

I

(Résolutions, recommandations et avis)

AVIS

CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES

Avis du contrôleur européen de la protection des données sur l'initiative de la République fédérale d'Allemagne, en vue de l'adoption d'une décision du Conseil concernant la mise en œuvre de la décision 2007/.../JAI relative à l'approfondissement de la coopération transfrontière, notamment en vue de lutter contre le terrorisme et la criminalité transfrontière

(2008/C 89/01)

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,

vu le règlement (CE) n° 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données, et notamment son article 41,

A ADOPTÉ L'AVIS SUIVANT

I. INTRODUCTION

1. Le 9 novembre 2007 a été publiée au Journal officiel l'initiative de la République fédérale d'Allemagne, en vue de l'adoption d'une décision du Conseil concernant la mise en œuvre de la décision 2007/.../JAI relative à l'approfondissement de la coopération transfrontière, notamment en vue de lutter contre le terrorisme et la criminalité transfrontière ⁽¹⁾ (ci-après dénommée «l'initiative»). Cette initiative est complétée par une annexe du 18 octobre 2007 contenant des détails complémentaires concernant la mise en œuvre de la décision 2007/.../JAI (ci-après dénommée «l'annexe») ⁽²⁾.

⁽¹⁾ JO C 267 du 9.11.2007, p. 4.

⁽²⁾ L'annexe n'a pas encore été publiée au Journal officiel, mais elle est disponible dans le registre du Conseil (document 11045/1/07 REV 1 ADD 1).

2. Le CEPD n'a pas été invité à formuler un avis sur l'initiative précitée. Il rend donc d'office le présent avis, comme il l'a fait pour l'initiative en vue de l'adoption d'une décision du Conseil, le 4 avril 2007 ⁽³⁾.

3. Bien que l'État membre qui prend l'initiative d'une mesure législative en vertu du titre VI du traité UE ne soit pas légalement tenu de demander l'avis du CEPD, la procédure n'exclut cependant pas cette possibilité. Par ailleurs, dans son avis du 4 avril 2007, le CEPD recommandait que soit ajoutée la phrase suivante à l'article 34 de cette décision du Conseil: «Il consulte le CEPD avant d'arrêter de telles mesures». Malheureusement, cette recommandation n'a pas été suivie, malgré la logique sous-jacente: les mesures de mise en œuvre ont la plupart du temps des incidences sur le traitement des données à caractère personnel. L'initiative de la République fédérale d'Allemagne est une claire illustration de cette logique.

4. Le CEPD ne tire aucune conclusion définitive de cette position, qui correspond à l'approche adoptée par le Conseil, à savoir de modifier le moins possible l'initiative, de façon à ce qu'elle soit pleinement compatible avec le texte du traité de Prüm signé antérieurement par un certain nombre d'États membres. Le CEPD reviendra plus loin dans le présent avis sur l'incidence de cette approche du point de vue de la démocratie.

II. CONTEXTE ET CADRE JURIDIQUE

5. Le traité de Prüm a été signé en mai 2005 par sept États membres, en dehors du cadre du traité UE. D'autres États membres ont par la suite adhéré à ce traité.

⁽³⁾ JO C 169 du 21.7.2007, p. 2.

6. Le traité de Prüm est complété par un accord d'exécution, dont la base est l'article 44 dudit traité et qui a été conclu le 5 décembre 2006. Cet accord d'exécution est nécessaire au fonctionnement du traité de Prüm.
7. Les principaux éléments du traité de Prüm seront intégrés dans le cadre juridique de l'Union européenne, après l'adoption de la décision 2007/... du Conseil concernant l'initiative de 15 États membres (ci-après dénommée «l'initiative Prüm»), qui a déjà fait l'objet d'un accord politique au sein du Conseil. Cette intégration était dès le départ dans l'intention des parties contractantes au traité UE, comme le confirme le préambule du traité de Prüm.
8. L'intention, pendant la procédure législative devant conduire à l'adoption de la décision du Conseil, n'était pas de poursuivre le débat sur les questions principales, mais de parvenir à un accord sur l'acquis du traité de Prüm. Cette intention était d'autant plus importante que, en attendant cette procédure législative, le processus de ratification du traité s'est poursuivi dans un certain nombre d'États membres et le traité est entré en vigueur.

III. OBJET ET ÉLÉMENTS FONDAMENTAUX DU PRÉSENT AVIS

9. Le présent avis mettra l'accent sur le projet de décision du Conseil concernant les règles de mise en œuvre. Les points soulevés dans le précédent avis du CEPD sur la décision du Conseil concernant l'initiative de Prüm restent valables et ne seront pas repris, sauf s'il est nécessaire de mettre en lumière les points que le législateur pourrait encore traiter via les règles de mise en œuvre.
10. Dans ce contexte, il importe de souligner que les règles de mise en œuvre revêtent une importance particulière parce que, en dehors de quelques dispositions administratives et techniques, elles définissent des aspects et des outils essentiels du système et de son fonctionnement. Ainsi, le chapitre 1 des règles de mise en œuvre énonce les définitions des termes employés dans la décision du Conseil concernant le traité de Prüm. Par ailleurs, les règles de mise en œuvre établissent des dispositions communes en matière d'échange de données (chapitre 2), et définissent les caractéristiques spécifiques de l'échange de données d'ADN (chapitre 3), de données dactyloscopiques (chapitre 4) et de données relatives à l'immatriculation des véhicules (chapitre 5). Les dispositions finales du chapitre 6 contiennent des dispositions importantes concernant l'adoption de règles de mise en œuvre supplémentaires dans le manuel ainsi que l'évaluation de l'application de la décision.
11. En outre, l'annexe sera examinée dans la mesure où elle contribue, ou devrait contribuer, à définir les caractéristiques du système proposé et les garanties à fournir aux personnes concernées.

IV. GÉNÉRALITÉS

Marge de manœuvre limitée

12. Le CEPD note que, en l'occurrence également, la préexistence de règles de mise en œuvre déjà en vigueur pour la

convention de Prüm semble réduire sensiblement la marge de manœuvre effective dont dispose le Conseil. De fait, selon le considérant 3 et l'article 18 de l'initiative, la décision de mise en œuvre ainsi que le manuel se fondent sur l'accord d'exécution adopté le 5 décembre 2006 concernant la mise en œuvre administrative et technique du traité de Prüm. En conséquence, selon la présente initiative, les 27 États membres devront suivre la voie définie par les sept États membres qui ont signé le traité de Prüm.

13. Cette approche est un obstacle à la mise en place d'un processus législatif véritablement transparent et démocratique, car elle réduit considérablement la possibilité de mener un large débat et de prendre effectivement en compte le rôle législatif du Parlement européen et le rôle consultatif des autres institutions, dont le CEPD. Le CEPD recommande que l'initiative et son annexe fassent l'objet d'un débat ouvert auquel contribueraient tous les acteurs institutionnels, compte tenu également du rôle de colégislateur à part entière que jouera le Parlement européen dans ce domaine lorsque le traité modificatif, signé à Lisbonne le 13 décembre, entrera en vigueur.

Cadre juridique de la protection des données et relation avec le projet de décision-cadre sur la protection des données dans le cadre du troisième pilier

14. Le cadre juridique applicable à la protection des données est complexe et fluctuant. De fait, le chapitre 6 de l'initiative Prüm énonce quelques garanties et règles spécifiques en matière de protection des données. Cependant, ces règles spécifiques ne sont pas autonomes et elles doivent se fonder, pour fonctionner convenablement, sur un cadre complet et général régissant la protection des données à caractère personnel traitées par les autorités policières et judiciaires. À l'heure actuelle, l'article 25 de l'initiative Prüm renvoie à la convention n° 108 du Conseil de l'Europe. Toutefois, le CEPD a souligné à plusieurs reprises la nécessité de préciser davantage les principes énoncés dans la convention n° 108, et de veiller ainsi à un niveau de protection des données élevé, harmonisé et par conséquent approprié pour garantir à la fois les droits des citoyens et l'efficacité de la coopération en matière répressive au sein d'un espace de liberté, de sécurité et de justice ⁽¹⁾.
15. Dans cette perspective, la Commission a proposé dès octobre 2005 un instrument général, le projet de décision-cadre du Conseil sur la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale («projet de décision-cadre sur la protection des données dans le cadre du troisième pilier»). Cette proposition n'a pas encore été adoptée par le Conseil; son examen se poursuit et elle peut donc faire l'objet d'éventuelles modifications, sans parler du retard supplémentaire que pourraient accuser son adoption et sa mise en œuvre. Toutefois, il est clair dès à présent que cette décision-cadre, en l'état, ne serait applicable qu'aux données à caractère personnel échangées avec d'autres États membres et non au traitement des données à l'intérieur d'un pays ⁽²⁾.

⁽¹⁾ Voir, plus récemment, l'avis du CEPD sur Prüm, § 57-76 et le troisième avis du CEPD du 27 avril 2007 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, § 14 (JO C 139 du 23.6.2007, p. 1).

⁽²⁾ La dernière version en date de cette proposition est disponible dans le registre du Conseil (document 16397/07).

16. Par ailleurs, le texte actuel du projet de décision-cadre sur la protection des données dans le cadre du troisième pilier, malgré son objectif d'assurer un niveau élevé de protection des données, n'apporte qu'une harmonisation et des garanties minimales. Cela signifie que certains instruments, tels que l'initiative actuelle, pour lesquels il aurait été utile de disposer d'un cadre général régissant la protection des données, vont désormais servir à combler les lacunes laissées par le projet de décision-cadre sur la protection des données dans le cadre du troisième pilier.
17. Le CEPD réaffirme donc d'une part que les décisions du Conseil concernant le traité de Prüm ne devraient pas entrer en vigueur avant que les États membres aient mis en œuvre une décision-cadre générale sur la protection des données dans le cadre du troisième pilier. Cette condition devrait figurer explicitement dans l'initiative, et dépendre de la vérification préalable du bon fonctionnement des garanties de protection des données au sein du système d'échange de données. Dans ce contexte, il est également essentiel de garantir que les relations entre instruments juridiques sont clarifiées de façon à ce que la décision-cadre sur la protection des données dans le cadre du troisième pilier s'applique en tant que «lex generalis» tout en permettant l'applicabilité d'autres garanties spécifiques et de normes plus strictes spécialement définies dans l'initiative de Prüm ⁽¹⁾.
18. D'autre part, le législateur devrait préciser que les règles spécifiques en matière de protection des données concernant l'ADN, les empreintes digitales et l'immatriculation des véhicules prévues au chapitre 6 de l'initiative de Prüm, sont applicables non seulement à l'échange de ces données, mais aussi à leur collecte, à leur conservation et à leur traitement au niveau national, ainsi qu'à la fourniture d'autres données à caractère personnel relevant du champ d'application de la décision du Conseil. Cette clarification serait conforme à l'article 24, paragraphe 2, de l'initiative de Prüm, et la conséquence logique de l'obligation incombant aux États membres de collecter, conserver et échanger les types de données susmentionnées.
19. Ce point est encore plus important si l'on considère que le champ d'application du projet de décision-cadre sur la protection des données dans le cadre du troisième pilier ne couvrira probablement pas le traitement domestique des données à caractère personnel. Le Conseil a pris cette décision tout en précisant que ce choix ne limite pas la capacité de la base juridique de couvrir ce type d'opérations de traitement. Dans ce contexte, comme l'ensemble actuel d'initiatives — qui comprend l'initiative de Prüm et les règles de mise en œuvre — impose l'obligation de créer et de tenir à jour certaines bases de données, comme la base de données d'ADN, il devrait également contenir des garanties concernant les opérations de traitement — notamment, la collecte et la conservation des profils d'ADN — découlant de la collecte et de la conservation des données. Dans le cas contraire, si leur application devait être limitée aux données échangées, ces instruments juridiques ne comprendraient pas les dispositions appropriées en matière de protection des données à caractère personnel qui devraient s'appliquer

à toute action fondée sur l'article 30, paragraphe 1, point b), du traité UE.

20. Le CEPD invite le législateur à veiller à ce que, conformément à l'article 30, paragraphe 1, point b), du traité UE, un cadre juridique clair, efficace et complet en matière de protection des données, combinant différents instruments juridiques et des dispositions générales et des garanties spécifiques, soit en place avant l'entrée en vigueur de l'initiative en question.
21. Dans le présent avis, le CEPD renverra donc, le cas échéant, aux points qui n'ont pas encore été (complètement) traités dans le projet de décision-cadre sur la protection des données dans le cadre du troisième pilier et qui doivent donc être pris en considération dans la mise en œuvre du système prévue par l'initiative.

Transparence du processus décisionnel et des règles de mise en œuvre

22. Le CEPD souligne que la transparence est un élément essentiel tant dans le processus décisionnel que dans la mise en œuvre des règles. La transparence devrait donc permettre d'une part la participation pleine et effective de tous les acteurs institutionnels concernés et elle devrait d'autre part favoriser le débat public et une bonne information des citoyens.
23. Malheureusement, dans le cas présent, une série d'obstacles affecte la transparence: il n'y a pas d'exposé des motifs qui présente les raisons sous-tendant les mesures proposées, leur efficacité et les autres voies possibles; le texte de l'annexe est encore incomplet, il n'est pas encore publié au Journal officiel, il n'est pas traduit dans toutes les langues officielles, les références aux articles et la terminologie sont souvent inexacts et les déclarations des États membres sur le contenu des bases de données d'ADN ne sont pas disponibles; l'initiative elle-même ne définit pas les obligations ou les mécanismes nécessaires pour informer les citoyens sur les mesures prises et les modifications de ces mesures.
24. Le CEPD recommande donc d'améliorer la transparence des mesures, avec la mise à disposition, le plus rapidement possible, de la version définitive de l'annexe et la mise en place de mécanismes d'information des citoyens sur les caractéristiques des systèmes, sur leurs droits et sur les moyens de les exercer. Ces campagnes d'information devraient être mentionnées explicitement dans l'initiative ou dans son annexe.

Taille du système

25. L'initiative en question reprend fidèlement les règles de mise en œuvre établies par le traité de Prüm. Toutefois, comme cela a déjà été indiqué dans l'avis sur l'initiative de Prüm du Conseil (§ 33-35), les mécanismes conçus pour l'échange d'informations entre quelques États membres ne conviennent pas nécessairement, et peuvent donc nécessiter des adaptations quand il s'agit de les appliquer à un système à beaucoup plus grande échelle, tel que l'échange d'informations entre 27 États membres.

⁽¹⁾ En ce qui concerne ce point, le texte de l'article 27 ter du dernier projet de décision-cadre sur la protection des données dans le cadre du troisième pilier doit faire l'objet d'un examen et d'une discussion approfondis.

26. De fait, l'action à petite échelle favorise les contacts étroits entre les États membres concernés, tant en matière répressive qu'en ce qui concerne le contrôle des risques relatifs à la protection des données à caractère personnel. Ce n'est pas le cas dans un système plus large, dans lequel les pratiques nationales et les régimes juridiques diffèrent considérablement en matière de collecte, de conservation et de traitement des données, notamment en ce qui concerne les profils d'ADN et les empreintes digitales. En outre, l'utilisation de langues différentes et de concepts juridiques différents peut nuire à l'exactitude des échanges de données entre pays de traditions juridiques différentes. C'est pourquoi le CEPD invite le législateur à prendre dûment en considération la taille du système dans la suite des discussions sur l'initiative en question, en veillant à ce que l'augmentation du nombre d'États membres participants n'implique pas une diminution de l'efficacité de ce système. En particulier, il conviendrait de définir, dans les règles de mise en œuvre, des formats spécifiques de communication des données, tenant compte également des différences de langues, et l'exactitude des échanges de données devrait faire l'objet d'une surveillance permanente.

Participation des autorités de protection des données

27. L'initiative devrait reconnaître le rôle important que doivent jouer les autorités indépendantes de contrôle dans le cadre des échanges transfrontières de données à grande échelle, et elle devrait leur permettre de s'acquitter effectivement de leur mission.
28. Tout d'abord, le cadre juridique actuel ne prévoit pas que l'on consulte ni que l'on associe les autorités de contrôle compétentes aux travaux en ce qui concerne les modifications à apporter aux règles de mise en œuvre et à leur annexe (article 18 de l'initiative), à la mise en œuvre des règles de protection des données par les États membres (article 20), ou à l'évaluation de l'échange de données (article 21). Il est, par exemple, particulièrement regrettable que le chapitre IV de l'annexe, qui fixe les règles à suivre pour évaluer la mise en œuvre, ne mentionne absolument pas les autorités compétentes en matière de protection des données. Le CEPD recommande que le rôle consultatif essentiel que jouent ces autorités soit explicitement reconnu par les articles susmentionnés.
29. Ensuite, l'initiative devrait garantir que les États membres fournissent aux autorités chargées de la protection des données les ressources (complémentaires) nécessaires pour mener à bien leur rôle de supervision découlant de la mise en œuvre du système proposé.
30. Enfin, l'initiative devrait prévoir que les autorités compétentes en matière de protection des données se réunissent régulièrement au niveau de l'UE en vue de coordonner leurs activités et d'harmoniser l'application de ces instruments.
- Cette possibilité devrait figurer explicitement dans l'initiative, dans la mesure où la décision-cadre sur la protection des données dans le cadre du troisième pilier n'établit pas de forum plus général pour les autorités compétentes en matière de protection des données au niveau de l'UE.

V. POINTS PARTICULIERS

Définitions

31. L'article 2 de l'initiative énonce une série de définitions, qui reprennent en partie celles figurant dans la décision du Conseil. Il convient de souligner en premier lieu que les définitions visées à l'article 2 de l'initiative ne correspondent pas exactement aux définitions visées dans la décision du Conseil, notamment à son article 24. Le législateur devrait aligner les formulations des deux textes afin d'éviter tout problème de mise en œuvre.
32. Ensuite, le CEPD, dans son avis sur l'initiative de Prüm, regrettait déjà l'absence de définition précise des données à caractère personnel (§ 41-43). Cette absence est d'autant plus regrettable dans les règles de mise en œuvre proposées qu'il est clair que le projet de décision-cadre sur la protection des données dans le cadre du troisième pilier ne sera pas applicable à la collecte ni au traitement des données à caractère personnel effectués au niveau national, et notamment des profils d'ADN. Le CEPD invite donc une nouvelle fois le législateur à introduire une définition claire et complète des données à caractère personnel.
33. Dans cette optique, les dispositions de mise en œuvre devraient également clarifier l'applicabilité des règles de protection des données aux profils d'ADN non identifiés — qui n'ont pas encore été attribués à une personne identifiée. De fait, ces données sont collectées, échangées, et comparées en vue d'être attribuées aux personnes à qui elles appartiennent. C'est pourquoi, comme l'objectif du système est d'identifier ces personnes et que ces données sont en principe censées n'être que temporairement «non identifiées», elles devraient également être couvertes par la plupart, voire la totalité, des dispositions et garanties applicables aux données à caractère personnel ⁽¹⁾.
34. De même, en ce qui concerne la définition de la «partie non codante de l'ADN» [article 2, point e)], le CEPD rappelle une nouvelle fois ⁽²⁾ que la capacité de certaines régions chromosomiques à fournir les caractéristiques héréditaires sensibles d'un organisme peut augmenter avec l'évolution de la science. C'est pourquoi, la définition de la «partie non codante» devrait pouvoir évoluer, et comporter l'obligation de ne plus utiliser les marqueurs d'ADN qui, du fait des progrès de la science, peuvent fournir des informations sur des caractéristiques héréditaires spécifiques ⁽³⁾.

⁽¹⁾ Sur l'applicabilité des règles de protection des données aux profils d'ADN, voir l'avis n° 4/2007 du groupe de l'article 29 sur le concept de données à caractère personnel, adopté le 20 juin 2007 (référence WP136) p. 8-9; le même avis donne des clarifications sur le cas analogue de l'applicabilité des règles de protection des données aux adresses IP dynamiques, p. 16-17.

⁽²⁾ Voir également l'avis du CEPD du 28 février 2006 sur la proposition de décision-cadre du Conseil relative à l'échange d'informations en vertu du principe de disponibilité (COM (2005) 490 final), § 58-60 (JO C 116 du 17.5.2006).

⁽³⁾ Voir, dans le même sens, l'annexe I de la résolution du Conseil du 25 juin 2001 relative à l'échange des résultats des analyses d'ADN (JO C 187 du 3.7.2001, p. 1).

Exactitude des consultations et des comparaisons automatisées

35. L'article 8 de l'initiative régit les consultations et les comparaisons automatisées des profils d'ADN, en stipulant que la notification automatisée d'une concordance «est effectuée uniquement si la consultation ou la comparaison automatisée a mis en évidence une concordance basée sur un nombre minimum de loci». Ce minimum est fixé au chapitre I de l'annexe: chaque État membre veille à ce que les profils d'ADN disponibles contiennent au moins six des sept loci «standard» de l'UE (chapitre I, § 1.1, de l'annexe); la comparaison sera effectuée entre les valeurs des loci comparés figurant dans les profils d'ADN transmis et consultés (§ 1.2); il y a concordance si toutes les valeurs des loci comparés sont les mêmes («concordance exacte») ou si seulement une valeur est différente («concordance partielle») (§ 1.2); les deux types de concordance (exacte et partielle) sont communiqués (§ 1.3).
36. À propos de ce mécanisme, le CEPD note que l'exactitude de la concordance est une condition essentielle. Plus le nombre de loci concordants est élevé, plus le risque de fausse concordance entre profils d'ADN comparés est faible. Dans le contexte actuel de l'Union européenne, l'existence et la structure des bases de données d'ADN varient d'un pays à l'autre, de même que le nombre et les séries de loci utilisés. L'annexe fixe à six le nombre minimum de loci pour que la concordance soit positive, sans donner d'information sur le taux d'erreur envisagé dans ce système. Sur ce point, le CEPD note que de nombreux pays utilisent un nombre supérieur de loci en vue d'accroître la précision des concordances et de réduire la probabilité de fausses concordances⁽¹⁾. Il serait donc essentiel, afin d'évaluer correctement le degré d'exactitude du système envisagé, de fournir des informations sur le taux d'erreur envisagé pour chaque nombre de loci comparés.
37. Cela signifie également que le nombre minimum de loci est un élément essentiel et qu'il doit à ce titre être fixé dans le texte de l'initiative plutôt que dans son annexe (qui, selon l'article 18 de l'initiative, peut être modifiée par le Conseil statuant à la majorité qualifiée et sans consulter le Parlement), afin d'éviter qu'une diminution du nombre de loci n'affecte l'exactitude des résultats. Le risque d'erreurs et de fausses concordances devrait être dûment pris en considération: il conviendrait à cette fin que toute concordance partielle soit signalée comme telle (ce qui permettrait aux autorités destinataires de savoir que cette concordance n'est pas aussi fiable qu'une concordance exacte).
38. Par ailleurs, il est reconnu dans l'initiative elle-même que les consultations et les comparaisons peuvent générer des concordances multiples, comme l'indique explicitement l'article 8 de l'initiative en ce qui concerne les profils d'ADN et le chapitre 3 (point 1.2) de l'annexe en ce qui concerne les véhicules. Dans tous ces cas, il conviendrait d'effectuer de nouveaux contrôles et vérifications afin de déterminer quelles sont les raisons d'une concordance multiple et quelle est la concordance exacte, avant de procéder à un nouvel échange de données à caractère personnel sur la base de la concordance en question.
39. Dans la même optique, le CEPD recommande de mieux informer, notamment les services de police chargés des comparaisons et des consultations d'ADN, sur le fait que les profils d'ADN ne sont pas des identifiants uniques: dans un certain nombre de loci, même les concordances exactes n'excluent pas la possibilité de fausses concordances, autrement dit, la possibilité qu'une personne soit reliée par erreur à un profil d'ADN. De fait, des erreurs peuvent survenir dans les comparaisons et les consultations de profils d'ADN à différents stades: piètre qualité des échantillons d'ADN au moment du prélèvement, risque d'erreurs techniques dans l'analyse de l'ADN, erreurs de saisie, ou simple concordance fortuite dans les loci examinés aux fins de la comparaison. S'agissant de ce dernier point, le taux d'erreur risque d'augmenter lorsque le nombre de loci diminue et que la base de données augmente.
40. On peut appliquer le même raisonnement en ce qui concerne l'exactitude de la concordance des empreintes digitales. L'article 12 de l'initiative dispose que la numérisation des données dactyloscopiques et leur transmission aux autres États membres s'effectuent selon un format de données uniforme, décrit au chapitre II de l'annexe. En outre, les États membres doivent s'assurer que les données dactyloscopiques qu'ils transmettent sont d'une qualité suffisante en vue d'une comparaison par les systèmes automatisés d'identification des empreintes digitales (AFIS: Automated Fingerprint Identification System). Le chapitre 2 de l'annexe donne des détails sur le format à utiliser. Dans ce contexte, le CEPD note que, en vue de garantir l'exactitude du processus de concordance, l'initiative et son annexe devraient harmoniser le plus possible les différents systèmes AFIS utilisés dans les États membres et la manière dont ces systèmes sont utilisés, en particulier en ce qui concerne le taux de faux rejets. Selon le CEPD, cette information devrait figurer dans le manuel élaboré conformément à l'article 18, paragraphe 2, de l'initiative.
41. Il convient de souligner un autre élément essentiel, à savoir que les bases de données d'ADN (et d'empreintes digitales) devraient être délimitées avec précision, car elles peuvent contenir, selon les États membres, les profils d'ADN ou les empreintes digitales de différents types de personnes concernées (criminels, suspects, autres personnes présentes sur la scène de crime, etc.). Malgré toutes ces différences, l'initiative ne délimite pas les différents types de bases de données qui seront utilisés par chacun des États membres, et l'annexe ne comporte pas encore de déclarations à cet effet. On risque donc d'observer des concordances entre des données d'ADN et des empreintes digitales se rapportant à des catégories de personnes non homogènes et souvent sans pertinence.
42. Selon le CEPD, l'initiative devrait préciser quels types de personnes concernées feront l'objet d'échanges de données et comment leurs statuts différents seront communiqués aux autres États membres dans le cadre d'une comparaison ou d'une consultation. Ainsi, l'initiative pourrait établir l'obligation de fournir dans le rapport de concordance des informations sur le type de personnes concernées dont les données d'ADN ou les empreintes digitales ont donné lieu à une concordance positive, dans la mesure où ces informations sont accessibles aux autorités requises.

(¹) Par exemple, au RU, la base nationale de données d'ADN a fait passer de six à dix le nombre de loci utilisés pour les profils d'ADN, en vue d'améliorer la fiabilité du système.

Évaluation de l'échange d'informations

43. L'évaluation de l'échange d'informations, prévue à l'article 21 de l'initiative et au chapitre 4 de l'annexe, est un élément positif. Cependant, ces dispositions se concentrent sur la mise en œuvre administrative, technique et financière des échanges automatisés de données, sans même mentionner l'évaluation de la mise en œuvre des règles de protection des données.
44. Le CEPD suggère donc que l'accent soit mis sur l'évaluation des aspects relatifs à la protection des données dans le cadre des échanges d'informations, en accordant une attention particulière à la finalité de ces échanges, aux méthodes d'information des personnes concernées, à l'exactitude des données échangées et aux fausses concordances, aux demandes d'accès aux données à caractère personnel, à la durée de conservation des données et à l'efficacité des mesures de sécurité. Dans ce contexte, la participation des autorités et des experts compétents en matière de protection des données devrait être dûment prévue, par exemple en stipulant que les experts en matière de protection des données participent aux visites d'évaluation prévues au chapitre 4 de l'annexe et que les autorités de protection des données concernées reçoivent le rapport d'évaluation décrit à l'article 20 de l'initiative et au chapitre 4 de l'annexe.

Réseau de communication et aspects techniques du système

45. L'article 4 de l'initiative dispose que tous les échanges électroniques de données s'effectuent via le réseau de communication «TESTA II». Dans ce contexte, il est indiqué, page 76, point 54, de l'annexe, que «le système est en conformité avec les questions relatives à la protection des données visées dans le règlement (CE) n° 45/2001 (articles 21, 22 et 23) et la directive 95/46/CE». Le CEPD recommande que cette information soit clarifiée, également en ce qui concerne le rôle que les institutions communautaires joueront dans le système. Dans ce contexte, il conviendrait de tenir pleinement compte des rôles de supervision et de conseil impartis au CEPD en vertu du règlement (CE) n° 45/2001.
46. Par ailleurs, lorsque la version finale de l'annexe sera achevée et qu'elle contiendra tous les détails et les déclarations précisant les caractéristiques des systèmes, le CEPD examinera s'il y a lieu de rendre un avis sur les aspects plus techniques du système.

VI. CONCLUSIONS

- Le CEPD recommande que l'initiative et son annexe fassent l'objet d'un débat ouvert auquel contribueraient tous les acteurs institutionnels, compte tenu également du rôle de colégislateur à part entière que jouera le Parlement européen dans ce domaine lorsque le traité modificatif, signé à Lisbonne le 13 décembre, entrera en vigueur.
- Le CEPD invite le législateur à veiller à ce que, conformément à l'article 30, paragraphe 1, point b), du traité UE, un cadre juridique clair, efficace et complet en matière de protection des données, combinant différents instruments juridiques et des dispositions générales et des garanties spécifiques, soit en place avant l'entrée en vigueur de l'initiative en question.

- Dans cette optique, le CEPD réaffirme d'une part, que les décisions du Conseil concernant le traité de Prüm ne devraient pas entrer en vigueur avant que les États membres aient mis en œuvre une décision-cadre générale sur la protection des données dans le cadre du troisième pilier, qui serait une «lex generalis» complétée par les dispositions de l'initiative de Prüm permettant l'application de garanties spécifiques et de normes plus strictes spécialement définies.
- D'autre part, le législateur devrait préciser que les règles spécifiques en matière de protection des données concernant l'ADN, les empreintes digitales et l'immatriculation des véhicules prévues au chapitre 6 de l'initiative de Prüm, sont applicables non seulement à l'échange de ces données, mais aussi à leur collecte, à leur conservation et à leur traitement au niveau national, ainsi qu'à la fourniture d'autres données à caractère personnel relevant du champ d'application de la décision du Conseil.
- Le CEPD recommande d'améliorer la transparence des mesures, avec la mise à disposition, le plus rapidement possible, de la version définitive de l'annexe et la mise en place de mécanismes d'information des citoyens sur les caractéristiques des systèmes, sur leurs droits et sur les moyens de les exercer.
- Le CEPD invite le législateur à prendre dûment en considération la taille du système dans la suite des discussions sur l'initiative en question, en veillant à ce que l'augmentation du nombre d'États membres participants n'implique pas une diminution de l'efficacité de ce système. En particulier, il conviendrait de définir, dans les règles de mise en œuvre, des formats spécifiques de communication des données, tenant compte également des différences de langues, et l'exactitude des échanges de données devrait faire l'objet d'une surveillance permanente.
- Le CEPD recommande que le rôle consultatif essentiel des autorités compétentes en matière de protection des données soit explicitement reconnu dans les articles relatifs aux modifications à apporter aux modalités de mise en œuvre et à leur annexe (article 18), à la mise en œuvre des règles de protection des données par les États membres (article 20), ou à l'évaluation de l'échange d'informations (article 21). Par ailleurs, l'initiative devrait garantir que les États membres fournissent aux autorités chargées de la protection des données les ressources (complémentaires) nécessaires pour mener à bien leur rôle de supervision découlant de la mise en œuvre du système proposé et que les autorités compétentes en matière de protection des données se réunissent régulièrement au niveau de l'UE en vue de coordonner leurs activités et d'harmoniser l'application de ces instruments.
- Le CEPD invite donc une nouvelle fois le législateur à introduire une définition claire et complète des données à caractère personnel. Dans cette optique, les dispositions de mise en œuvre devraient également clarifier l'applicabilité des règles de protection des données aux profils d'ADN non identifiés, qui n'ont pas encore été attribués à une personne identifiée. Le CEPD rappelle aussi que la définition de la «partie non codante» devrait pouvoir évoluer, et comporter l'obligation de ne plus utiliser les marqueurs d'ADN qui, du fait des progrès de la science, peuvent fournir des informations sur des caractéristiques héréditaires spécifiques.

- Le CEPD recommande que, dans le contexte des consultations et des comparaisons automatisées, l'exactitude du processus d'établissement de la concordance soit dûment prise en compte.
 - Cela signifie que, en ce qui concerne les comparaisons et les consultations de données d'ADN, il conviendrait que des informations soient fournies sur le taux d'erreur envisagé pour chaque nombre de loci comparés, que les concordances partielles soient signalées comme telles, que de nouveaux contrôles soient effectués en cas de concordances multiples, et que l'on fasse mieux comprendre que les profils d'ADN ne sont pas des identifiants uniques. En ce qui concerne les empreintes digitales, l'initiative devrait harmoniser le plus possible les différents systèmes AFIS utilisés dans les États membres et la manière dont ces systèmes sont utilisés, en particulier en ce qui concerne le taux de faux rejets.
 - En outre, les bases de données d'ADN et d'empreintes digitales devraient être délimitées avec précision, car elles peuvent contenir, selon les États membres, les profils d'ADN ou les empreintes digitales de différents types de personnes. L'initiative devrait préciser quels types de personnes feront l'objet d'échanges de données et comment leurs statuts différents seront communiqués aux autres États membres dans le cadre d'une comparaison.
- Le CEPD suggère que l'accent soit mis sur l'évaluation des aspects relatifs à la protection des données dans le cadre des échanges d'informations, en accordant une attention particulière à la finalité de ces échanges, aux méthodes d'information des personnes concernées, à l'exactitude des données échangées et aux fausses concordances, aux demandes d'accès aux données à caractère personnel, à la durée de conservation des données et à l'efficacité des mesures de sécurité. Dans ce contexte, la participation des autorités et des experts compétents en matière de protection des données devrait être dûment prévue.
- Le CEPD recommande que l'utilisation du réseau de communication «TESTA II» et sa conformité avec le règlement (CE) n° 45/2001 soit clarifiée, également en ce qui concerne le rôle que les institutions communautaires joueront dans ce système.

Fait à Bruxelles, le 19 décembre 2007.

Peter HUSTINX

Contrôleur européen de la protection des données
