I

(Résolutions, recommandations et avis)

AVIS

CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES

Avis du contrôleur européen de la protection des données sur la proposition modifiée 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) nº (…/…) (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 la proposition de décision du Conseil relative aux demandes de comparaison avec les données Eurodac présentées par les services répressifs des États membres et Europol à des fins répressives

(2010/C 92/01)

LE CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES,

vu le traité instituant la Communauté européenne, et notamment son article 286,

vu la Charte des droits fondamentaux de l'Union européenne, et notamment son article 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) nº 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données [2], et notamment son article 41,

vu la demande d'avis formulée conformément à l'article 28, paragraphe 2, du règlement (CE) nº 45/2001, transmise par la Commission au CEPD le 15 septembre 2009,

A ADOPTÉ L'AVIS SUIVANT:

I. INTRODUCTION

1. Le 10 septembre 2009, la Commission a adopté deux propositions, à savoir la proposition modifiée 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) nº (…/…) (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) [3], et la proposition de décision du Conseil relative aux demandes de comparaison avec les données Eurodac présentées par les services répressifs des États membres et Europol à des fins répressives [4]. Le 15 septembre 2009, elle a transmis ces deux propositions (ci-après dénommées «les propositions» ou «le règlement proposé» et «la décision proposée») au CEPD pour consultation, conformément à l'article 28, paragraphe 2, du règlement (CE) nº45/2001. Le CEPD a également reçu l'analyse d'impact s'y rapportant.

2. Le CEPD se félicite d'avoir été consulté et recommande que cette consultation soit mentionnée dans les considérants de la proposition, comme cela a été le cas pour plusieurs autres textes législatifs sur lesquels il a été consulté conformément au règlement (CE) nº 45/2001.

3. Ces propositions revêtent un intérêt particulier pour le CEPD, compte tenu notamment de la mission de contrôle qu'il exerce sur la base de données de l'Unité centrale d'Eurodac et du contrôle coordonné qu'il doit assurer sur le système Eurodac dans son ensemble avec les autorités nationales chargées de la protection des données.

[1] JO L 281 du 23.11.1995, p. 31.
[2] JO L 8 du 12.1.2001, p. 1.
[3] COM(2009) 342 final.
[4] COM(2009) 344 final.

4. La question de l'accès à des systèmes d'information à grande échelle développés à des fins répressives a déjà été traitée par le CEPD dans le cadre de l'accès au système d'information sur les visas par les services répressifs et par Europol ([5]). Le sujet des propositions est aussi étroitement lié à la refonte générale du règlement Eurodac et du règlement de Dublin, sur lesquels le CEPD a émis des avis le 18 février 2009 ([6]).

II. CONTENU ET CONTEXTE DES PROPOSITIONS

5. Les propositions jettent la base du droit reconnu aux autorités désignées des États membres et d'Europol de demander une comparaison de données dactyloscopiques ou d'empreintes latentes avec les données Eurodac. Une comparaison fructueuse donnera lieu à une réponse positive d'Eurodac, qui sera accompagnée par toutes les données stockées dans Eurodac concernant les empreintes digitales en question. Les demandes d'informations supplémentaires à la suite d'une réponse positive ne sont pas régies par la proposition de décision du Conseil, mais sont couvertes par les instruments existants relatifs aux échanges d'informations en matière répressive. Le champ des propositions est la lutte contre les infractions terroristes et les infractions pénales graves, telles que la traite des êtres humains et le trafic de drogue ([7]).

6. L'article 7 de la décision proposée détermine les conditions de la consultation des données Eurodac par les autorités désignées: la consultation n'est autorisée 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 2008/615/JAI du Conseil relative à l'approfondissement de la coopération transnationale, notamment en vue de lutter contre le terrorisme et la criminalité transnationale ([8]) n'a donné aucun résultat positif et si la comparaison est nécessaire pour lutter contre les infractions terroristes et autres infractions pénales graves, si elle est nécessaire dans un cas précis et s'il existe des motifs raisonnables de penser qu'elle contribuera considérablement à lutter contre les infractions pénales en question. Le CEPD note que l'article 7 n'exige pas que la personne concernée faisant l'objet de la demande relative aux empreintes digitales soit soupçonnée d'avoir commis l'une de ces infractions.

7. Il convient de rappeler que la création du système Eurodac avait pour but de faciliter l'application du règlement de Dublin II, qui permet de déterminer quel est l'État membre responsable de l'examen de la demande d'asile, grâce à la comparaison des empreintes digitales des demandeurs d'asile et des immigrants clandestins, ledit système permettant aux États membres d'identifier les demandeurs d'asile et les personnes appréhendés à l'occasion du franchissement illicite d'une frontière extérieure de la Communauté. En comparant les empreintes digitales, les États membres peuvent établir si un demandeur d'asile ou un ressortissant étranger se trouvant illégalement sur le territoire d'un État membre a déjà demandé l'asile dans un autre État membre ou si un demandeur d'asile est entré sur le territoire de l'Union de manière illicite. Au moment de l'adoption du règlement Eurodac, l'accès des services de police à ce système n'avait pas été prévu; les empreintes digitales étaient collectées en vue de la finalité bien précise visée à l'article 1er, paragraphe 1, dudit règlement.

8. L'article 1er, paragraphe 2, du règlement proposé élargit désormais la finalité du système Eurodac à la prévention et la détection des infractions terroristes et autres infractions pénales graves et aux enquêtes en la matière, aux conditions énoncées dans les propositions. Ce changement de finalité est expliqué dans le considérant 6, selon lequel «la base de données Eurodac ayant été créée pour faciliter l'application du règlement de Dublin, l'accès à Eurodac aux fins de la prévention ou de la détection des infractions terroristes et d'autres infractions pénales graves, ou des enquêtes en la matière constitue un changement de la finalité initiale d'Eurodac, qui entraîne une ingérence dans l'exercice du droit au respect de la vie privée des personnes dont les données à caractère personnel sont traitées dans Eurodac.»

9. L'accès des services répressifs au système Eurodac avait déjà été annoncé antérieurement, quelques années après l'adoption du règlement Eurodac; il en est question dans plusieurs documents, tels que le programme de La Haye, les conclusions du comité mixte du Conseil JAI des 12 et 13 juin 2007 et la communication de la Commission au Conseil et au Parlement européen sur le renforcement de l'efficacité et de l'interopérabilité des bases de données européennes dans le domaine de la justice et des affaires intérieures et sur la création de synergies entre ces bases, du 24 novembre 2005 ([9]): «En ce qui concerne l'objectif de lutte contre le terrorisme et la criminalité, le Conseil considère maintenant comme une lacune l'absence d'accès des autorités chargées de la sécurité intérieure aux données du VIS. On pourrait formuler la même remarque au sujet de toutes les données d'immigration contenues dans le SIS II et à propos des données Eurodac».

10. Comme l'analyse d'impact et l'exposé des motifs le constatent, les propositions visant à rendre le système Eurodac accessible aux services répressifs ont suscité de vives critiques de la part de diverses parties prenantes.

([5]) Avis du contrôleur européen de la protection des données sur la proposition de décision du Conseil concernant l'accès en consultation au système d'information sur les visas (VIS) par les autorités des États membres compétentes en matière de sécurité intérieure et par l'Office européen de police (Europol) aux fins de la prévention et de la détection des infractions terroristes et des autres infractions pénales graves, ainsi qu'aux fins des enquêtes en la matière (COM(2005) 600 final), JO C 97 du 25.4.2006, p. 6.

([6]) Avis du 18 février 2009 sur la proposition de règlement concernant la création du système Eurodac pour la comparaison des empreintes digitales aux fins de l'application efficace du règlement (CE) nº (.../...) (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) (COM(2008)825) et avis du 18 février 2009 sur la proposition de règlement du Parlement européen et du Conseil 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 (COM(2008)820 final).

([7]) Voir notamment l'article 1er de la décision proposée.

([8]) JO L 210 du 6.8.2008, p. 1, ci-après dénommée «la décision Prüm».

([9]) COM(2005) 597 final, point 4.6.

III. OBJET PRINCIPAL DE L'AVIS DU CEPD

11. Le CEPD analysera dans le présent avis la légitimité des propositions en question. Cette analyse le conduira à exprimer de sérieux doutes à ce sujet ainsi que sur l'opportunité d'adopter des instruments législatifs sur la base de ces propositions.

12. L'analyse sera effectuée en tenant compte des éléments suivants:

a) La ligne de démarcation: comment établir un juste équilibre entre l'exigence de sécurité publique et le droit à la protection des données?

b) Les propositions s'inscrivent dans le prolongement de deux tendances plus générales:

i) il est devenu de plus en plus facile pour les services répressifs d'utiliser les données à caractère personnel de personnes n'ayant aucune implication directe dans une infraction donnée, les données en question ayant été collectées à d'autres fins;

ii) de nouveaux instruments juridiques ont été proposés pour compléter des instruments déjà en vigueur, mais pas encore pleinement mis en œuvre — ce qui permet de s'interroger sur le caractère nécessaire de ces nouveaux instruments.

c) Les circonstances particulières du présent dossier: les services répressifs ont déjà accès à de nombreuses informations dans ce domaine.

d) La proposition aura surtout des conséquences pour un groupe social particulièrement vulnérable, à savoir les demandeurs d'asile, qui risque d'être encore plus stigmatisé.

e) Le moment choisi pour adopter ces propositions: les propositions ont été adoptées sans attendre deux changements de contexte importants, susceptibles d'avoir sur elles des répercussions importantes, à savoir le programme de Stockholm et l'entrée en vigueur (éventuelle) du traité de Lisbonne. En outre, elles ont été élaborées sans références à la refonte générale des règlements Eurodac et Dublin, que le Conseil et le Parlement européen examinent encore.

f) La compatibilité avec l'article 8 de la Convention européenne des droits de l'homme.

13. Dans le présent avis, le CEPD ne procède pas à une analyse détaillée du fond des diverses dispositions des propositions, qui présentent dans l'ensemble une bonne qualité législative: elles sont bien rédigées et prévoient des conditions strictes pour que les autorités désignées des États membres et Europol puissent demander la comparaison de données dactyloscopiques avec celles de la base de données centrale d'Eurodac. On trouvera néanmoins quelques observations sur le fond aux points 49 et 50.

IV. LE LIGNE DE DÉMARCATION

14. Le CEPD souligne que l'amélioration de l'échange d'informations est un but politique essentiel de l'Union européenne. L'importance de l'échange d'informations mérite d'autant plus d'être soulignée qu'il n'existe pas de force de police européenne, de système européen de justice pénale ou de contrôle aux frontières entièrement harmonisé. Les mesures dans ce domaine constituent donc une contribution essentielle de l'Union européenne, car elles permettent aux autorités nationales des États membres de lutter efficacement contre la criminalité transnationale et de protéger les frontières extérieures de manière effective; elles ne devraient néanmoins pas seulement contribuer à la sécurité des citoyens, mais également à garantir leurs libertés fondamentales.

15. En d'autres termes, les gouvernements ont besoin d'instruments appropriés pour assurer la sécurité de tous les citoyens, mais ils sont également tenus, au sein de notre société européenne, de respecter pleinement les droits fondamentaux des citoyens. C'est au législateur communautaire qu'il appartient d'assurer cet équilibre. Dans sa communication du 10 juin 2009 sur un espace de liberté, de sécurité et de justice au service des citoyens [10], la Commission mentionne explicitement la nécessité d'atteindre cet équilibre, qui accuse également une place importante dans les discussions en vue d'un programme pluriannuel concernant l'espace de liberté, de sécurité et de justice (programme de Stockholm).

16. Il convient de souligner dans ce contexte que la protection des données ne nuit aucunement à l'intérêt légitime des gouvernements de protéger la sécurité publique. Si des données sont nécessaires en vue d'une finalité spécifique et légitime, elles peuvent être utilisées — s'il le faut, moyennant des mesures supplémentaires fournissant les garanties adéquates. Il est donc essentiel que des informations ne soient collectées, échangées et traitées que sur la base de besoins concrets en matière de sécurité et en tenant compte des principes de protection des données.

17. La lutte contre les infractions terroristes et autres infractions graves [11] peut certainement être un motif légitime justifiant le traitement de données à caractère personnel, dans le respect des droits fondamentaux à la vie privée et à la protection des données. Toutefois, pour être valable, la nécessité de l'ingérence doit s'appuyer sur des éléments clairs et indéniables, et la proportionnalité du traitement doit être démontrée. Cette exigence s'impose d'autant plus dans le cas d'une atteinte considérable à la vie privée des personnes concernées, comme celle que prévoient les propositions.

[10] COM(2009) 262 final. Voir également l'avis du CEPD du 10 juillet 2009 concernant cette communication, point 22.

[11] La finalité pour laquelle la comparaison de données dactyloscopiques est autorisée au titre de l'article 1er de la décision proposée.

V. **PROLONGEMENT DE TENDANCES PLUS GÉNÉRALES**

Tendance à donner aux services répressifs un accès étendu aux données

18. Il convient de souligner que les propositions s'inscrivent 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, mais qu'elles constituent également un pas supplémentaire 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; il s'agit en outre de données qui ont été collectées à d'autres fins que la lutte contre la criminalité. En voici quelques exemples récents:

— la directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE ([12]);

— la décision 2008/633/JAI du Conseil du 23 juin 2008 concernant l'accès en consultation au système d'information sur les visas (VIS) par les autorités désignées des États membres et par l'Office européen de police (Europol) aux fins de la prévention et de la détection des infractions terroristes et des autres infractions pénales graves, ainsi qu'aux fins des enquêtes en la matière ([13]);

— la proposition de décision-cadre du Conseil relative à l'utilisation des données des dossiers passagers (Passenger Name Record — PNR) à des fins répressives ([14]).

19. Dans les avis qu'il a rendus sur ces initiatives, le CEPD s'est montré critique quant au fait d'octroyer aux services répressifs l'accès à des données à caractère personnel relatives à des personnes qui ne sont soupçonnées d'aucune infraction, lesdites données ayant été collectées à d'autres fins. Il a souligné qu'il fallait fournir une justification appropriée à cette ingérence et en vérifier la nécessité et la proportionnalité. Dans son avis relatif aux PNR, il a même mis en garde contre une évolution vers une société de surveillance totale.

20. Cette approche a été développée dans son avis sur la communication de la Commission du 10 juin 2009 intitulée «Un espace de liberté, de sécurité et de justice au service des citoyens» ([15]), où il demande que la tendance consistant à utiliser à des fins répressives des informations collectées à d'autres fins fasse l'objet d'une attention particulière dans le programme de Stockholm. Il convient d'instaurer des conditions strictes en exigeant, par exemple, que les données soient proportionnées, étroitement ciblées et, en principe, fondées sur des suspicions concernant des personnes déterminées.

Nécessité d'un débat général sur l'accès des autorités répressives

21. Il convient de placer le présent avis dans le contexte d'un débat plus vaste sur l'avenir de l'échange d'informations au sein de l'UE et de la tendance de plus en plus marquée à donner aux services répressifs l'accès à d'immenses bases de données. Le CEPD saisit cette occasion pour souligner la nécessité d'évaluer au cas par cas toute proposition de cette nature et d'aborder la question de manière cohérente, globale et tournée vers l'avenir, en se plaçant de préférence dans la perspective du programme de Stockholm.

22. Aujourd'hui plus que jamais, une réflexion approfondie s'impose sur ce que doivent être l'échange d'informations au sein de l'UE et les systèmes d'information à grande échelle; elle devrait tenir compte à la fois des implications pour la vie privée et de l'efficacité recherchée par les services répressifs et avoir lieu non seulement lorsque de nouveaux instruments sont proposés et examinés, mais aussi après la mise en œuvre de ces instruments, au moyen d'examens périodiques. Dans ce domaine, il faut prévoir des garanties «sur mesure» et accorder une plus grande attention au principe de limitation de la finalité. La réflexion devrait également tenir compte de l'entrée en vigueur (éventuelle) du traité de Lisbonne et de ses conséquences pour les systèmes fondés sur une base juridique relevant du premier et du troisième pilier.

Évaluation des instruments en vigueur

23. Les propositions en cause ont été adoptées en complément des instruments juridiques en vigueur utilisés pour la consultation d'empreintes digitales, qui n'ont toutefois pas été mis totalement en œuvre. Dans ce contexte, le CEPD attire en particulier l'attention sur la décision de Prüm ([16]), qui doit être mise en oeuvre par les États membres d'ici à juin 2011. Sur la base de cette décision, les États membres s'octroient les uns aux autres un accès automatisé, entre autres aux systèmes automatisés d'identification par empreintes digitales (AFIS) nationaux sur la base d'un système «hit/no hit». Si une interrogation fondée sur la décision de Prüm fournit un résultat positif, des informations complémentaires, dont des données à caractère personnel, peuvent être obtenues dans l'État membre ayant enregistré l'empreinte digitale dans son AFIS national conformément au droit interne, y compris au moyen de l'entraide judiciaire.

([12]) JO L 105 du 13.4.2006, p. 54. Avis du CEPD du 26 septembre 2005, JO C 298 du 29.11.2005, p. 1.
([13]) JO L 218 du 13.8.2008, p. 129.
([14]) Non encore adoptée par le Conseil; dernier texte en date disponible sur le registre du Conseil, doc. 5618/09 du 29 juin 2009. Avis du CEPD du 20 décembre 2007, JO C 110 du 1er mai 2008, p. 1.
([15]) Voir note de bas de page 8.
([16]) Voir également point 6 et note de bas de page 6.

24. Un autre instrument qui pourrait s'avérer utile dans ce contexte est la décision-cadre 2006/960/JAI du Conseil du 18 décembre 2006 relative à la simplification de l'échange d'informations et de renseignements entre les services répressifs des États membres de l'Union européenne ([17]). Cet instrument facilite l'échange d'informations (c'est-à-dire les données dactyloscopiques ainsi que les informations supplémentaires) détenues par les services répressifs des États membres ou mises à leur disposition. Cet instrument est opérationnel depuis le 18 décembre 2008.

25. Le seul instrument qui existe depuis plus longtemps et dont disposent les États membres est l'entraide judiciaire traditionnelle, au titre de laquelle les autorités judiciaires des États membres peuvent 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 sur la base de la convention relative à l'entraide judiciaire en matière pénale.

26. Le CEPD estime qu'il est essentiel, dans le cadre de l'évaluation de la nécessité de l'accès au système Eurodac, de commencer par mettre en œuvre les nouveaux instruments communautaires qui permettent la consultation par un État membre des empreintes digitales et autres données détenues par les services répressifs d'un autre État membre, puis d'en évaluer l'application.

27. Le respect du principe de proportionnalité suppose non seulement que la mesure proposée soit efficace, mais également que l'objectif prévu par la proposition ne puisse être atteint au moyen des instruments existants; ces instruments doivent donc être soigneusement évalués avant de mettre en place des mesures supplémentaires ou nouvelles relatives au traitement d'informations à caractère personnel. Selon le CEPD, aucune évaluation globale de cette nature n'a eu lieu.

VI. **LES CIRCONSTANCES PARTICULIÈRES DU PRÉSENT DOSSIER**

28. Pour commencer, le CEPD fait observer que, dans sa communication du 24 novembre 2005, la Commission a rappelé que «la demande d'asile ou la demande de visa n'indique en aucune façon qu'une personne jusque-là innocente commettra une infraction pénale ou un acte terroriste» ([18]).

29. Les propositions concernent l'accès à des données à caractère personnel relatives à des personnes qui non seulement ne sont soupçonnées d'aucune infraction, mais qui ont également besoin d'une plus grande protection, dans la mesure où elles fuient des persécutions. Ces personnes constituent une population particulièrement vulnérable, dont la situation précaire doit être prise en compte pour évaluer le caractère nécessaire et la proportionnalité de la mesure proposée.

30. Selon l'exposé des motifs de la décision proposée, il y a une insuffisance structurelle en matière d'information et de vérification en l'absence d'un système unique accessible aux services répressifs et permettant de déterminer l'État membre qui dispose d'informations concernant un demandeur d'asile.

31. En admettant que ce soit le cas, cela ne répond pas à la question de savoir pourquoi il est nécessaire de disposer de ces informations lorsqu'il s'agit de demandeurs d'asile qui, comme on l'a dit, constituent un groupe vulnérable et ne sont en général pas soupçonnés d'infraction, alors qu'on ne dispose d'aucune information similaire relative aux empreintes digitales pour les autres groupes de la société. En admettant qu'il y ait des raisons à cette exigence, la Commission ne les indique pas.

32. Le CEPD attire également l'attention sur une autre justification des propositions. Selon l'exposé des motifs de la décision proposée, si une interrogation fondée sur la décision de Prüm fournit un résultat positif, des informations complémentaires, dont des données à caractère personnel, peuvent être obtenues dans l'État membre ayant enregistré l'empreinte digitale dans son AFIS national conformément au droit interne, y compris au moyen de l'entraide judiciaire. La Commission semble ensuite justifier la proposition en utilisant, entre autres, l'argument suivant: «Bien que cette procédure puisse s'avérer utile pour les États membres qui conservent, dans leur AFIS national, les empreintes digitales des demandeurs d'asile avec d'autres empreintes digitales recueillies par les services répressifs, elle sera sans utilité pour les États membres qui ne conservent pas les empreintes digitales des demandeurs d'asile dans leur AFIS national si elles ne sont pas liées à des activités criminelles». Cet argument est également mis en avant dans l'analyse d'impact qui accompagne les propositions.

33. Pour le CEPD, cet argument est dénué de toute pertinence. La conservation systématique d'empreintes digitales de demandeurs d'asile qui ne sont impliqués dans aucune infraction dans la même base de données que d'autres empreintes digitales — de demandeurs d'asile ou d'autres personnes soupçonnées d'avoir commis une infraction — collectées par des services répressifs est très préoccupante au regard du principe de la limitation de la finalité et de la légitimité du traitement des données. Au lieu d'avancer cet argument, la Commission devrait se demander si ladite conservation systématique est conforme au droit de l'UE sur la protection des données.

VII. **LE MOMENT CHOISI POUR ADOPTER LES PROPOSITIONS**

34. Les propositions sont adoptées par la Commission dans une période de changement.

([17]) JO L 386 du 29.12.2006, p. 89.
([18]) Communication mentionnée au point 9 du présent avis.

35. En premier lieu, l'adoption du programme de Stockholm est prévue pour décembre 2009. L'élaboration de ce programme pluriannuel concernant l'espace de liberté, de sécurité et de justice a donné lieu à des discussions intenses au cours des derniers mois. L'utilisation et l'échange d'informations en constitueront un thème important, y compris la mise au point d'un modèle d'information européen ([19]) ou d'une stratégie européenne de gestion des informations ([20]). Dans ce contexte, le CEPD plaide en faveur d'une approche équilibrée dans laquelle la vie privée et les garanties en matière de protection des données sont intégrées, au niveau le plus précoce, aux systèmes d'information. Les activités du groupe ad hoc du Conseil sur l'échange d'informations sont étroitement liées au programme de Stockholm, et porteront très probablement sur l'objet des deux propositions en question.

36. En second lieu, le CEPD attire l'attention sur la nécessité de réfléchir aux conséquences de l'entrée en vigueur du traité de Lisbonne sur la future législation concernant les activités des services répressifs: la première conséquence sera que toute proposition de cette nature fera à l'avenir l'objet d'une procédure législative ordinaire, ce qui implique une participation à part égale du Conseil et du Parlement européen; la seconde est liée à la suppression de la structure en piliers du traité de l'UE. Le traité de Lisbonne pourrait exiger de la Commission qu'elle présente une nouvelle proposition fondée sur une nouvelle base juridique et, éventuellement, qu'elle fusionne le règlement proposé et la décision proposée dans un seul instrument juridique — ce qui contribuerait en tout état de cause à la clarté juridique.

37. En troisième lieu, le CEPD se demande s'il est nécessaire d'adopter ces propositions dans le cadre d'une procédure distincte de la refonte générale du règlement Eurodac et du règlement de Dublin, lesquels sont toujours examinés par le Parlement et le Conseil. En effet, alors que les discussions fondamentales sur la modification du système Eurodac ne sont pas achevées, les présentes propositions vont entraîner une modification de la finalité du système Eurodac, ce qui est aussi une modification de fond. Il aurait été plus cohérent de joindre ces propositions à la refonte générale ([21]) ou de les reporter jusqu'à l'adoption de la première modification.

38. Dans ces conditions, il est préférable de reporter l'adoption de la proposition afin d'éviter l'incertitude juridique. La Commission ne demande pas que les propositions soient adoptées en urgence, urgence qui n'est certainement pas démontrée par une autre circonstance.

VIII. LA COMPATIBILITÉ AVEC L'ARTICLE 8 DE LA CONVENTION EUROPÉENNE DES DROITS DE L'HOMME

39. L'exposé des motifs du règlement proposé traite clairement de la conformité avec les droits fondamentaux, notamment avec l'article 8 de la Charte des droits fondamentaux de l'UE, relatif à la protection des données à caractère personnel: selon la Commission, afin de garantir que le traitement de données à caractère personnel à des fins répressives ne contrevienne pas au droit fondamental à la protection desdites données et, en particulier, aux principes de nécessité et de proportionnalité, la proposition prévoit de soumettre l'accès des services répressifs à Eurodac à des conditions strictes.

40. Le CEPD n'est pas convaincu par cette déclaration de la Commission: il est essentiel d'évaluer si les propositions respectent la notion de légitimité prévue par l'article 8 de la Convention européenne des droits de l'homme (CEDH) telle qu'interprétée par la Cour de justice et la Cour européenne des droits de l'homme. Les propositions devraient satisfaire aux principes de nécessité et de proportionnalité, en tenant compte des instruments déjà disponibles, et la Commission devrait en faire la démonstration crédible dans la proposition ou dans l'exposé des motifs. L'arrêt faisant jurisprudence en la matière a été rendu dans l'affaire *S. et Marper/Royaume-Uni* ([22]).

41. Selon le considérant 6 de la décision proposée, «toute ingérence de ce type doit être conforme à la loi, qui doit être formulée avec une précision suffisante pour permettre à toute personne d'adapter son comportement et qui doit protéger les personnes contre tout traitement arbitraire et indiquer de façon suffisamment explicite le pouvoir d'appréciation conféré aux autorités compétentes et la manière dont ce pouvoir doit s'exercer. Toute ingérence doit être nécessaire dans une société démocratique pour répondre à un intérêt légitime et proportionné et doit revêtir un caractère proportionné par rapport à l'objectif légitime qu'elle vise». Cependant, les considérants n'indiquent pas en quoi l'instrument proposé est nécessaire.

42. Selon la jurisprudence constante de la Cour européenne des droits de l'homme, une ingérence est considérée comme nécessaire dans une société démocratique pour un but légitime défini par l'article 8, paragraphe 2), de la CEDH si elle répond a «un besoin social impérieux» et, en particulier, si la mesure prise est proportionnée au but légitime poursuivi et si les raisons invoquées par les autorités nationales pour justifier la mesure sont «pertinentes et suffisantes» ([23]). Les autorités nationales jouissent également d'une marge d'appréciation «dont l'ampleur dépend non seulement de la finalité, mais encore du caractère propre de l'ingérence» ([24]). Cette marge est d'autant plus restreinte que le droit en cause est important pour garantir à l'individu la jouissance effective des droits fondamentaux ou d'ordre «intime» qui lui sont reconnus ([25]).

([19]) Terminologie utilisée par la Commission dans sa communication du 10 juin 2009 mentionnée dans la note de bas de page 8.
([20]) Terminologie utilisée par la présidence suédoise.
([21]) Voir point 4.
([22]) Requêtes jointes n° 30562/04 et 30566/04, *S. et Marper c. Royaume-Uni*, arrêt du 4 décembre 2008, CEDH, non encore publié.
([23]) Voir, entre autres, l'arrêt Gillow/Royaume-Uni du 24 novembre 1986, séries A n° 109, § 55.
([24]) Voir l'arrêt Leander/Suède du 26 mars 1987, séries A n° 116, § 59. Voir également l'arrêt de la Cour de justice du 20 mai 2003 dans les affaires C-465/2000, C-138/01 et C-139/01 Österreichischer Rundfunk et autres, Recueil 2003, p. I-4989, point 83.
([25]) Connors/Royaume-uni, arrêt du 27 mai 2004, n° 66746/01, § 82.

43. Dans ce contexte, il est nécessaire dans un premier temps de cerner précisément la finalité poursuivie par le traitement de données à caractère personnel prévu: a-t-elle été clairement identifiée et le caractère nécessaire et proportionné du traitement a-t-il été démontré? Il convient également de prouver qu'il n'existe aucun autre moyen plus respectueux de la vie privée pour réaliser la finalité prévue.

44. Selon le considérant 6 de la décision proposée, la finalité initiale du système Eurodac a été modifiée ([26]). Le simple fait de modifier un texte législatif ne suffit néanmoins pas à produire une mesure compatible avec l'article 8 de la CEDH; l'on peut même soutenir que la modification législative n'entraîne ici aucun changement de finalité: les données resteront conservées à l'avenir dans le système Eurodac à l'unique fin de faciliter l'application du règlement de Dublin; ce n'est que dans des situations exceptionnelles, examinées plus haut, que les autorités répressives des États membres y auront accès. Les propositions ne modifient donc pas la finalité, mais doivent être considérées comme des exceptions apportées au principe de la limitation de la finalité, exceptions qui peuvent être admises à certaines conditions au titre de l'article 13 de la directive 95/46/CE. Or, le CEPD est loin d'être convaincu que ces conditions sont réunies en l'espèce.

45. Le CEPD insiste dans ce contexte sur le fait que se contenter de déclarer dans la proposition législative que la finalité a été modifiée ne rend pas celle-ci acceptable; une modification législative n'implique pas d'office une évaluation différente du caractère nécessaire et proportionné des propositions dans une société démocratique ni de leur respect des dispositions mentionnées au point précédent.

46. Il est clair que les instruments proposés par la Commission constituent une ingérence dans la vie privée. Leur utilité et leur nécessité sont cependant loin d'être démontrées: leur nécessité devrait être prouvée en apportant des preuves convaincantes de l'existence d'un lien entre les demandeurs d'asile et le terrorisme ou la grande criminalité; or, les propositions n'établissent nullement ce lien. Certes, des suspects peuvent être entrés dans l'UE en présentant une fausse demande d'asile, mais le fait qu'il s'agisse là d'un scénario possible n'en fait pas un modèle général qui justifierait l'adoption des instruments.

47. Une autre inquiétude particulière dans ce contexte est le risque de stigmatisation qui découle du fait que des personnes se retrouvant dans la situation de demandeurs d'asile, qui n'ont été accusées d'aucun délit et qui bénéficient de la présomption d'innocence, soient traitées de la même manière que des personnes qui sont a priori suspectes ([27]). À ce sujet, la Cour européenne des droits de l'homme rappelle que le droit reconnu à chacun par la convention de bénéficier de la présomption d'innocence couvre la règle générale suivante: aucun soupc on quant à l'innocence d'une personne ne peut être exprimé après l'acquittement de celle-ci ([28]).

48. De surcroît, le CEPD estime qu'un éventuel argument selon lequel l'accès direct des autorités répressives à Eurodac serait pratique, aisé et rapide ne permettrait pas de conclure que la proposition respecte le critère de la nécessité. La preuve de la nécessité ne peut reposer sur une simple utilité de l'accès, même si ce dernier est assorti de strictes garanties pour la protection des données. En résumé, le CEPD doute fortement que les propositions soient légitimes au sens de l'article 8 de la CEDH.

IX. **BRÈVES OBSERVATIONS SUR LE FOND**

49. À titre indicatif uniquement, le CEPD recommande d'apporter une précision au texte de l'article 2 *bis* du règlement proposé ou, à titre subsidiaire, d'ajouter dans la décision proposée que l'accès à Eurodac peut être accordé aux autorités répressives lorsqu'elles ont un motif précis de croire qu'un suspect a introduit une demande d'asile antérieurement. Bien que suggérée dans le rapport explicatif, cette condition ne fait pas partie du texte de la proposition elle-même. Le CEPD estime que cette garantie apporterait une importante valeur ajoutée; sa suggestion n'implique toutefois pas qu'il accepte le principe de l'accès des autorités répressives à Eurodac: il s'agit uniquement d'une recommandation faite à titre subsidiaire.

50. Le CEPD fait également observer que les critères stricts de l'accès à Eurodac par des autorités désignées ([29]) ne s'appliquent pas à l'accès d'Europol aux données Eurodac: Europol peut en effet introduire des demandes de comparaison aux fins d'une analyse spécifique ou d'une analyse générale et de type stratégique. Le CEPD se demande comment ces plus grandes facilités octroyées à Europol peuvent se concilier avec l'exposé des motifs de la Commission, selon lequel l'accès n'est nécessaire que dans des cas bien précis, dans des circonstances définies et à de strictes conditions.

X. **CONCLUSION**

51. Le CEPD exprime de sérieux doutes quant à la légitimité des propositions et quant à l'opportunité d'adopter des instruments législatifs sur leur base. Ces doutes reposent sur les considérations figurant dans le présent avis, qui peuvent être résumées comme suit.

52. Le CEPD souligne que l'amélioration de l'échange d'informations est un but politique essentiel de l'Union européenne. Les gouvernements ont besoin d'instruments appropriés pour assurer la sécurité de tous les citoyens, mais ils sont également tenus, au sein de notre société européenne, de respecter pleinement les droits fondamentaux des citoyens. C'est au législateur communautaire qu'il appartient d'assurer cet équilibre.

([26]) Voir le point 8 du présent avis.
([27]) S. et Marper, arrêt précité.
([28]) Asan Rushiti/Autriche, n° 28389/95, arrêt du 21 mars 2000, point 31 (avec d'autres références), 33 EHRR 56.
([29]) Article 7 de la décision proposée; voir le point 6 ci-dessus.

53. Adopter des mesures permettant de lutter contre les infractions terroristes et autres infractions graves peut être un motif légitime justifiant le traitement de données à caractère personnel, à condition que la nécessité de l'ingérence s'appuie sur des éléments clairs et indéniables et que le caractère proportionné du traitement soit démontré. Cette exigence s'impose d'autant plus que les propositions concernent un groupe vulnérable, qui a besoin d'une plus grande protection dans la mesure où il fuit des persécutions. La situation précaire de ces personnes doit être prise en compte pour évaluer le caractère nécessaire et proportionné de la mesure proposée. Le CEPD fait aussi valoir le risque de stigmatisation dudit groupe.

54. Le CEPD recommande d'évaluer la légitimité des propositions dans un contexte élargi, à savoir:

a) la tendance visant à accorder aux services répressifs l'accès à des données à caractère personnel relatives à des personnes qui ne sont soupçonnés d'aucune infraction, les données en question ayant été collectées à d'autres fin;

b) la nécessité d'évaluer au cas par cas toute proposition de cette nature et d'aborder la question de manière cohérente, globale et tournée vers l'avenir, en se plaçant de préférence dans la perspective du programme de Stockholm;

c) la nécessité de commencer par mettre en œuvre les nouveaux instruments communautaires qui permettent la consultation par un État membre des empreintes digitales et autres données détenues par les services répressifs d'un autre État membre, puis d'en évaluer l'application;

d) le caractère urgent de la proposition, compte tenu de l'évolution du cadre juridique et politique.

55. Pour ce qui est de la compatibilité des propositions avec l'article 8 de la CEDH, le CEPD met en cause la changement de finalité du système et fait valoir que se contenter de déclarer dans la proposition législative que la finalité a été modifiée ne constitue pas ledit changement. De surcroît, une modification législative n'implique pas d'office une évaluation différente de la nécessité et de la proportionnalité des propositions dans une société démocratique ni de leur respect d'autres dispositions, notamment des règles sur la limitation de la finalité figurant dans la directive 95/46/CE.

56. Le CEPD insiste sur le fait que le caractère nécessaire devrait être démontré en apportant des preuves convaincante d'un lien entre les demandeurs d'asile et le terrorisme ou la grande criminalité, ce que les propositions n'établissent nullement.

57. Enfin, le CEPD se félicite d'avoir été consulté et recommande que cette consultation soit mentionnée dans les considérants de la proposition, comme cela a été le cas pour plusieurs autres textes législatifs sur lesquels il a été consulté conformément au règlement (CE) n° 45/2001. Il émet aussi quelques observations sur le fond des propositions.

Fait à Bruxelles, le 7 octobre 2009.

Peter HUSTINX

Contrôleur européen de la protection des données