Avis du contrôleur européen de la protection des données sur la communication de la Commission au Parlement européen et au Conseil intitulée «Un espace de liberté, de sécurité et de justice au service des citoyens»

(2009/C 276/02)

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,

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, et notamment son article 41,

A ADOPTÉ L'AVIS SUIVANT:

I. INTRODUCTION

1. Le 10 juin 2009, la Commission a adopté sa communication au Parlement européen et au Conseil intitulée «Un espace de liberté, de sécurité et de justice au service des citoyens» ([1]). Le CEPD présente le présent avis conformément à l'article 41 du règlement (CE) nº 45/2001.

2. Préalablement à l'adoption de la communication, la Commission a consulté de façon informelle le CEPD à son sujet, par lettre du 19 mai 2009. Le CEPD a répondu à cette consultation le 20 mai 2009 en envoyant des observations informelles destinées à améliorer le texte de la communication. Il a, en outre, activement contribué à la lettre du 14 janvier 2009 du groupe de travail «Police et justice» concernant le programme pluriannuel en matière de liberté, de sécurité et de justice ([2]).

3. La communication (point 1) souligne que l'Union «doit se doter d'un nouveau programme multi annuel qui, à partir des progrès et en tirant les leçons des faiblesses actuelles, se projette vers l'avenir avec ambition. Ce nouveau programme devra définir des priorités pour les cinq prochaines années». Ce programme pluriannuel (déjà connu sous le nom de «programme de Stockholm») constituera le prolongement des programmes de Tampere et de La Haye, qui ont imprimé un puissant élan politique à l'espace de liberté, de sécurité et de justice.

4. La communication est destinée à servir de base à ce nouveau programme pluriannuel. Le CEPD note dans ce contexte que, bien que les programmes pluriannuels ne soient pas en eux-mêmes des instruments contraignants, ils ont une incidence considérable sur la politique que les institutions mèneront dans le domaine concerné, puisqu'ils donneront lieu à de nombreuse actions concrètes, législatives ou non.

5. La communication s'inscrit dans cette perspective. Elle constitue la nouvelle étape d'un débat qui a plus ou moins débuté avec la présentation, en juin 2008, de deux rapports par les «groupes sur l'avenir» établis par la présidence de Conseil afin de formuler des idées: «Liberté, sécurité, protection de la vie privée — Les affaires intérieures européennes dans un monde ouvert» ([3]) et «Propositions en vue du futur programme de l'UE dans le domaine de la justice» ([4]).

II. PRINCIPAL CONTENU DE L'AVIS

6. Dans le présent avis, le CEPD ne se contente pas de réagir à la communication: il contribue également au débat plus général sur l'avenir de l'espace de liberté, de sécurité et de justice, qui doit déboucher sur un nouveau programme de travail stratégique (le programme de Stockholm), comme annoncé par la présidence suédoise de l'UE ([5]). Dans cet avis, le CEPD examinera aussi certaines des conséquences de l'entrée en vigueur éventuelle du traité de Lisbonne.

7. Une description des principaux aspects examinés dans l'avis (partie III) sera suivie par une évaluation générale de la communication (partie IV).

8. La partie V traite de la question de savoir comment répondre à la nécessité de continuer à garantir la protection de la vie privée et des données à caractère personnel alors que les échanges de ce type de données sont sans cesse plus nombreux. L'accent sera mis sur le point 2.3 de la communication, qui porte sur la protection des données à caractère personnel et de la vie privée, et, de manière plus générale, sur la nécessité d'adopter de nouvelles actions, législatives ou non, pour améliorer le cadre de la protection des données.

([1]) COM(2009) 262 final (ci-après «la communication»).

([2]) Non publié. Le groupe de travail «Police et justice» a été créé par la Conférence européenne des commissaires à la protection des données pour mettre au point ses positions dans le domaine répressif et agir en son nom dans les dossiers urgents.

([3]) Document nº 11657/08 du Conseil (ci-après «le rapport sur les affaires intérieures»).

([4]) Document nº 11549/08 du Conseil (ci-après le «rapport sur la justice»).

([5]) Programme de travail de l'UE établi par le gouvernement, http://www.regeringen.se

9. Dans la partie VI, le CEPD examinera les besoins et les possibilités en ce qui concerne la conservation, l'accès et l'échange d'informations à des fins répressives ou, selon les termes de la communication, dans le cadre d'«une Europe qui protège». Le point 4 de la communication énonce un certain nombre d'objectifs liés au flux d'informations et aux outils technologiques, en particulier les points 4.1.2 (Maîtriser l'information), 4.1.3 (Mobiliser les outils technologiques nécessaires) et 4.2.3.2 (Les systèmes d'information). La mise au point d'un modèle européen d'information (point 4.1.2) peut être considérée comme la proposition la plus ambitieuse dans ce contexte. Dans son avis, le CEPD procédera à une analyse approfondie de cette proposition.

10. La partie VII évoque brièvement un aspect concret de l'espace de liberté, de sécurité et de justice qui revêt de l'importance pour la protection des données: l'accès à la justice et à la justice en ligne.

III. **ASPECTS EXAMINÉS DANS L'AVIS**

11. Le présent avis analysera la communication et, plus généralement, l'avenir de l'espace de liberté, de sécurité et de justice tel qu'il est envisagé dans le cadre d'un nouveau programme pluriannuel en prenant comme principal angle de vue la nécessité de protéger les droits fondamentaux. Il s'inscrira également dans le prolongement des contributions du CEPD à l'élaboration de la politique de l'UE dans ce domaine, essentiellement dans le cadre de son rôle consultatif. À ce jour, le CEPD a adopté plus de 30 avis et observations sur des initiatives découlant du programme de La Haye, qui figurent tous sur son site internet.

12. Dans son analyse de la communication, le CEPD tiendra compte en particulier des quatre aspects énoncés ci-dessous, qui sont importants pour l'avenir de l'espace de liberté, de sécurité et de justice. Ils jouent tous également un rôle fondamental dans la communication.

13. Le premier aspect est la croissance exponentielle des informations numériques sur les citoyens à la suite des progrès réalisés dans les technologies de l'information et de la communication ([6]). La société se dirige vers ce que l'on appelle souvent la «société de la surveillance», dans laquelle chaque transaction et presque chaque geste des citoyens sont susceptibles de laisser une trace numérique. L'«internet des objets» et l'«environnement intelligent» connaissent déjà un développement rapide dû à l'utilisation des étiquettes RFID. Le recours aux caractéristiques numérisées du corps humain (biométrique) se généralise. Il en résulte un monde de plus en plus connecté, dans lequel les organisations chargées de la sécurité publique peuvent avoir accès à d'importants volumes d'informations potentiellement utiles, ce qui peut avoir une incidence directe sur la vie des personnes concernées.

14. Le deuxième aspect est l'internationalisation. À l'ère numérique, les échanges de données ne sont pas cantonnés à l'intérieur des frontières de l'Union européenne, alors que, dans le même temps, une coopération internationale portant sur l'ensemble des activités de l'UE dans le cadre de l'espace de liberté, de sécurité et de justice devient de plus en plus nécessaire: la lutte contre le terrorisme, la coopération policière et judiciaire, la justice civile et les contrôles aux frontières n'en sont que quelques exemples.

15. Le troisième aspect est l'utilisation des données à des fins répressives: en raison des menaces récentes, qu'elles soient ou non liées au terrorisme, auxquelles la société est exposée, les services répressifs disposent de possibilités accrues de collecter, conserver et échanger des données à caractère personnel (ou les demandent). Dans de nombreux cas, le secteur privé joue un rôle actif, comme en attestent, entre autres, la directive relative à la conservation des données ([7]) et les différents instruments concernant les dossiers passagers ([8]).

16. Le quatrième aspect est la libre circulation. Le développement progressif de l'espace de liberté, de sécurité et de justice requiert la poursuite de l'élimination des frontières internes et des obstacles éventuels à la libre circulation au sein de cet espace. Les nouveaux instruments adoptés dans ce domaine ne devraient en aucun cas créer de nouveaux obstacles. La libre circulation comprend, en l'occurrence, la libre circulation des personnes et la libre circulation des données (à caractère personnel).

17. Ces quatre aspects montrent que le contexte dans lequel les informations sont utilisées évolue rapidement. Il ne fait dès lors aucun doute qu'il est important de disposer d'un mécanisme solide pour protéger les droits fondamentaux des citoyens et, notamment, leur droit au respect de leur vie privée et à la protection de leurs données à caractère personnel. C'est pour ces motifs que le CEPD choisit le besoin de protection comme principal angle de vue pour son analyse, comme indiqué au point 11.

([6]) Le rapport sur les affaires intérieures évoque même, à ce propos, un «raz-de-marée numérique».

([7]) 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 de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE, JO L 105 du 13.4.2006, p. 54.

([8]) Voir, par exemple, l'accord entre l'Union européenne et les États-Unis d'Amérique sur le traitement et le transfert de données des dossiers passagers (données PNR) par les transporteurs aériens au ministère américain de la sécurité intérieure (DHS) (accord PNR 2007), JO L 204 du 4.8.2007, p. 18, et la proposition de décision-cadre du Conseil relative à l'utilisation des données des dossiers passagers (Passenger Name Record — PNR) à des fins répressives, COM(2007) 654 final.

IV. APPRÉCIATION GÉNÉRALE

18. La communication et le programme de Stockholm visent à préciser les intentions de l'UE pour les cinq prochaines années, et pourraient avoir des effets à plus long terme encore. Le CEPD constate que la Commission ne tient pas compte du traité de Lisbonne dans sa communication. Tout en comprenant la raison qui a motivé cette attitude, il déplore néanmoins que la Commission n'ait pas exploité toutes les possibilités supplémentaires offertes par ce traité. La perspective ouverte par le traité de Lisbonne sera mise davantage en exergue dans le présent avis.

19. La communication s'appuie sur les résultats des actions menées ces dernières années par l'UE dans le cadre de l'espace de liberté, de sécurité et de justice. Ces résultats peuvent être décrits comme déterminés par les événements, l'accent étant mis sur les mesures qui étendent les pouvoirs des autorités répressives et qui sont intrusives pour les citoyens. C'est particulièrement vrai dans les domaines où des données à caractère personnel sont utilisées et échangées de manière intensive et qui revêtent donc une importance capitale en ce qui concerne la protection des données. Les résultats sont déterminés par les événements en ce sens que des événements extérieurs tels que le 11 septembre et les attentats de Madrid et de Londres ont déclenché une intense activité législative. À titre d'exemple, le transfert aux États-Unis des données relatives aux passagers peut être considéré comme la conséquence du 11 septembre ([9]), tandis que les attentats de Londres ont conduit à l'adoption de la directive 2006/24/CE sur la conservation des données ([10]). La priorité est allée aux mesures intrusives, le législateur européen ayant privilégié des mesures qui facilitent l'utilisation et l'échange de données, alors que les mesures visant à garantir la protection des données à caractère personnel se voyaient attribuer un caractère moins urgent. La principale mesure de protection qui a été adoptée est la décision-cadre 2008/977/JAI du Conseil relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale ([11]), après trois ans de discussion au Conseil, dont le résultat n'est pas pleinement satisfaisant (voir points 29 et 30).

20. L'expérience de ces dernières années montre qu'avant d'adopter de nouveaux instruments, il convient de mener une réflexion sur les conséquences qu'auront ceux-ci pour les autorités répressives et les citoyens européens. Il faudrait, à cette fin, tenir dûment compte des coûts sur le plan du respect de la vie privée et de l'efficacité aux fins de la répression, en premier lieu lorsque de nouveaux instruments sont proposés et examinés, mais également après leur entrée en vigueur, au moyen de réexamens périodiques. Il est aussi essentiel de mener une telle réflexion avant de fixer dans un nouveau programme pluriannuel les principales initiatives pour le proche avenir.

21. Le CEPD se félicite du fait que, dans la communication, la protection des droits fondamentaux et, en particulier, la protection des données à caractère personnel, soit considérée comme l'une des questions clés en ce qui concerne l'avenir de l'espace de liberté, de sécurité et de justice. Au point 2 de la communication, l'UE est qualifiée d'espace unique pour la protection des droits fondamentaux fondés sur des valeurs communes. Il est également positif que l'adhésion à la Convention européenne des droits de l'homme soit mentionnée comme une question prioritaire — et même comme la première priorité — dans la communication. Cette adhésion est une étape importante en vue de mettre en place un système harmonieux et cohérent pour la protection des droits fondamentaux. Enfin et surtout, la protection des données se voit accorder une place de premier plan dans la communication.

22. Cette priorité de la communication témoigne d'une ferme intention de veiller à la protection des droits des citoyens et, ce faisant, d'adopter une approche plus équilibrée. Les gouvernements ont besoin d'instruments appropriés pour garantir la sécurité des citoyens mais, au sein de notre société européenne, ils sont tenus de respecter intégralement les droits fondamentaux de ces derniers. Pour que l'espace de liberté, de sécurité et de justice soit au service du citoyen ([12]), il faut une Union européenne qui maintienne cet équilibre.

23. Selon le CEPD, la communication prend très bien en compte la nécessité de maintenir un tel équilibre, y compris la nécessité d'assurer la protection des données à caractère personnel. Elle reconnaît qu'un changement de priorité est nécessaire. C'est important, car il convient d'éviter que les politiques menées dans le cadre de l'espace de liberté, de sécurité et de justice ne favorisent une évolution progressive vers une société de la surveillance. Le CEPD s'attend à ce que Conseil adopte la même approche dans le programme de Stockholm, en tenant compte notamment des orientations énoncées au point 25 ci-dessous.

24. C'est d'autant plus essentiel que l'espace de liberté, de sécurité et de justice façonne le cadre de vie des citoyens, en particulier la sphère privée, protégée par les droits fondamentaux, de leur responsabilité personnelle et de la sécurité politique et sociale, comme l'a très récemment déclaré la Cour constitutionnelle allemande dans son arrêt du 30 juin 2009 relatif au traité de Lisbonne ([13]).

([9]) L'accord PNR 2007 mentionné dans la note de base de page précédente et ses prédécesseurs.

([10]) 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 de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE, JO L 105 du 13.4.2006, p. 54. Bien qu'elle ait pour base juridique l'article 95 du traité CE, elle a été adoptée en réaction immédiate aux attentats de Londres.

([11]) 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, JO L 350 du 30.12.2008, p. 60.

([12]) Voir le titre de la communication.

([13]) Communiqué de presse n° 72/2009 de la Cour constitutionnelle fédérale d'Allemagne du 30 juin 2009, point 2 c).

25. Le CEPD souligne que, dans un tel domaine:

— l'échange d'informations entre les autorités des États membres, y compris, le cas échéant, avec les instances ou bases de données européennes, devrait suivre des mécanismes adéquats et efficaces qui respectent intégralement les droits fondamentaux des citoyens et garantissent la confiance mutuelle,

— cela suppose non seulement la disponibilité des informations, ainsi que la reconnaissance mutuelle des systèmes juridiques des États membres (et de l'UE), mais également une harmonisation des normes de protection des informations, au moyen, par exemple, d'un cadre commun pour la protection des données,

— l'application de ces normes communes ne devrait pas être limitée aux seules situations présentant des dimensions transfrontières. La confiance mutuelle ne peut exister que lorsque les normes sont solides et systématiquement respectées, que la dimension transfrontière soit présente ou non. En outre, en particulier lorsqu'il s'agit de l'utilisation des informations, les différences entre données «internes» et «transfrontières» ne peuvent fonctionner dans la pratique ([14]).

V. **INSTRUMENTS RELATIFS À LA PROTECTION DES DONNÉES**

V.1. **Vers un régime complet de protection des données**

26. Le CEPD approuve l'approche stratégique consistant à accorder, dans la communication, une place de premier plan à la protection des données. En effet, de nombreuses initiatives menées dans le cadre de l'espace de liberté, de sécurité et de justice reposent sur l'utilisation de données à caractère personnel, et une bonne protection des données est indispensable à leur succès. Le respect de la vie privée et la protection des données ne constituent pas seulement une obligation légale de plus en plus largement admise au niveau de l'UE, mais également une question capitale pour les citoyens européens, comme le montrent les résultats de l'Eurobaromètre ([15]). En outre, la limitation de l'accès aux données à caractère personnel est également essentielle pour obtenir la confiance des services répressifs.

27. Au point 2.3 de la communication, un régime complet de protection des données couvrant tous les domaines de compétence de l'UE est jugé nécessaire ([16]). Le CEPD soutient sans réserve cet objectif, indépendamment de l'entrée en vigueur du traité de Lisbonne. Il note également qu'un tel régime ne signifie pas nécessairement qu'un cadre juridique unique sera appliqué à tous les traitements. Dans le cadre des traités actuellement en vigueur, les possibilités d'adopter un cadre juridique complet applicable à l'ensemble des traitements sont limitées en raison de la structure en piliers et du fait que — dans le premier pilier du moins — la protection des données traitées par les institutions européennes est garantie en vertu d'une base juridique distincte (l'article 286 du traité CE). Cependant, le CEPD fait observer que certaines améliorations pourraient être apportées en exploitant pleinement les possibilités offertes par les traités actuels, comme la Commission l'a déjà souligné dans sa communication intitulée «Mise en œuvre du programme de La Haye: la voie à suivre» ([17]). Après l'entrée en vigueur du traité de Lisbonne, l'article 16 du traité sur le fonctionnement de l'Union européenne fournira la base juridique nécessaire pour un cadre juridique complet applicable à l'ensemble des traitements.

28. Le CEPD note qu'il est fondamental, en tout état de cause, d'assurer la cohérence du cadre juridique relatif à la protection des données, si nécessaire par l'harmonisation et la consolidation des différents instruments juridiques applicables dans l'espace de liberté, de sécurité et de justice.

Dans le cadre des traités actuellement en vigueur

29. Une première étape a été franchie récemment avec l'adoption de la décision-cadre 2008/977/JAI du Conseil ([18]). Toutefois, cet instrument juridique ne peut être considéré comme un cadre complet puisque ses dispositions n'ont pas de portée générale. Elles ne s'appliquent pas aux situations internes, lorsque les données à caractère personnel proviennent de l'État membre qui les utilise. Cette limite ne peut que diminuer la valeur ajoutée de la décision-cadre du Conseil, à moins que tous les États membres ne décident d'inclure les situations internes dans la législation nationale transposant ses dispositions, ce qui est peu probable.

30. La deuxième raison pour laquelle le CEPD estime que la décision-cadre 2008/977/JAI du Conseil ne contient pas un cadre satisfaisant à long terme pour la protection des données dans un espace de liberté, de sécurité et de justice est que plusieurs de ses dispositions essentielles ne sont pas comptabiles avec la directive 95/46/CE. Dans le cadre des traités actuellement en vigueur, une deuxième étape pourrait consister à élargir le champ d'application de la décision-cadre du Conseil et à la rendre conforme à la directive 95/46/CE.

31. L'élaboration d'une vision claire et à long terme pourrait imprimer un nouvel élan à la réalisation d'un régime complet de protection des données. Cette vision pourrait comprendre une approche globale et cohérente en ce qui concerne la définition de la collecte et des échanges de données — ainsi que l'exploitation des bases de données existantes — et, dans le même temps, les garanties relatives

([14]) Le CEPD a développé ce dernier point dans son avis du 19 décembre 2005 sur la proposition de décision-cadre du Conseil relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale [COM(2005) 475 final], JO C 47 du 25.2.2006, p. 27, points 30 à 32.

([15]) La protection des données au sein de l'Union européenne — Les perceptions des citoyens — Rapport analytique, Flash Eurobaromètre 225, janvier 2008, http://www.ec.europa.eu/public_opinion/flash/fl_225_en.pdf

([16]) Voir également les orientations prioritaires de la communication.

([17]) COM(2006) 331 final du 28 juin 2006.

([18]) Voir note 11.

à la protection des données. Elle devrait prévenir les empiètements et les doubles emplois entre les instruments (et donc entre les traitements de données à caractère personnel). Elle devrait aussi favoriser la cohérence des politiques de l'UE dans ce domaine et la confiance dans la manière dont les autorités publiques traitent les données des citoyens. Le CEPD recommande au Conseil d'annoncer la nécessité d'une vision claire et à long terme dans le programme de Stockholm.

32. Le CEPD recommande également d'évaluer et de mettre en perspective les mesures qui ont déjà été adoptées dans ce domaine, ainsi que leur application concrète et leur efficacité. Il conviendrait, dans le cadre de cette évaluation, de tenir dûment compte des coûts des mesures précitées sur le plan du respect de la vie privée et de leur efficacité aux fins de la répression. Si ces évaluations devaient révéler que certaines mesures ne produisent pas les résultats escomptés ou ne sont pas proportionnées aux finalités poursuivies, les actions suivantes devraient être envisagées:

— en premier lieu, modifier ou abroger les mesures qui n'apparaissent pas suffisamment justifiées par l'apport d'une valeur ajoutée concrète pour les autorités répressives et les citoyens européens,

— en deuxième lieu, examiner les possibilités d'améliorer l'application des mesures existantes,

— en troisième lieu seulement, proposer de nouvelles mesures législatives s'il est vraisemblable que celles-ci soient nécessaires aux fins envisagées. De nouveaux instruments ne devraient être adoptés que s'ils apportent une valeur ajoutée claire et concrète pour les autorités répressives et les citoyens européens.

Le CEPD recommande de faire référence à un système d'évaluation des mesures existantes dans le programme de Stockholm.

33. Enfin et surtout, il conviendrait d'accorder une attention particulière à une meilleure mise en œuvre des garanties existantes, conformément à la communication de la Commission sur le suivi du programme de travail pour une meilleure mise en application de la directive sur la protection des données ([19]) et aux suggestions formulées par le CEPD dans son avis sur cette communication ([20]). La Commission ne peut malheureusement pas lancer de procédures d'infraction dans le cadre du troisième pilier.

Dans le cadre du traité de Lisbonne

34. Le traité de Lisbonne ouvre la possibilité de mettre en place un véritable cadre complet pour la protection des données. L'article 16, paragraphe 2, du traité sur le fonctionnement de l'Union européenne impose au Conseil et au Parlement européen de fixer les règles relatives à la protection des données par les institutions, organes et organismes de l'Union, ainsi que par les États membres dans l'exercice d'activités qui relèvent du champ d'application du droit de l'Union et par les acteurs privés.

35. Le CEPD comprend que l'accent placé dans la communication sur un régime complet de protection des données traduit l'ambition de la Commission de proposer un cadre juridique applicable à tous les traitements. Il approuve sans réserve cette ambition, qui aurait pour résultats d'améliorer la cohérence du système, de garantir la sécurité juridique et, par conséquent, de renforcer la protection. Elle éviterait notamment de se trouver confronté dans le futur à la difficulté que représente le traçage d'une ligne de démarcation entre les piliers lorsque des données collectées dans le secteur privé à des fins commerciales sont utilisées ensuite à des fins répressives. Cette ligne de démarcation entre les piliers ne reflète pas totalement la réalité, comme le montrent les importants arrêts rendus par la Cour de justice dans des affaires relatives aux dossiers passagers ([21]) et à la conservation des données ([22]).

36. Le CEPD propose de souligner dans le programme de Stockholm cette justification d'un régime complet de protection des données. Elle montre qu'un tel régime n'est pas une simple préférence mais une nécessité due à l'évolution des pratiques concernant l'utilisation des données. Le CEPD recommande d'inscrire parmi les priorités du programme de Stockholm la nécessité d'adopter un nouveau cadre législatif pour remplacer, entre autres, la décision-cadre 2008/977/JAI du Conseil.

37. Le CEPD souligne que le concept d'un régime complet de protection des données basé sur un cadre juridique général n'exclut pas l'adoption de règles complémentaires relatives à la protection des données dans le secteur policier et judiciaire. Ces règles pourraient tenir compte des besoins spécifiques du secteur répressif, comme le prévoit la déclaration 21 annexée au traité de Lisbonne ([23]).

V.2. **Rappel des principes relatifs à la protection des données**

38. La Communication relève les évolutions technologiques qui transforment la communication entre les particuliers et les organisations publiques et privées. Elles requièrent, selon la Commission, le rappel d'un certain nombre de principes fondamentaux relatifs à la protection des données.

([19]) COM(2007) 87 final du 7.3.2007.

([20]) Avis du 25 juillet 2007, JO C 255 du 27.10.2007, p. 1. Voir en particulier le point 30.

([21]) Arrêt de la Cour du 30 mai 2006 dans les affaires jointes C-317/04 et C-318/04, Parlement européen/Conseil (C-317/04) et Commission des Communautés européennes (C-318/04), Recueil 2006, p. I-4721.

([22]) Arrêt de la Cour du 10 février 2009 dans l'affaire C-301/06, Irlande/Parlement européen et Conseil, non encore publié.

([23]) Voir la déclaration 21 sur la protection des données à caractère personnel dans le domaine de la coopération judiciaire en matière pénale et de la coopération policière, annexée à l'acte final de la conférence intergouvernementale qui a adopté le traité de Lisbonne, JO C 115 du 9.5.2008, p. 345.

39. Le CEPD se félicite de cette intention. Une évaluation de l'efficacité de ces principes à la lumière des évolutions technologiques est extrêmement utile. En premier lieu, il est important de noter que le rappel et la réaffirmation des principes relatifs à la protection des données ne doivent pas toujours être directement liés aux évolutions technologiques. Cela pourrait également être nécessaire dans d'autres perspectives, mentionnées dans la partie III ci-dessus, telles que l'internationalisation, l'utilisation croissante de données à des fins répressives et la libre circulation.

40. En outre, le CEPD estime que cette évaluation peut être réalisée dans le cadre de la consultation publique qui a été annoncée par la Commission lors de la conférence «Données personnelles — plus d'utilisation, plus de protection?», qui s'est tenue les 19 et 20 mai 2009. Cette consultation publique pourrait apporter une contribution précieuse ([24]). Le CEPD suggère que le lien entre les intentions annoncées au point 2.3 de la communication et la consultation publique sur l'avenir de la protection des données soit souligné par le Conseil dans le texte du programme de Stockholm et par la Commission dans ses déclarations publiques sur la consultation.

41. Une telle évaluation pourrait porter, par exemple, sur les points suivants:

— les données à caractère personnel dans le cadre de l'espace de liberté, de sécurité et de justice sont généralement d'une nature particulièrement sensibles, comme c'est le cas des données relatives aux condamnations pénales, des données détenues par les services de police et des données biométriques, telles que les empreintes digitales et les profils ADN,

— leur traitement peut avoir des conséquences négatives pour les personnes concernées, compte tenu en particulier des pouvoirs coercitifs que détiennent les autorités répressives. En outre, le contrôle et l'analyse des données sont de plus en plus automatisés et très souvent réalisés sans intervention humaine. La technologie permet l'utilisation de bases de données contenant des données à caractère personnel à des fins de recherche générale (fouille de données («data mining», profilage, etc.). Les obligations légales sur lesquelles est basé le traitement de données devraient être clairement précisées,

— l'une des pierres angulaires de la législation relative à la protection des données est que les données à caractère personnel doivent être collectées à des fins déterminées et ne peuvent être utilisées d'une manière qui soit incompatible avec ces fins. L'utilisation à des fins incompatibles ne devrait être autorisée que dans la mesure où elle est prévue par la loi et nécessaire à la poursuite d'intérêts publics spécifiques, tels que ceux prévus à l'article 8, paragraphe 2, de la Convention européenne des droits de l'homme,

— la nécessité de respecter le principe de la limitation de la finalité pourrait avoir des incidences sur les tendances actuelles en matière d'utilisation des données. Les services répressifs utilisent des données qui ont été collectées par des sociétés privées à des fins commerciales, dans les secteurs des télécommunications, des transports et de la finance. En outre, des systèmes d'information à grande échelle sont mis en place, notamment dans les domaines de l'immigration et des contrôles aux frontières. Par ailleurs, des interconnexions entre bases de données et des accès à celles-ci sont autorisés, élargissant ainsi les finalités pour lesquelles les données à caractère personnel ont été initialement collectées. Il convient de mener une réflexion sur ces tendances actuelles, y compris sur les adaptations et/ou sauvegardes additionnelles possibles, le cas échéant,

— outre les principes relatifs à la protection des données mentionnés dans la communication, l'évaluation devrait porter sur la nécessité d'assurer la transparence du traitement, qui permet aux personnes concernées d'exercer leurs droits. La transparence est une question particulièrement délicate dans le domaine répressif, notamment parce qu'elle doit être mise en balance avec les risques qu'elle fait peser sur les enquêtes,

— il convient de trouver des solutions pour les échanges avec les pays tiers.

42. L'évaluation devrait par ailleurs examiner les possibilités d'améliorer l'effectivité de l'application des principes relatifs à la protection des données. Dans ce contexte, il pourrait être utile d'accorder une attention particulière aux instruments susceptibles de renforcer les responsabilités des responsables de traitements. Ces instruments doivent permettre de leur faire assumer l'entière responsabilité de la gestion des données. La «gouvernance des données» est une notion utile dans ce contexte. Elle englobe tous les moyens légaux, techniques et organisationnels par lesquels les organisations assurent une pleine responsabilisation quant à la manière dont les données sont gérées, telles que la planification et le contrôle, l'utilisation d'une technologie bien conçue, la formation adéquate du personnel, les audits de conformité, etc.

V.3. **Technologies respectueuses de la vie privée**

43. Le CEPD se félicite que le point 2.3 de la communication fasse référence à la certification relative au respect de la vie privée. Une référence pourrait également être faite à la notion de «prise en compte du respect de la vie privée dès la conception» («privacy by design»), ainsi qu'à la nécessité d'identifier les meilleures techniques disponibles qui soient conformes au cadre de l'UE relatif à la protection des données.

44. Selon le CEPD, la prise en compte du respect de la vie privée dès la conception et les technologies respectueuses de la vie privée pourraient constituer des instruments utiles pour une meilleure protection, ainsi que pour une utilisation plus efficace de l'information. Il suggère deux voies à suivre, qui ne sont pas incompatibles:

— un système de certification relative au respect de la vie privée et à la protection des données ([25]) comme option pour les constructeurs et les utilisateurs de systèmes d'information, soutenu ou non par un financement ou une mesure législative de l'UE,

([24]) Le groupe de l'article 29 sur la protection des données, auquel le CEPD participe, a décidé de préparer activement sa contribution à cette consultation publique.

([25]) Le «European Privacy Seal» (EuroPriSe) (label européen de protection des données à caractère personnel) en est un exemple.

— une obligation légale pour les constructeurs et les utilisateurs de systèmes d'information d'utiliser des systèmes respectant le principe de la prise en compte du respect de la vie privée dès la conception. Il peut être nécessaire à cette fin d'élargir le champ d'application actuel de la législation relative à la protection des données afin de rendre les constructeurs responsables des systèmes d'information qu'ils développent ([26]).

Le CEPD suggère de mentionner ces deux voies possibles dans le programme de Stockholm.

V.4. **Aspects externes**

45. Un autre sujet mentionné dans la communication est la mise au point et la promotion de normes internationales pour la protection des données. De nombreuses activités visant à établir des normes applicables à l'échelle mondiale sont menées actuellement, par exemple par la Conférence internationale des commissaires à la protection des données et de la vie privée. Dans un avenir proche, ces travaux pourraient déboucher sur un accord international. Le CEPD suggère que le programme de Stockholm soutienne ces activités.

46. La communication fait également état de la conclusion d'accords bilatéraux, sur la base des progrès déjà réalisés avec les États-Unis. Le CEPD partage l'avis selon lequel un cadre juridique clair est nécessaire pour le transfert de données aux pays tiers et a donc accueilli positivement les travaux menés conjointement par les autorités de l'UE et des États-Unis au sein du groupe de contact à haut niveau concernant un éventuel instrument transatlantique pour la protection des données, tout en préconisant de faire preuve d'une plus grande clarté et d'accorder davantage d'attention à certaines questions ([27]). À cet égard, il est également intéressant de relever les idées formulées dans le rapport sur les affaires intérieures à propos d'un espace transatlantique de coopération en matière de liberté, sécurité et justice sur lequel, selon le rapport, l'UE devrait prendre une décision d'ici à 2014. Un tel espace ne sera pas possible sans garanties adéquates en matière de protection des données.

47. Le CEPD estime que les normes européennes pour la protection des données, fondées sur la convention 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ([28]), ainsi que sur la jurisprudence de la Cour de justice des Communautés européenne et de la Cour européenne des droits de l'homme, devraient déterminer le niveau de protection offert par un accord général avec les États-Unis sur la protection et l'échange de données. Cet accord général pourrait servir de base à des arrangements spécifiques relatifs à l'échange de données à caractère personnel. Cet aspect est d'autant plus important au regard de l'intention formulée au point 4.2.1 de la communication, qui prévoit que l'Union européenne devra conclure, lorsque nécessaire, des accords de coopération policière.

48. Le CEPD comprend parfaitement qu'il est nécessaire d'améliorer la coopération internationale, y compris, dans certains cas, avec des pays qui ne protègent pas les droits fondamentaux. Il est toutefois ([29]) indispensable de tenir compte du fait que cette coopération internationale risque d'entraîner une intensification importante de la collecte et du transfert international de données. Dès lors, il est essentiel que les principes du traitement loyal et licite — ainsi que les principes du respect des procédures en général — s'appliquent à la collecte et au transfert de données à caractère personnel sur l'ensemble du territoire de l'UE, et que les données à caractère personnel ne soient transférées à des pays tiers ou à des organisations internationales que si ces tiers garantissent un niveau de protection adéquat ou d'autres mesures de protection appropriées.

49. En conclusion, le CEPD recommande de souligner, dans le programme de Stockholm, l'importance de conclure des accords généraux avec les États-Unis et d'autres pays tiers concernant la protection des données et l'échange de données, sur la base du niveau de protection garanti sur l'ensemble du territoire de l'UE. Dans une perspective plus large, il insiste sur l'importance de promouvoir activement le respect des droits fondamentaux et, en particulier, la protection des données auprès des pays tiers et des organisations internationales ([30]). En outre, le programme de Stockholm pourrait faire référence au principe général selon lequel l'échange de données à caractère personnel avec des pays tiers requiert un niveau adéquat de protection ou d'autres mesures de protection appropriées dans ces pays.

VI. **UTILISATION DES INFORMATIONS**

VI.1. **Vers un modèle européen d'information**

50. Un meilleur échange d'informations est un objectif politique essentiel pour l'Union européenne, au sein de l'espace de liberté, de sécurité et de justice. Le point 4.1.2 de la communication souligne que la sécurité dans l'Union repose sur des mécanismes performants d'échanges d'informations entre les autorités nationales et les autres acteurs européens. En l'absence d'une force de police européenne, d'un système européen de justice pénale et d'un système européen de contrôles aux frontières, il est logique de mettre ainsi l'accent sur l'échange d'informations.

([26]) Les utilisateurs de systèmes d'informations sont couverts par la législation relative à la protection des données, en tant que responsables de traitements ou sous-traitants.

([27]) Voir l'avis du CEPD du 11 novembre 2008 concernant le rapport final du groupe de contact à haut niveau UE/États-Unis sur le partage d'informations et la protection de la vie privée et des données à caractère personnel, JO C 128 du 6.6.2009, p. 1.

([28]) STE n° 108 du 28.1.1981.

([29]) Voir la lettre du CEPD du 28 novembre 2005 concernant la communication de la Commission intitulée «Une stratégie relative à la dimension externe de l'espace de liberté, de sécurité et de justice», disponible sur le site internet du CEPD.

([30]) La jurisprudence récente relative aux listes de terroristes confirme que des garanties sont nécessaires — également dans les relations avec les Nations unies — afin de s'assurer que les mesures de lutte contre le terrorisme sont conformes aux normes de l'UE relatives aux droits fondamentaux (affaires jointes C-402/05 et C-415/05 P, Kadi et Al Barakaat International Foundation/Conseil, arrêt du 3 septembre 2008, non encore publié).

Les mesures relatives à l'information constituent donc des contributions fondamentales de l'Union européenne qui permettent aux autorités des États membres de lutter efficacement contre la criminalité transfrontière et de protéger les frontières extérieures de manière performante. Elles ne contribuent toutefois pas seulement à la sécurité des citoyens mais également à leur liberté — la libre circulation des personnes a été citée précédemment parmi les aspects examinés dans le présent avis — et à la justice.

51. C'est précisément pour ces raisons que le principe de disponibilité a été introduit dans le programme de La Haye. Il suppose que les informations nécessaires à la lutte contre la criminalité puissent franchir sans entraves les frontières intérieures de l'UE. Des expériences récentes montrent qu'il a été difficile de mettre en œuvre ce principe dans des mesures législatives. La proposition de décision-cadre du Conseil du 12 octobre 2005 relative à l'échange d'informations en vertu du principe de disponibilité ([31]) n'a pas été acceptée par le Conseil. Les États membres n'étaient pas prêts à accepter toutes les conséquences du principe de disponibilité. La préférence a été accordée à des instruments de portée plus limitée ([32]), tels que 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 («décision de Prüm») ([33]).

52. Si le principe de disponibilité se trouvait au cœur du programme de La Haye, la Commission semble adopter à présent une approche plus modeste. Elle envisage de stimuler davantage l'échange d'informations entre les autorités des États membres en introduisant un modèle européen d'information. La présidence suédoise de l'UE suit la même ligne ([34]). Elle présentera une proposition de stratégie pour l'échange d'informations. Le Conseil a déjà entamé ses travaux sur ce projet ambitieux de stratégie européenne de gestion de l'information, qui est étroitement lié au modèle européen d'information. Le CEPD prend note de ces évolutions avec grand intérêt et souligne qu'il convient, dans le cadre de ces projets, d'accorder l'attention voulue aux éléments relatifs à la protection des données.

Le modèle européen d'information et la protection des données

53. Avant toute chose, il convient de souligner que l'avenir de l'espace de liberté, de sécurité et de justice ne devrait pas être déterminé par les technologies, c'est-à-dire que les possibilités presque illimitées offertes par les nouvelles technologies devraient toujours être passées au crible des principes relatifs à la protection des données et utilisées uniquement dans la mesure où elles sont conformes à ces principes.

54. Le CEPD note que la communication ne présente pas le modèle d'information comme un simple modèle technique, doté d'une puissante capacité d'analyse stratégique et permettant une meilleure collecte et un meilleur traitement des informations opérationnelles. Elle reconnaît également que les aspects d'ordre politique, tels que les critères régissant la collecte, le partage et le traitement des informations, devraient être pris en considération, dans le respect des principes relatifs à la protection des données.

55. Les technologies de l'information et le cadre juridique sont — et demeureront — tous deux essentiels. Le CEPD se félicite que la communication parte du principe selon lequel un modèle européen d'information ne peut être conçu sur la base de considérations techniques. Il est fondamental que les informations soient collectées, partagées et traitées uniquement sur la base de besoins concrets en matière de sécurité et en tenant compte des principes relatifs à la protection des données. Le CEPD adhère également sans réserve à l'idée qu'il est nécessaire de mettre au point un mécanisme de suivi pour examiner comment l'échange d'informations fonctionne. Il suggère que le Conseil développe ces éléments dans le programme de Stockholm.

56. Dans ce contexte, le CEPD souligne que la protection des données, qui vise à protéger les citoyens, ne doit pas être considérée comme un obstacle à une gestion efficace des données. Elle fournit d'importants outils pour améliorer la conservation et l'échange des informations, ainsi que l'accès à celles-ci. Les droits des personnes concernées d'être informées des données les concernant qui font l'objet d'un traitement et d'obtenir la rectification des données inexactes peuvent également améliorer l'exactitude des données contenues dans les systèmes de gestion des données.

57. La législation relative à la protection des données comporte en substance les conséquences suivantes: si des données sont nécessaires à une fin spécifique et légitime, elles peuvent être utilisées; si elles ne sont pas nécessaires à une fin bien déterminée, les données à caractère personnel ne devraient pas être utilisées. Dans le premier cas, des mesures additionnelles peuvent être requises pour fournir des garanties adéquates.

58. Le CEPD émet cependant des réserves quant au fait que la communication mentionne l'«identification des besoins futurs» en tant que partie intégrante du modèle d'information. Il souligne que, dans le futur également, le principe de la limitation de la finalité devrait servir de principe directeur lors de la mise en place des systèmes d'information ([35]). C'est l'une des garanties fondamentales que le système de protection des données fournit au citoyen: ce dernier doit savoir à l'avance pour quelle finalité des données le concernant sont collectées et qu'elles ne seront utilisées que pour cette finalité, notamment dans le futur. Cette garantie est d'ailleurs consacrée à l'article 8 de la Charte des droits fondamentaux de l'Union européenne. Le principe de la limitation de la finalité connaît des exceptions — revêtant une importance particulière dans le cadre de l'espace de liberté, de sécurité et de justice -, qui ne devraient toutefois pas déterminer la construction d'un système.

([31]) COM(2005) 490 final.

([32]) Du point de vue de la disponibilité, la décision de Prüm contient des dispositions ambitieuses concernant l'utilisation des données biométriques (ADN et empreintes digitales).

([33]) JO L 210 du 6.8.2008, p. 1.

([34]) Voir le programme de travail de l'UE établi par le gouvernement cité dans la note 5, page 2.

([35]) Voir aussi le point 41 ci-dessus.

Choisir l'architecture adéquate

59. Choisir l'architecture adéquate pour l'échange d'informations est le point de départ de tout le processus. L'importance de disposer d'architectures d'information appropriées est reconnu dans la communication (point 4.1.3), mais, et c'est regrettable, uniquement en ce qui concerne l'interopérabilité.

60. Le CEDP souligne un autre aspect: dans le cadre du modèle européen d'information, les exigences en matière de protection des données devraient faire partie intégrante du processus de développement du système et ne devraient pas être simplement considérées comme une condition nécessaire de la légalité d'un système ([36]). Il convient de tenir compte de la notion de «prise en compte du respect de la vie privée dès la conception» et de la nécessité d'identifier les «meilleures techniques disponibles» ([37]), comme indiqué au point 43 ci-dessus. Le modèle européen d'information devrait être fondé sur ces notions, ce qui signifie plus concrètement que les systèmes d'information élaborés à des fins de sécurité publique devraient toujours être construits conformément au principe de la « prise en compte du respect de la vie privée dès la conception». Le CEPD recommande au Conseil d'inclure ces éléments dans le programme de Stockholm.

Interopérabilité des systèmes

61. Le CEPD souligne que l'interopérabilité n'est pas une question purement technique mais qu'elle a également des conséquences pour la protection du citoyen, en particulier la protection des données. Du point de vue de la protection des données, l'interopérabilité des systèmes, si elle est réalisée efficacement, présente des avantages évidents aux fins d'éviter une double conservation. Néanmoins, il est également évident que rendre techniquement possible l'accès à des données ou leur échange constitue, dans de nombreux cas, une puissante incitation à y accéder de facto ou à les échanger. En d'autres termes, l'interopérabilité comporte des risques particuliers d'interconnexion entre des bases de données poursuivant des finalités différentes ([38]). Elle peut affecter les strictes limitations de la finalité des bases de données.

62. En résumé, le simple fait qu'il soit techniquement possible de procéder à des échanges d'informations numériques entre des bases de données interopérables ou de fusionner ces bases de données ne justifie pas qu'il soit fait exception au principe de la limitation de la finalité. L'interopérabilité devrait, dans des cas concrets, reposer sur des choix politiques clairs et rigoureux. Le CEPD suggère de spécifier cette notion dans le programme de Stockholm.

([36]) Voir le document intitulé «Guidelines and criteria for the development, implementation and use of Privacy Enhancing Security Technologies» (lignes directrices et critères pour le développement, la mise en oeuvre et l'utilisation des technologies de sécurité renforçant la protection de la vie privée) (http://www.prise.oeaw.ac.at).

([37]) Par «meilleures techniques disponibles», on entend le stade de développement le plus efficace et avancé des activités et de leurs modes d'exploitation, démontrant l'aptitude pratique de techniques particulières à constituer, en principe, la base d'applications et de systèmes d'information et de communication qui soient conformes à l'exigence du respect de la vie privée, de la protection des données et de la sécurité figurant dans le cadre réglementaire de l'UE.

([38]) Voir les observations du CEPD relatives à la communication de la Commission sur l'interopérabilité des bases de données européennes, 10 mars 2006, disponible à l'adresse suivante: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consuultation/Comments/2006/06-03-10_Interoperability_EN.pdf

VI.2. **Utilisation des informations collectées à d'autres fins**

63. La communication n'évoque pas explicitement l'une des plus importantes tendances observées ces dernières années: l'utilisation à des fins répressives de données collectées dans le secteur privé à des fins commerciales. Cette tendance n'est pas uniquement liée aux données générées par l'utilisation des communications électroniques et aux données des passagers aériens qui se rendent dans certains pays tiers ([39]); elle concerne également le secteur financier. La directive 2005/60/CE du Parlement européen et du Conseil du 26 octobre 2005 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux et du financement du terrorisme ([40]) en est un exemple. Un autre exemple bien connu et très controversé concerne le traitement, par la Society for Worldwide Interbank Financial Telecommunication (SWIFT) ([41]), de données à caractère personnel nécessaires aux fins du programme de surveillance des transactions financières de terroristes du ministère des finances des États-Unis.

64. Le CEPD estime que ces tendances requièrent une attention particulière dans le programme de Stockholm. Elles peuvent être considérées comme des dérogations au principe de la limitation de la finalité et sont souvent très intrusives sur le plan de la vie privée car les données utilisées peuvent révéler beaucoup sur le comportement des individus. Chaque fois que des mesures intrusives sont proposées, il doit exister des preuves très solides de leur nécessité. Si ces preuves sont fournies, il convient de veiller à ce que les droits des personnes bénéficient d'une protection totale.

65. Selon le CEPD, l'utilisation à des fins répressives de données à caractère personnel collectées à des fins commerciales ne devrait être autorisée que dans des conditions strictes, telles que celles énoncées ci-dessous:

— les données sont utilisées uniquement à des fins bien spécifiées, telles que la lutte contre le terrorisme ou les formes graves de criminalité, à déterminer au cas par cas,

— les données sont transférées via un système «push» plutôt que par un système «pull» ([42]),

([39]) Voir point 15 ci-dessus.

([40]) JO L 309 du 25.11.2005, p. 15.

([41]) Voir l'avis 10/2006 du groupe de l'article 29 sur le traitement des données à caractère personnel par la Society for Worldwide Interbank Financial Telecommunication (SWIFT).

([42]) Dans le cadre du système «push», le responsable du traitement transmet les données à la demande du service répressif. Dans le cadre du système « pull», le service répressif a accès à la base de données du responsable du traitement et en extrait les informations. Dans le deuxième cas, il est plus difficile pour le responsable du traitement d'exercer sa responsabilité.

— les demandes de données devraient être proportionnées, étroitement ciblées et, en principe, fondées sur des suspicions concernant des personnes déterminées,

— les recherches à caractère routinier, la fouille de données et le profilage devraient être évités,

— toute utilisation de données à des fins répressives devrait être journalisée afin de permettre un contrôle effectif de cette utilisation par la personne concernée exerçant ses droits, par les autorités chargées de la protection des données et par le pouvoir judiciaire.

VI.3. **Systèmes d'information et organes de l'UE**

Systèmes d'information avec ou sans stockage centralisé ([43])

66. Au cours des dernières années, le nombre de systèmes d'information fondés sur la législation de l'UE s'est accru sensiblement au sein de l'espace de liberté, de sécurité et de justice. Il est parfois décidé d'établir un système qui implique le stockage centralisé de données au niveau européen, alors que, dans d'autres cas, la législation ne prévoit que l'échange d'informations entre bases de données nationales. Le système d'information Schengen constitue probablement le meilleur exemple d'un système avec stockage centralisé. La décision 2008/615/JAI du Conseil (décision de Prüm) ([44]) contient, du point de vue de la protection des données, l'exemple le plus significatif d'un système sans stockage centralisé puisqu'elle prévoit un échange massif de données biométriques entre les autorités des États membres.

67. La communication montre que cette tendance à la création de nouveaux systèmes se poursuivra. Un premier exemple, tiré du point 4.2.2, est le système d'information étendant le système européen d'information sur les casiers judiciaires (ECRIS) aux ressortissants de pays non membres de l'UE. La Commission a déjà commandé une étude sur un fichier européen des ressortissants de pays tiers ayant fait l'objet d'une condamnation, qui conduira peut-être à la création d'une base de données centralisée. L'échange d'informations sur les personnes inscrites dans les registres d'insolvabilité d'autres États membres, dans le cadre de la justice en ligne (point 3.4.1 de la communication), sans stockage centralisé, en est un deuxième exemple.

68. Un système décentralisé offre certains avantages du point de vue de la protection des données. Il évite le double stockage des données — par l'autorité de l'État membre concerné et dans le système centralisé —, la responsabilité concernant les données est claire puisque l'autorité de l'État membre sera responsable du traitement, et le contrôle par le pouvoir judiciaire et les autorités chargées de la protection des données peut être exercé au niveau des États membres. Néanmoins, ce système présente également des désavantages lorsque des données sont échangées avec d'autres juridictions, par exemple lorsqu'il s'agit de veiller à ce que les informations soient mises à jour tant dans le pays d'origine que dans le pays de destination et en ce qui concerne la façon de garantir un contrôle efficace dans les deux pays. Il est plus délicat encore de déterminer à qui échoit la responsabilité du système technique utilisé pour les échanges. Ces désavantages peuvent être surmontés en optant pour un système centralisé dont la responsabilité incombe aux organes européens, à tout le moins pour certaines parties du système (telles que l'infrastructure technique).

69. Dans ce contexte, il serait utile de mettre au point des critères concrets permettant de trancher entre systèmes centralisés ou décentralisés, afin de pouvoir faire des choix politiques clairs et rigoureux dans des cas pratiques. Ces critères pourraient contribuer au fonctionnement des systèmes proprement dits, ainsi qu'à la protection des données des citoyens. Le CEPD suggère de mentionner l'intention d'élaborer de tels critères dans le programme de Stockholm.

Systèmes d'information à grande échelle

70. Le point 4.2.3.2 de la communication se penche brièvement sur l'avenir des systèmes d'information à grande échelle, en accordant une attention particulière au système d'information Schengen (SIS) et au système d'information sur les visas (VIS).

71. Le point 4.2.3.2 fait également état de la création d'un système électronique d'enregistrement des entrées sur le territoire des États membres et des sorties de ce territoire, ainsi que des programmes d'enregistrement des voyageurs. Ce système a été annoncé précédemment par la Commission dans le cadre du «paquet frontières», à l'initiative du vice-président Frattini ([45]). Dans ses observations préliminaires ([46]), le CEPD s'est montré assez critique vis-à-vis de cette proposition en estimant que la nécessité d'un système aussi intrusif, qui viendrait s'ajouter aux système à grande échelle existants, n'avait pas été suffisamment démontrée. Le CEPD ne relève aucun nouvel élément justifiant un tel système et suggère dès lors au Conseil de ne pas mentionner cette idée dans le programme de Stockholm.

72. Dans ce contexte, le CEPD souhaite faire référence aux avis qu'il a rendus sur différentes initiatives dans le domaine de l'échange d'informations au sein de l'UE ([47]), dans lesquels il a formulé de nombreuses suggestions et observations sur les incidences que l'utilisation de grandes bases de données au niveau de l'UE pourrait avoir sur la protection des données. Il a, entre autres, accordé une attention particulière à la nécessité de mettre en place des garanties

([43]) Le stockage centralisé signifie, dans le présent contexte, le stockage à un niveau central européen, tandis que le stockage décentralisé désigne le stockage au niveau des États membres.

([44]) Voir note 33.

([45]) Communication de la Commission intitulée «Préparer les prochaines évolutions de la gestion des frontières dans l'Union européenne», COM(2008) 69 du 13.2.2008.

([46]) Observations préliminaires du CEPD sur trois communications de la Commission concernant la gestion des frontières [COM(2008) 69, COM(2008) 68 et COM(2008) 67], 3 mars 2008. http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2008/08-03-03_Comments_border_package_EN.pdf

([47]) En particulier: avis du 23 mars 2005 sur la proposition de règlement du Parlement européen et du Conseil concernant le système d'information sur les visas (VIS) et l'échange de données entre les États membres sur les visas de court séjour, JO C 181 du 23.7.2005, p. 13, et avis du 19 octobre 2005 sur trois propositions concernant le système d'information Schengen de deuxième génération (SIS II), JO C 91 du 19.4.2006, p. 38.

solides et taillées sur mesure, ainsi qu'au principe de proportionnalité et à la nécessité de réaliser des analyses d'impact avant la proposition ou la mise en œuvre de toute mesure dans ce domaine. Le CEPD a toujours préconisé un juste équilibre conforme à la protection des données entre les exigences de sécurité et la protection de la vie privée des personnes concernées par ces systèmes. Il a adopté la même attitude lorsqu'il agissait en tant que superviseur des parties centrales de ces systèmes.

73. Par ailleurs, le CEPD saisit l'occasion pour souligner qu'il convient d'adopter une approche cohérente en ce qui concerne les échanges d'informations au sein de l'UE en général en veillant à la compatibilité juridique, technique et au niveau du contrôle entre les systèmes déjà en place et ceux qui sont en cours de développement. En effet, aujourd'hui plus qu'auparavant, il est clairement nécessaire d'avoir une vision courageuse et globale de la configuration que nous voulons donner aux échanges d'informations dans l'UE et à l'avenir des systèmes d'information à grande échelle. Ce n'est que sur la base d'une telle vision qu'un système électronique d'enregistrement des entrées sur le territoire des États membres et des sorties de ce territoire pourrait être envisagé.

74. Le CEPD suggère de faire référence dans le programme de Stockholm à l'intention de mettre au point une telle vision, qui devrait comprendre une réflexion sur l'entrée en vigueur éventuelle du traité de Lisbonne et ses conséquences pour les systèmes fondés sur une base juridique relevant du premier ou du troisième pilier.

75. Enfin, la communication mentionne la création d'une nouvelle agence qui deviendrait également compétente pour le système d'enregistrement électronique des entrées et des sorties. Entre-temps, la Commission a adopté une proposition relative à la création d'une telle agence ([48]). Le CEPD soutient a priori cette proposition car elle peut améliorer le fonctionnement de tels systèmes, y compris la protection des données. Il rendra un avis à son sujet en temps utile.

Europol et Eurojust

76. Le rôle d'Europol est évoqué à plusieurs reprises dans la communication, qui souligne, parmi les questions prioritaires, qu'Europol doit jouer un rôle central dans la coordination, l'échange d'informations et la formation des professionnels. De même, le point 4.2.2 de la communication fait référence aux récentes modifications du cadre juridique régissant la coopération entre Eurojust et Europol et annonce que les travaux visant au renforcement d'Eurojust se poursuivront, en particulier pour ce qui concerne les enquêtes dans le domaine de la criminalité organisée transfrontière. Le CEPD souscrit sans réserve à ces objectifs, à condition que les garanties relatives à la protection des données soient respectées de manière appropriée.

77. Dans ce contexte, le CEPD se félicite du nouveau projet d'accord récemment dégagé entre Europol et Eurojust ([49]), qui vise à améliorer et à renforcer la coopération entre ces deux organes et à permettre un échange mutuel efficace d'informations. Une protection efficace et effective des données joue un rôle crucial à cet égard.

VI.4. **Utilisation des données biométriques**

78. Le CEPD observe que la communication n'aborde pas la question de l'utilisation croissante des données biométrique dans le cadre de différents instruments juridiques de l'Union européenne relatifs à l'utilisation des échanges d'informations, y compris les instruments établissant les systèmes d'information à grande échelle. C'est regrettable, car il s'agit d'une question particulièrement importante et sensible du point de vue de la protection des données et du respect de la vie privée.

79. Bien que le CEPD reconnaisse les avantages généraux qu'offre l'utilisation des données biométriques, il n'a cessé d'attirer l'attention sur les impacts majeurs d'une telle utilisation sur les droits des personnes et de suggérer de l'assortir de garanties strictes dans chaque système particulier. L'arrêt récent de la Cour européenne des droits de l'homme dans l'affaire S. et Marper c. Royaume-Uni ([50]) fournit des indications utiles dans ce contexte, notamment concernant la justification et les limites de l'utilisation des données biométriques. En particulier, les données ADN peuvent révéler des informations sensibles sur les personnes, compte tenu aussi du fait que les possibilités techniques utilisées pour extraire les informations de l'ADN continuent de se développer. Dans le cas d'une utilisation à grande échelle de données biométriques dans les systèmes d'information, il existe également un problème dû aux inexactitudes inhérentes à la collecte et à la comparaison de données biométriques. Pour ces motifs, le législateur de l'UE devrait faire preuve de modération dans l'utilisation de ces données.

80. Une autre question récurrente ces dernières années est l'utilisation des empreintes digitales d'enfants et de personnes âgées, en raison des imperfections inhérentes aux systèmes biométriques en ce qui concerne ces groupes d'âge. Le CEPD a demandé une étude approfondie afin de déterminer de manière appropriée la précision de ces systèmes ([51]). Il a proposé un âge limite de 14 ans pour les enfants, à moins que l'étude ne démontre la nécessité de fixer une autre limite. Le CEPD recommande de faire état de cette question dans le programme de Stockholm.

([48]) Proposition de règlement du Parlement européen et du Conseil portant création d'une agence pour la gestion opérationnelle du système d'information Schengen (SIS II), du système d'information sur les visas (VIS), d'EURODAC et des autres systèmes d'information à grande échelle dans le domaine de la liberté, de la sécurité et de la justice, présentée par la Commission le 24 juin 2009 [COM(2009) 293].

([49]) Projet d'accord, approuvé par le Conseil, qui doit encore être signé par les deux parties. Voir registre du Conseil:http://register.consilium.europa.eu/pdf/en/09/st10/st10019.en09.pdf http://register.consilium.europa.eu/pdf/en/09/st10/st10019.en09.pdf http://register.consilium.europa.eu/pdf/fr/09/st10/st10107.fr09.pdf

([50]) Requêtes jointes n° 30562/04 et 30566/04, S. et Marper c. Royaume-Uni, arrêt du 4 décembre 2008, CEDH, non encore publié.

([51]) Avis du 26 mars 2008 concernant la proposition de règlement modifiant le règlement (CE) n° 2252/2004 du Conseil établissant des normes pour les éléments de sécurité et les éléments biométriques intégrés dans les passeports et les documents de voyage délivrés par les États membres, JO C 200 du 6.8.2008, p. 1.

81. Cela dit, le CEPD estime qu'il serait utile de mettre au point des critères concrets pour l'utilisation des données biométriques. Ces critères devraient garantir que les données sont utilisées uniquement lorsqu'elles sont nécessaires, adéquates et proportionnées et lorsqu'une finalité explicite, déterminée et légitime a été démontrée par le législateur. Plus précisément, les données biométriques, et en particulier les données ADN, ne devraient pas être utilisées si l'effet recherché peut être obtenu en utilisant d'autres informations moins sensibles.

VII. **ACCÈS À LA JUSTICE ET À LA JUSTICE EN LIGNE**

82. La technologie sera aussi utilisée comme instrument aux fins d'une meilleure coopération judiciaire. Selon le point 3.4.1 de la communication, la justice en ligne est censée offrir aux citoyens un accès plus aisé à la justice. Elle consiste en un portail contenant des informations et permettant la tenue de vidéoconférences dans le cadre des procédures judiciaires. Elle permet en outre les procédures judiciaires en ligne et prévoit l'interconnexion des registres nationaux, tels que les registres d'insolvabilité. Le CEPD constate que la communication ne mentionne pas de nouvelles initiatives dans le domaine de la justice en ligne mais qu'elle consolide des actions déjà mises en route. Il est associé à certaines de ces actions, dans le cadre du suivi de l'avis qu'il a rendu le 19 décembre 2008 sur la communication de la Commission intitulée «Vers une stratégie européenne en matière d'e-Justice» ([52]).

83. La justice en ligne est un projet ambitieux qui mérite un soutien sans réserve. Elle peut effectivement améliorer le secteur de la justice en Europe et la protection judiciaire du citoyen. Elle marque une avancée significative vers un espace européen de la justice. Sans perdre du vue cette appréciation positive, quelques remarques peuvent être formulées.

— Les systèmes technologiques utilisés pour la justice en ligne devraient être mis en place conformément au principe de la «prise en compte du respect de la vie privée dès la conception». Comme indiqué précédemment à propos du modèle européen d'information, il convient avant tout de choisir l'architecture adéquate.

— L'interconnexion et l'interopérabilité des systèmes devraient respecter le principe de la limitation de la finalité.

— Les responsabilités des différents acteurs devraient être définies avec précision.

— Les conséquences pour les particuliers de l'interconnexion des registres nationaux contenant des données à caractère personnel sensibles, tels que les registres d'insolvabilité, devraient faire l'objet d'une analyse préalable.

VIII. **CONCLUSIONS**

84. Le CEPD approuve le fait que la communication mette l'accent sur la protection des droits fondamentaux et, en particulier, sur la protection des données à caractère personnel, qui constitue une des questions clés en ce qui concerne l'avenir de l'espace de liberté, de sécurité et de justice. Selon lui, la communication promeut à juste titre un équilibre entre la nécessité de disposer d'instruments appropriés pour garantir la sécurité des citoyens et la protection de leurs droits fondamentaux. Elle reconnaît qu'il conviendrait d'accorder une plus grande place à la protection des données à caractère personnel.

85. Le CEPD soutient sans réserve le point 2.3 de la communication, qui préconise un régime complet de protection des données couvrant tous les domaines de compétence de l'UE, indépendamment de l'entrée en vigueur du traité de Lisbonne. Dans ce contexte, il recommande:

— d'annoncer, dans le programme de Stockholm, la nécessité d'une vision claire et à long terme concernant ce régime complet,

— d'examiner les mesures qui ont été adoptées dans ce domaine, ainsi que leur application concrète et leur efficacité, en tenant compte de leurs coûts sur le plan du respect de la vie privée et de leur efficacité aux fins de la répression,

— d'inscrire parmi les priorités du programme de Stockholm la nécessité d'adopter un nouveau cadre législatif pour remplacer, entre autres, la décision-cadre 2008/977/JAI du Conseil.

86. Le CEPD prend note avec satisfaction de l'intention de la Commission de réaffirmer les principes relatifs à la protection des données, ce qui devrait intervenir en relation avec la consultation publique annoncée par la Commission lors de la conférence «Données personnelles — plus d'utilisation, plus de protection?», qui s'est tenue les 19 et 20 mai 2009. En ce qui concerne le fond, le CEPD souligne l'importance du principe de la limitation de la finalité, qui constitue l'une des pierres angulaires de la législation en matière de protection des données, et ajoute qu'il convient d'examiner les possibilités d'améliorer l'application effective des principes relatifs à la protection des données au moyen d'instruments permettant de renforcer les responsabilités des responsables de traitements.

87. La prise en compte du respect de la vie privée dès la conception et les technologies respectueuses de la vie privée pourraient être encouragées par:

— un système de certification relative au respect de la vie privée et à la protection des données en tant qu'option pour les constructeurs et les utilisateurs des systèmes d'information,

— une obligation légale pour les constructeurs et les utilisateurs de systèmes d'information d'utiliser des systèmes conformes au principe de la prise en compte du respect de la vie privée dès la conception.

88. En ce qui concerne les aspects extérieurs de la protection des données, le CEPD recommande:

— de souligner, dans le programme de Stockholm, l'importance de conclure des accords généraux avec les États-Unis et d'autres pays tiers concernant la protection des données et l'échange de données,

([52]) Avis du CEPD du 19 décembre 2008 sur la communication de la Commission intitulée «Vers une stratégie européenne en matière d'e-Justice», JO C 128 du 6.6.2009, p. 13.

— de promouvoir activement le respect des droits fondamentaux, et en particulier de la protection des données, auprès des pays tiers et des organisations internationales,

— d'indiquer, dans le programme de Stockholm, que l'échange de données à caractère personnel avec des pays tiers requiert un niveau adéquat de protection ou d'autres mesures de protection appropriées dans ces pays.

89. Le CEPD prend note avec intérêt des progrès réalisés sur la voie d'une stratégie européenne de gestion de l'information et d'un modèle européen d'information et souligne l'attention qu'il convient de porter dans le cadre de ces projets aux éléments relatifs à la protection des données, à développer dans le programme de Stockholm. L'architecture pour l'échange d'informations devrait reposer sur la «prise en compte du respect de la vie privée dès la conception» et sur les «meilleures techniques disponibles».

90. Le simple fait qu'il soit techniquement possible de procéder à des échanges d'informations numériques entre des bases de données interopérables ou de fusionner ces bases de données ne justifie pas qu'il soit fait exception au principe de la limitation de la finalité. L'interopérabilité devrait, dans des cas concrets, reposer sur des choix politiques clairs et rigoureux. Le CEPD suggère de spécifier ce principe dans le programme de Stockholm.

91. Selon le CEPD, l'utilisation à des fins répressives de données à caractère personnel collectées à des fins commerciales ne devrait être autorisée que dans des conditions strictes, énoncées au point 65 du présent avis.

92. D'autres suggestions peuvent être formulées concernant l'utilisation d'informations personnelles:

— mettre au point des critères concrets permetttant de trancher entre systèmes centralisés et décentralisés et faire état, dans le programme de Stockholm, de l'intention d'élaborer de tels critères,

— la création d'un système électronique d'enregistrement des entrées sur le territoire des États membres et des sorties de ce territoire, ainsi que de programmes d'enregistrement des voyageurs, ne devrait pas être mentionnée dans le programme de Stockholm,

— soutenir le renforcement d'Europol et d'Eurojust, ainsi que le nouvel accord récemment dégagé entre ces deux organes,

— élaborer des critères concrets pour l'utilisation des données biométrique afin de garantir que les données sont utilisées uniquement lorsqu'elles sont nécessaires, adéquates et proportionnées et lorsqu'une finalité explicite, déterminée et légitime a été démontrée par le législateur. Les données ADN ne devraient pas être utilisées si l'effet recherché peut être obtenu en utilisant d'autres informations moins sensibles.

93. Le CEDP est favorable à la justice en ligne et a formulé quelques observations quant à la manière d'améliorer le projet (voir point 83).

Fait à Bruxelles, le 10 juillet 2009.

Peter HUSTINX

Contrôleur européen de la protection des données