activités est prévu. En outre, à l'article 4, paragraphe 5, la disponibilité de la plateforme est fixée à 24 heures par jour, sept jours par semaine. Cela montre que le système est considéré comme critique. Toutefois, aucun détail n'est fourni sur ce «système de maintien des activités» ni sur ses besoins en matière de sécurité et de protection des données.

72. Un système critique devrait être couvert par un plan bien étudié et éprouvé de maintien des activités (en cas de perturbations ou catastrophes majeures), ce qui a des répercussions sur la protection des données, la sécurité et les coûts. Il convient d'apporter un soin particulier à la définition des besoins de disponibilité du système, en tenant compte des besoins de maintenance et des pannes imprévues. En outre, il y a lieu de décrire les exigences en matière de maintien des activités. Lors de la détermination des mesures relative au maintien des activités, leur incidence sur la protection des données doit être prise en considération. Cette incidence peut être due à l'existence de copies de données, de supports de sauvegarde et d'autres endroits et systèmes physiques où les données seraient physiquement accessibles. Le CEPD recommande de remplacer le système de maintien des activités par la nécessité d'un plan de maintien des activités à l'article 3, paragraphe 1, et à l'article 4, paragraphe 5, et de prévoir une base juridique pour la mise en œuvre des mesures contenant les modalités de ce plan.

6.2. Articles 9, 14 et 17: enregistrements impossibles

73. Le CEPD rappelle le problème de l'«enregistrement impossible», à savoir la situation dans laquelle les empreintes digitales d'une personne ne sont pas utilisables. Il importe de veiller à ce qu'un «enregistrement impossible» n'entraîne pas automatiquement un déni de droit pour les demandeurs d'asile. La proposition envisage déjà partiellement l'enregistrement impossible à l'article 9, paragraphes 1 et 2, mais ces dispositions considèrent uniquement l'hypothèse d'un enregistrement temporairement impossible, alors que dans certains cas, cette impossibilité est permanente. Par conséquent, le CEPD recommande d'ajouter aux articles 9, 14 et 17 une disposition prévoyant qu'une impossibilité temporaire ou permanente de fournir des empreintes digitales exploitables ne porte pas atteinte à la situation légale de l'individu. Dans tous les cas, elle ne peut constituer un motif suffisant pour refuser d'examiner ou rejeter une demande d'asile[62].

6.3. Article 16: conservation des données

[61] Voir l'article 23 de la proposition de la Commission en vue d'un 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, et l'avis du CEPD du 7 mars 2012, points 177-182. Voir également les avis du CEPD du 15 décembre 2010 et du 18 février 2009.

[62] Voir l'avis du CEPD du 15 décembre 2010 sur la création d'EURODAC pour la comparaison des empreintes digitales, section IV, JO C 101 du 1.4.2011, p. 14.

74. Le CEPD salue la modification apportée à l'article 16 fixant à un an la période de conservation des données (au lieu de deux dans le texte actuel du règlement). Cela constitue une bonne application du principe de qualité des données, selon lequel les données doivent être conservées pour une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées[63].

6.4. Article 29: droit d'information

75. Le CEPD souligne que les informations doivent être communiquées d'une manière qui permette au demandeur d'asile de comprendre parfaitement sa situation ainsi que l'étendue de ses droits, y compris les démarches qu'il peut effectuer pour donner suite aux décisions administratives prises à son sujet. À cet égard, le CEPD se réjouit des ajouts apportés à l'article 29, paragraphe 1, qui s'alignent sur la proposition d'un règlement général sur la protection des données[64].

76. Le CEPD salue la rédaction d'une brochure commune claire et simple contenant les informations à fournir à la personne concernée et l'obligation, pour les États membres, de fournir les informations d'une manière adaptée à l'âge lorsque la personne est mineure. Cela contribue à une meilleure harmonisation et à un meilleur respect du règlement EURODAC, conformément aux recommandations du groupe de coordination de contrôle d'EURODAC[65].

6.5. Articles 28 et 36: conservation des enregistrements, registre et documentation

77. Pour les besoins du contrôle de la protection des données et de la sécurité des données, l'Agence IT, les États membres et Europol conservent des relevés de toutes les opérations de traitements de données effectuées au sein du système central (article 28) d'une part et résultant des demandes de comparaison avec les données d'EURODAC d'autre part (article 36). Toutefois, bien que les objectifs soient les mêmes (protection des données et sécurité des données), le libellé n'est pas identique dans les deux dispositions (par exemple, l'article 28 mentionne le service *qui a […] saisi ou extrait les données*, tandis que l'article 36 fait référence au nom de *l'autorité qui a demandé l'accès* en vue d'une comparaison). Afin de garantir la cohérence et de permettre un contrôle approprié, le CEDP recommande de fusionner ces deux dispositions en une seule utilisant les termes de l'article 36, qui sont plus précis et plus complets.

---

[63] Voir l'article 6, paragraphe 1, point e), de la directive 95/46/CE et l'article 4, paragraphe 1, point e), du règlement (CE) n° 45/2001. Voir également l'article 4, paragraphe 2, de la décision-cadre 2008/977/JAI du Conseil.

[64] Voir l'avis du CEPD du 15 décembre 2010 et les articles 11 et 14 de la proposition d'un 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.

[65] Voir la deuxième inspection coordonnées sur l'information des personnes concernées et l'évaluation de l'âge des jeunes demandeurs d'asile, disponible à la page suivante: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Eurodac/09-06-24_Eurodac_report2_EN.pdf.

78. Par ailleurs, l'article 36 prévoit la tenue de registres et la conservation de traces documentaires supplémentaires par les États membres et Europol aux fins de comparaison avec les enregistrements conservés par l'Agence IT (par exemple, les données d'identification de l'agent qui a effectué la recherche et celles de l'agent qui a ordonné la recherche ou la transmission). Le CEPD salue cette obligation, qui est conforme au principe de responsabilité et contribuera à garantir un contrôle effectif.

79. Enfin, le CEPD note que, si l'article 36 se rapporte à l'accès des autorités nationales de contrôle à ces traces, il n'est pas fait mention d'un accès similaire du CEPD et de l'autorité de contrôle d'Europol à celles respectivement conservées par l'Agence IT et Europol. Le CEPD recommande de modifier l'article 28 en ce sens.

6.6. Articles 31 et 32: modèle de contrôle

80. Le CEPD salue le modèle de contrôle prévu aux articles 31 et 32 de la proposition. Ce modèle est similaire à ceux du système d'information Schengen (2e génération) et du système d'information sur les visas[66]. Il reflète la pratique courante, qui a prouvé son efficacité et favorisé une coopération étroite entre le CEPD et les autorités nationales chargées de la protection des données. Par conséquent, le CEPD se réjouit de son intégration formelle dans la proposition et que, ce faisant, le législateur ait veillé à le rendre cohérent avec les systèmes de contrôle d'autres systèmes informatiques à grande échelle.

81. Le trente-quatrième considérant de la proposition fait explicitement référence à la surveillance de la licéité des traitements de données à caractère personnel d'Europol par l'autorité de contrôle créée par la décision Europol. Bien que la proposition contienne des dispositions spécifiques en matière de contrôle lorsque des opérations de traitement de données sont effectuées par des États membres ou par l'Agence IT (voir les articles 31 et 32), le CEPD note que le texte ne contient pas de disposition similaire sur le contrôle des opérations de traitement de données effectuées par Europol et recommande de remédier à ce problème.

6.7. Article 34: sécurité des données

82. Le CEPD a plusieurs suggestions à formuler en rapport avec l'article 34 sur la sécurité des données.
    - L'article 34, paragraphe 2, point a), ne devrait pas faire référence à des infrastructures critiques générales, mais à celles nécessaires au système. Nous suggérons de remplacer le terme «critiques» par celui de «nécessaires».
    - À l'article 34, paragraphe 2, point f), les termes «qu'avec […] un mode d'accès confidentiel» mériteraient d'être précisés.

[66] Voir les articles 41 à 43 du règlement VIS, l'article 46 du 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 du 28.12.2006, p. 4, et l'article 62 de la décision 2007/533/JAI du Conseil du 12 juin 2007 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen de deuxième génération (SIS II), JO L 265 du 7.8.2007, p. 63.

- À l'article 34, paragraphe 2, point g), le CEPD recommande d'ajouter les termes «*mettre à disposition leurs profils et toute autre information pertinente requise par les autorités aux fins de l'exécution du contrôle*». Le CEPD recommande également d'ajouter une référence explicite à l'article 28 de la directive 95/46/CE dans la mesure où les exigences relatives à la sécurité des données prévues à l'article 34 s'appliquent au transfert de données effectué afin de faciliter l'application du règlement de Dublin ainsi qu'au transfert à des fins répressives.
- À l'article 34, paragraphe 2, point i), il convient de s'assurer que les registres, ainsi que les données auxquelles ils se rapportent, sont protégés.
- Afin de garantir le contrôle de l'efficacité des mesures de sécurité, le CEPD recommande d'inclure à l'article 34, paragraphe 2, point k), 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.
- L'article 34 devrait également mentionner le plan de maintien des activités[67]. En ce qui concerne les incidents de sécurité, il devrait aussi inclure:
    - l'obligation, pour les États membres, d'informer l'Agence IT des incidents de sécurité qu'ils ont détectés dans leur système;
    - l'obligation, pour l'Agence IT, d'informer toutes les parties concernées en cas d'incidents de sécurité;
    - l'obligation, pour toutes les parties, de collaborer pendant un incident de sécurité;
    - l'obligation d'informer les autorités nationales chargées du contrôle et le CEPD.

6.8. Article 40: autocontrôle et rapport annuel

83. Aux termes de l'article 40, paragraphe 1, l'Agence IT soumet au Parlement européen et au Conseil un rapport annuel sur les activités du système central. Le CEPD demande à en être également destinataire.

84. D'autre part, l'article 40, paragraphe 2, de la proposition prévoit des procédures de contrôle. Le CEPD est d'avis que ce contrôle ne doit pas seulement concerner les aspects liés aux résultats, au rapport coût-efficacité et à la qualité des services, mais aussi le respect des exigences légales, notamment dans le domaine de la protection des données. L'article 40, paragraphe 2, devrait être modifié en conséquence.

85. Afin de réaliser cet autocontrôle de la licéité du traitement, la Commission devrait être autorisée à utiliser les traces conservées en vertu de l'article 28 de la proposition. Par conséquent, l'article 28 devrait prévoir que ces traces sont conservées non seulement pour surveiller la protection des données et en garantir la sécurité, mais aussi pour réaliser des autocontrôles réguliers d'EURODAC. Les rapports d'autocontrôle contribueront à la mission du CEPD et d'autres autorités chargées du contrôle, qui seront mieux à même de sélectionner les domaines prioritaires de leur contrôle.

[67] Voir les points 72-73 ci-dessus.

6.9. Article 43: publication de la liste d'autorités

86. Le CEPD salue l'obligation faite à la Commission de publier la liste des autorités ayant accès aux données d'EURODAC (article 43). Afin de renforcer la transparence et de créer un outil efficace et pratique en vue d'un meilleur contrôle du système (par exemple, à travers les autorités nationales chargées de la protection des données), le CEPD recommande d'obliger les États membres et Europol à actualiser en permanence les informations qu'ils ont fournies à la Commission. Il recommande en outre d'imposer que la Commission mette ces informations à la disposition des États membres, d'Europol et du public «grâce à une publication électronique actualisée en permanence».

7. CONCLUSIONS

87. Le CEPD note que, ces dernières années, la nécessité d'accéder aux données d'EURODAC à des fins répressives a été longuement débattue au sein de la Commission, du Conseil et du Parlement européen. Il comprend également que la disponibilité d'une base d'empreintes digitales peut constituer un outil supplémentaire utile dans la lutte contre la criminalité. Toutefois, le CEPD rappelle aussi que cet accès à EURODAC est lourd de conséquences pour la protection des données à caractère personnel des individus dont les données sont saisies dans le système EURODAC. Pour être valable, la nécessité de cet accès doit être étayée par des éléments manifestes et indéniables, et la proportionnalité du traitement démontrée. Cela s'impose d'autant plus en cas d'atteinte aux droits d'individus qui constituent un groupe vulnérable nécessitant une protection, comme la proposition le prévoit.

88. D'après le CEPD, les preuves apportées jusqu'à présent – et compte tenu notamment du contexte spécifique décrit ci-dessus – ne sont pas suffisantes ni assez à jour pour démontrer la nécessité et la proportionnalité de l'octroi d'un accès à EURODAC à des fins répressives. Il existe déjà un certain nombre d'instruments juridiques qui autorisent un État membre à consulter les empreintes digitales et d'autres données des services répressifs détenues par un autre État membre. Une bien meilleure justification est nécessaire au préalable pour permettre l'accès à des fins répressives.

89. Dans ce contexte, le CEPD recommande à la Commission de prévoir une nouvelle analyse d'impact qui considère l'ensemble des options politiques pertinentes, qui fournisse des preuves solides et des données statistiques fiables et qui comprenne une évaluation dans la perspective des droits fondamentaux.

90. Le CEPD a mis en évidence plusieurs problèmes supplémentaires, qui sont les suivants:

Législation applicable en matière de protection des données

91. Le CEPD souligne la nécessité de clarifier la manière dont les dispositions de la proposition précisant certains droits et obligations en matière de protection des

données se rapportent à la décision-cadre 2008/977/JAI du Conseil ainsi qu'à la décision 2009/371/JAI du Conseil (voir la section 4).

Conditions d'un accès à des fins répressives

Comme exposé ci-dessus, il y a lieu tout d'abord de démontrer que l'accès à EURODAC à des fins répressives est véritablement nécessaire et proportionné. Il conviendrait alors de tenir compte des observations qui suivent.

92. Le CEPD recommande de:

- préciser que le transfert des données d'EURODAC vers des pays tiers est interdit y compris en cas d'utilisation de ces données à des fins répressives (voir les points 43-44);
- ajouter les finalités répressives aux informations communiquées aux personnes concernées (voir le point 45);
- garantir sans équivoque que l'accès des autorités désignées aux données d'EURODAC est limité aux finalités répressives (voir le point 49);
- conditionner l'accès aux données d'EURODAC à des fins répressives à une autorisation judiciaire préalable ou, à tout le moins, prévoir que l'autorité chargée de la vérification remplit ses fonctions et ses tâches en toute indépendance et qu'elle ne reçoit pas d'instructions sur l'exercice de la vérification (voir les points 50-51);
- ajouter le critère de la «nécessité d'empêcher un danger imminent lié à une infraction terroriste ou à une autre infraction pénale grave» à la définition du cas exceptionnel justifiant la consultation des données d'EURODAC sans la vérification préalable de l'autorité chargée de la vérification et introduire un délai concret pour la vérification a posteriori (voir les points 53-54);
- en ce qui concerne les conditions d'accès, ajouter comme conditions i) une consultation préalable du système d'information sur les visas, ii) l'existence de «bonnes raisons de croire que l'auteur d'une infraction terroriste ou d'une autre infraction pénale grave a demandé l'asile», et iii) une contribution «considérable» à des finalités répressives, et clarifier ce qu'il y a lieu d'entendre par «motifs raisonnables» (voir les points 56-57);
- décrire, dans un considérant, le type de situations justifiant un accès *direct* d'Europol à la base de données centrales d'EURODAC et prévoir que les conditions strictes d'accès applicables aux autorités nationales désignées s'appliquent également à Europol (voir les points 58-59);
- faire en sorte que la comparaison d'empreintes digitales à des fins répressives soit soumise, dans tous les cas, au minimum à des garanties identiques à celles prévues pour les finalités liées au règlement de Dublin (voir le point 62);
- préciser plus clairement les règles relatives à la conservation et à la suppression des données (voir le point 64);
- clarifier les informations complétant le résultat positif («hit») qui seront communiquées, le cas échéant, à Europol (voir les points 65-66);
- spécifier la ou les finalité(s) précise(s) de la demande de comparaison avec les données d'EURODAC adressée par le conseil d'administration de l'Agence IT aux services répressifs des États membres ainsi que l'anonymisation des données par les services répressifs avant leur transmission au conseil d'administration et rétablir les règles relatives au secret professionnel (voir les points 67-68);

- prévoir l'accès du CEPD et de l'autorité de contrôle d'Europol aux enregistrements conservés par l'Agence IT et Europol, respectivement, ainsi que l'obligation de conserver également des enregistrements aux fins de la réalisation d'autocontrôles réguliers d'EURODAC (voir les points 79 et 85);
- clarifier le contrôle des activités de traitement de données d'Europol (voir le point 81).

Autres dispositions

93. Le CEPD recommande de:

- remplacer le système de maintien des activités par la nécessité d'un plan de maintien des activités et prévoir une base juridique pour les mesures de mise en œuvre contenant les modalités de ce plan (voir le point 72);
- veiller à ce qu'une impossibilité temporaire ou permanente de fournir des empreintes digitales exploitables ne porte pas atteinte à la situation légale de l'individu et que, dans tous les cas, elle ne constitue pas un motif suffisant pour refuser d'examiner ou rejeter une demande d'asile (voir le point 73);
- garantir la cohérence entre les obligations faites à l'Agence IT, aux États membres et à Europol de conserver des enregistrements et la documentation des activités de traitement de données (voir le point 77);
- améliorer les dispositions concernant la sécurité des données (voir le point 82);
- inclure le CEPD parmi les destinataires du rapport annuel de l'Agence IT (voir le point 83);
- ajouter à l'article 43 l'obligation, pour les États membres et Europol, d'actualiser en permanence les informations qu'ils ont fournies à la Commission et imposer que la Commission mette ces informations à la disposition des États membres, d'Europol et du public «grâce à une publication électronique actualisée en permanence» (voir le point 86).

Fait à Bruxelles, le 5 septembre 2012

(**signé**)

Peter HUSTINX
Contrôleur européen de la protection des données