

I

(Résolutions, recommandations et avis)

AVIS

CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES

Avis du contrôleur européen de la protection des données sur la proposition de décision du Conseil relative à la création du système européen d'information sur les casiers judiciaires (ECRIS), en application de l'article 11 de la décision-cadre 2008/.../JAI

(2009/C 42/01)

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,

vu la demande d'avis formulée conformément à l'article 28, paragraphe 2, du règlement (CE) n° 45/2001, adressée au CEPD le 27 mai 2008,

A ADOPTÉ L'AVIS SUIVANT:

I. OBSERVATIONS PRÉLIMINAIRES

1. Le 27 mai 2008, la Commission a adopté une proposition de décision du Conseil relative à la création du système européen d'information sur les casiers judiciaires (ECRIS), en application de l'article 11 de la décision-cadre 2008/.../JAI (ci-après dénommée «la proposition») ⁽¹⁾. La Commission a transmis la proposition au CEPD pour avis, conformément à l'article 28, paragraphe 2, du règlement (CE) n° 45/2001.

⁽¹⁾ Doc. COM(2008) 332 final.

2. La proposition vise à mettre en œuvre l'article 11 de la décision-cadre du Conseil relative à l'organisation et au contenu des échanges d'informations extraites du casier judiciaire entre les États membres ⁽²⁾ (ci-après dénommée «la décision-cadre du Conseil»), en vue de construire et de développer un système informatisé d'échange d'informations entre les États membres ⁽³⁾. Comme l'indique son article 1^{er}, elle porte création du système européen d'information sur les casiers judiciaires (ECRIS) et définit également les éléments d'un format standardisé pour l'échange électronique d'informations, ainsi que d'autres aspects techniques et généraux de la mise en œuvre visant à organiser et à faciliter les échanges d'informations.

3. Le CEPD se félicite de faire l'objet d'une consultation et recommande qu'il soit fait référence à cette consultation dans les considérants de la proposition, comme cela a été fait dans un certain nombre d'autres textes législatifs sur lesquels le CEPD a été consulté, conformément au règlement (CE) n° 45/2001.

II. HISTORIQUE ET CONTEXTE

4. Le CEPD rappelle qu'il a rendu un avis sur la décision-cadre du Conseil le 29 mai 2006. Parmi les éléments de cet avis qui méritent d'être rappelés, on peut citer:

— l'accent mis sur l'importance que revêt le format standardisé comme moyen d'éviter toute ambiguïté quant au contenu des informations extraites du casier judiciaire,

⁽²⁾ En attente d'adoption. La dernière version en date de la proposition, telle qu'elle a été reformulée par le Conseil, est disponible sur le registre public du Conseil (doc. 5968/08).⁽³⁾ Considérant 6 de la proposition.

- l'adhésion aux options retenues dans la décision-cadre du Conseil, qui consistent à ne pas prévoir la création d'une base de données européenne centralisée, ni permettre l'accès direct à des bases de données qu'il serait difficile de contrôler,
 - l'application de la 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 aux informations extraites des casiers judiciaires, notamment en rapport avec les transferts des données à caractère personnel aux pays tiers,
 - l'efficacité de l'échange d'informations dans un contexte de différences notables entre les législations nationales relatives aux casiers judiciaires, qui exige des mesures complémentaires,
 - la répartition des responsabilités entre les États membres et les difficultés soulevées par cette répartition en termes d'adéquation du contrôle. La désignation d'une autorité centrale au niveau national a été considérée comme un élément positif,
 - le large champ d'application de la décision-cadre du Conseil, celle-ci s'appliquant à toutes les condamnations inscrites au casier judiciaire.
5. Ces éléments de l'avis de 2006 demeurent valables pour le contexte dans lequel la proposition à l'examen sera analysée. En particulier, les divergences entre les législations nationales concernant les casiers judiciaires sont un élément déterminant de ce contexte. Du fait de ces divergences, des mesures complémentaires doivent être prises pour que le système d'échanges fonctionne. À ce titre, la proposition ECRIS constitue une mesure complémentaire. Cependant, ce contexte connaît également une évolution.
6. En premier lieu, la décision-cadre du Conseil et sa mise en œuvre dans le cadre de la proposition ECRIS s'inscrivent dans une série de nouveaux instruments juridiques destinés à faciliter l'échange d'informations entre les États membres de l'Union européenne à des fins répressives. Ils donnent tous corps au principe de disponibilité, tel qu'il a été introduit par le Programme de La Haye de 2004 ⁽¹⁾. Alors que la plupart de ces instruments portent essentiellement sur la coopération policière, l'instrument à l'examen est un moyen de coopération judiciaire en matière pénale au sens de l'article 31 du traité UE ⁽²⁾. Néanmoins, il vise le même objectif: faciliter l'échange d'informations à des fins répressives. Très souvent, ces instruments intègrent ou s'appuient sur des systèmes d'information et/ou sur la standardisation des pratiques d'échange. À cet égard, la proposition ECRIS n'est pas unique. Pour évaluer cette proposition, le CEPD peut mettre à profit l'expérience acquise, par le passé, dans le cadre d'instruments comparables.
7. En deuxième lieu, le cadre juridique de l'UE en matière de protection des données s'enrichit. L'adoption de la 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 (ci-après dénommée «la DCDT»), mentionnée au considérant 14 en tant que cadre général s'appliquant dans le contexte des échanges informatisés d'informations extraites des casiers judiciaires, devrait intervenir d'ici la fin de 2008. Cette décision-cadre du Conseil prévoira des garanties minimales pour la protection des données, dans le cas où des données à caractère personnel sont ou ont été transmises ou mises à disposition entre les États membres ⁽³⁾. La convergence des législations nationales s'en trouvera accrue pour ce qui concerne les conditions d'utilisation des données à caractère personnel (au sens de l'article 9 de la décision-cadre du Conseil sur les échanges d'informations extraites des casiers judiciaires).
8. À cet égard, il convient de souligner que les négociations sur la DCDT ont entraîné certaines modifications, dont certaines affectent nécessairement, de manière spécifique, le cadre juridique dans lequel se déroule l'échange d'informations extraites des casiers judiciaires:
- le champ d'application est désormais limité aux seules données à caractère personnel échangées avec d'autres États membres et ne couvre plus les données traitées uniquement à l'échelon national au sein d'un même État membre,
 - aucun mécanisme de coordination effective entre autorités compétentes en matière de protection des données n'est prévu.
9. Dans ce contexte, l'article 9 de la décision-cadre relative à l'échange d'informations extraites des casiers judiciaires — énonçant certaines «conditions d'utilisation des données à caractère personnel» — doit être considéré comme une *lex specialis* sur la protection des données, qui prévoit des garanties supplémentaires par rapport à celles énoncées dans la *lex generalis*, à savoir la DCDT. Cet article — en particulier en ses paragraphes 2 et 4 — précise le principe de limitation des finalités en ce qui concerne l'échange d'informations extraites des casiers judiciaires. Il ne prévoit des exceptions à ce principe que dans les circonstances explicitement mentionnées dans ces dispositions.
10. En troisième lieu, la Commission a présenté, en liaison étroite avec la proposition qui nous intéresse, une communication intitulée «Vers une stratégie européenne en matière d'e-Justice» ⁽⁴⁾. Avec cette communication, la Commission européenne entend contribuer au renforcement et au développement des outils e-Justice au niveau européen. La communication comporte un certain nombre d'initiatives qui auraient d'importantes répercussions sur la protection des données à caractère personnel, comme par exemple la création d'un réseau d'échanges sécurisé pour l'échange d'informations entre autorités judiciaires et la création d'une base de données européenne des traducteurs et interprètes en justice. Le CEPD prévoit de réagir à cette communication dans un document distinct.

⁽¹⁾ JO C 53 du 3.3.2005, p. 1.

⁽²⁾ L'échange d'informations par l'intermédiaire d'Eurojust en est un autre exemple. Le cadre juridique de cet échange sera modifié, après l'adoption d'une décision du Conseil sur le renforcement d'Eurojust et modifiant la décision 2002/187/JAI (voir l'initiative publiée au JO C 54 du 27.2.2008, p. 4).

⁽³⁾ Voir l'article 1^{er} de la proposition relative à cette décision-cadre du Conseil (dernière version en date disponible sur le registre du Conseil, 24 juin 2008, doc. 9260/08).

⁽⁴⁾ Communication de la Commission au Conseil, au Parlement européen et au Comité économique et social européen — Vers une stratégie européenne en matière d'e-Justice, doc. COM(2008) 329 final.

III. L'ÉCHANGE D'INFORMATIONS PRÉVU DANS LA DÉCISION-CADRE DU CONSEIL

11. L'article 11 de la décision-cadre du Conseil précise (au paragraphe 1) quelles informations doivent ou peuvent être transmises; il fournit également, au paragraphe 3, la base juridique de la proposition à l'examen. L'annexe II de la décision-cadre du Conseil présente le formulaire qui doit être utilisé pour l'échange. Ce document indique les informations que l'État membre requérant doit fournir et celles qui doivent être fournies en réponse à sa demande. Le formulaire peut être adapté par une décision du Conseil, comme le propose désormais la Commission.
12. L'article 11, paragraphe 1, établit une distinction entre les informations obligatoires, les informations facultatives, les informations complémentaires et toute autre information. Le formulaire qui figure à l'annexe II ne fait pas apparaître ces distinctions. À titre d'exemple, les informations relatives au nom des parents de la personne condamnée sont qualifiées, à l'article 11, d'informations facultatives ne devant être transmises que si elles figurent dans le casier judiciaire. Or, l'annexe II ne fait pas apparaître le caractère facultatif de cette transmission.
13. Le CEPD suggère de profiter des circonstances présentes pour remanier le formulaire afin de le mettre en conformité avec l'article 11. La transmission des données à caractère personnel sera ainsi limitée aux données réellement nécessaires aux fins de l'échange. Dans l'exemple susmentionné, la transmission automatique du nom des parents de la personne condamnée ne semble pas nécessaire. Elle pourrait causer inutilement du tort aux personnes concernées, notamment aux parents.

IV. LE SYSTÈME ECRIS

Observations d'ordre général

14. L'article 3 constitue l'élément central de la proposition. Il énonce que l'ECRIS est fondé sur une architecture informatique décentralisée et se compose de trois éléments: les bases de données relatives aux casiers judiciaires dans les États membres, une infrastructure de communication commune et un logiciel d'interconnexion.
15. Le CEPD appuie la présente proposition de création de l'ECRIS, sous réserve que les observations formulées dans le présent avis soient prises en compte.
16. Dans ce contexte, il souligne que, d'une part, aucune base de données européenne centrale n'est créée et qu'aucun accès direct aux bases de données relatives aux casiers judiciaires des autres États membres n'est prévu, tandis que, d'autre part, au niveau national, les compétences sont centralisées auprès des autorités centrales des États membres, désignées en application de l'article 3 de la décision-cadre du Conseil. Ce mécanisme limite au minimum le stockage et l'échange de données, tout en définissant clairement les compétences des autorités centrales. Dans le cadre de ce mécanisme, les États membres sont responsables du fonctionnement des bases de données nationales relatives aux casiers judiciaires et de l'efficacité des échanges. Ils sont également responsables du fonctionnement du logiciel d'interconnexion (article 3, paragraphe 2, de la proposition).
17. Il y aura une infrastructure commune. Il s'agira dans un premier temps du réseau S-TESTA ⁽¹⁾, qui pourra être remplacé par un autre réseau sécurisé géré par la Commission (article 3, paragraphe 4, de la proposition). Le CEPD croit comprendre que la Commission est responsable de l'infrastructure commune, bien que cela ne soit pas précisé à l'article 3. Le CEPD suggère de clarifier cette compétence dans le texte lui-même, pour des raisons de sécurité juridique.

Premier élément: les bases de données relatives aux casiers judiciaires dans les États membres

18. Dans son avis du 29 mai 2006, le CEPD s'est dit favorable à une architecture décentralisée, celle-ci permettant notamment d'éviter une reproduction supplémentaire de données à caractère personnel dans une base de données centrale. Le choix d'une architecture décentralisée implique automatiquement que les États membres sont responsables des bases de données relatives aux casiers judiciaires et du traitement des données à caractère personnel au sein de ces bases de données. Plus précisément, les autorités centrales des États membres sont, pour ce qui concerne ces bases de données, les responsables du traitement. En tant que responsables du traitement, elles sont responsables du contenu des bases de données et du contenu des informations qui sont échangées. La décision-cadre du Conseil établit les obligations incombant à l'État membre de condamnation et celles incombant à l'État membre de nationalité.
19. Dans ce cadre, l'ECRIS constitue un réseau d'entités homologues pour l'échange d'informations entre ces bases de données nationales. Un réseau d'entités homologues tel qu'ECRIS présente certains risques sur lesquels il convient de se pencher:
- dans la pratique, la répartition des compétences entre les autorités centrales des États membres ne fonctionne pas d'elle-même. Des mesures complémentaires sont nécessaires, pour veiller par exemple à ce que les informations détenues par l'État membre expéditeur et l'État membre destinataire (État de condamnation et État de nationalité) soient tenues à jour et identiques,
 - cette architecture entraîne une grande diversité dans la manière dont le système est appliqué par les différents États membres, diversité d'autant plus manifeste que les législations nationales divergent (comme c'est le cas en ce qui concerne les casiers judiciaires).
20. L'harmonisation de l'utilisation du réseau lui-même, ainsi que des procédures qui entourent son utilisation, est donc primordiale. Le CEPD note en particulier qu'il est important que l'utilisation du réseau se déroule intégralement de manière harmonisée, selon des critères élevés de protection des données. Les mesures d'exécution à arrêter en vertu de l'article 6 de la proposition sont donc de la plus haute importance. Le CEPD recommande que, à l'article 6, il soit fait référence à un niveau élevé de protection des données comme condition préalable à l'adoption de toutes les mesures d'exécution.

⁽¹⁾ Services télématiques transeuropéens entre administrations.

21. Les autorités nationales compétentes en matière de protection des données pourraient jouer un rôle à cet égard, à condition de fonctionner de manière harmonisée. Le CEPD suggère l'insertion d'un considérant soulignant le rôle des autorités compétentes en matière de protection des données, de la même manière que le considérant 11 et l'article 3, paragraphe 5, prévoient que la Commission fournit un appui aux États membres. Le nouveau considérant devrait également encourager les autorités compétentes en matière de protection des données à coopérer.
22. Enfin, le CEPD se félicite de la disposition figurant à l'article 3, paragraphe 3, visant à promouvoir l'usage des meilleures techniques disponibles afin d'assurer la confidentialité et l'intégrité des casiers judiciaires transmis aux autres États membres. Il serait toutefois souhaitable que les autorités compétentes en matière de protection des données participent également — associées en cela aux (autorités centrales des) États membres et à la Commission — au recensement de ces techniques.

Deuxième élément: l'infrastructure de communication commune

23. En raison de la responsabilité qui lui incombe à l'égard de l'infrastructure de communication commune, la Commission doit être considérée comme le fournisseur du réseau. Aux fins de la protection des données, la Commission peut être qualifiée de responsable du traitement au sens de l'article 2, point i), de la décision-cadre du Conseil relative à la protection des données à caractère personnel, même si ce n'est que pour une tâche limitée: fournir le réseau et en assurer la sécurité. Lorsque des données à caractère personnel seront traitées dans le cadre de la fourniture du réseau, ou si des problèmes de protection des données se posent en rapport avec la sécurité du réseau, le responsable sera la Commission, en qualité de responsable du traitement. Ce rôle de la Commission est comparable au rôle qu'elle joue dans les systèmes SIS, VIS et Eurodac, à savoir celui de responsable de la gestion opérationnelle (et non du contenu des données à caractère personnel). Ce rôle a été qualifié de «rôle de contrôleur sui generis»⁽¹⁾.
24. L'infrastructure de communication commune sera fondée sur S-TESTA, au moins à court terme. S-TESTA vise à interconnecter les organes de l'UE avec les autorités nationales, telles que les administrations et les agences réparties sur l'ensemble du territoire européen. Il s'agit d'un réseau de télécommunication spécialisé. Le centre d'exploitation du service est situé à Bratislava. Il constitue également le pilier d'autres systèmes d'information s'inscrivant dans un espace de liberté, de sécurité et de justice, tels que le Système d'information Schengen. Le CEPD souscrit au choix de S-TESTA, qui s'est avéré un système fiable en matière d'échange.
25. La responsabilité qui incombe à la Commission en tant que «contrôleur sui generis» a également des conséquences pour la législation applicable en matière de protection des données et pour le contrôle. L'article 3 du règlement 45/2001 dispose que ce règlement «s'applique au traitement de données à caractère personnel par toutes les institutions et tous les organes communautaires, dans la mesure où ce traitement est mis en œuvre pour l'exercice d'activités qui relèvent en tout ou en partie du champ d'application du droit communautaire».
26. Si les activités de traitement de la Commission relevaient en tout ou en partie du champ d'application du droit communautaire, il n'y aurait aucun doute quant à l'applicabilité du règlement 45/2001. En particulier, l'article 1^{er} de ce règlement prévoit que les institutions et organes communautaires assurent la protection des libertés et droits fondamentaux des personnes physiques, notamment de leur vie privée, à l'égard du traitement des données à caractère personnel. Aux termes de l'article 22 du règlement, la Commission doit «mettre en œuvre les mesures techniques et organisationnelles appropriées pour assurer un niveau de sécurité approprié au regard des risques présentés par le traitement et de la nature des données à caractère personnel à protéger». Ces activités ont lieu sous le contrôle du CEPD.
27. Cependant, en l'espèce et contrairement à ce qui se produit dans le cas du Système d'information Schengen⁽²⁾, il convient de noter que la base juridique des activités de traitement figure au titre VI du traité UE (troisième pilier). Cela signifie que ni le règlement n° 45/2001, ni aucun autre cadre juridique relatif à la protection des données et au contrôle, ne s'applique automatiquement aux activités de traitement de la Commission. Cela est regrettable pour une raison évidente, à savoir une protection insuffisante de la personne concernée, en particulier parce que le traitement de données à caractère personnel relatives aux condamnations pénales revêt un caractère sensible, comme en témoigne l'article 10, paragraphe 5, du règlement 45/2001 qui qualifie le traitement de données relatives aux condamnations pénales d'opérations de traitement susceptibles de présenter des risques particuliers. C'est également regrettable parce que le CEPD participe — sur la base d'autres instruments juridiques — au contrôle exercé sur S-TESTA. C'est pour cette raison que le CEPD propose d'ajouter à la décision une disposition indiquant que le règlement (CE) n° 45/2001 s'applique au traitement de données à caractère personnel relevant de la responsabilité de la Commission⁽³⁾.

Troisième élément: le logiciel d'interconnexion

28. La proposition distingue l'infrastructure technique commune permettant la connexion des bases de données et le logiciel d'interconnexion. Comme nous l'avons dit plus haut, les États membres sont responsables du fonctionnement du logiciel d'interconnexion. Aux termes du considérant 11, la Commission peut fournir ce logiciel mais les États membres semblent libres d'utiliser ou non ce logiciel au lieu de leur propre logiciel d'interconnexion.

⁽²⁾ Et de VIS et Eurodac, qui sont des systèmes relevant en tous points du champ d'application du droit communautaire.

⁽³⁾ Voir, à cet égard, dans le cadre du troisième pilier, l'article 39, paragraphe 6, de la décision du Conseil portant création de l'office européen de police (Europol), qui garantit l'application du règlement (CE) n° 45/2001 au traitement des données à caractère personnel relatives au personnel d'Europol (texte du 24 juin 2008, doc. 8706/08 du Conseil).

⁽¹⁾ Voir l'avis du 19 octobre 2005 sur trois propositions relatives au système d'information Schengen de deuxième génération (SIS II) (JO C 91 du 19.4.2006, p. 38, point 5.1).

29. La question se pose de savoir pourquoi il convient de distinguer les responsabilités selon qu'elles sont exercées à l'égard de l'infrastructure technique ou du logiciel d'interconnexion, et pourquoi la Commission ne devrait pas être responsable des deux. En effet, tous deux concernent le réseau formé par les autorités centrales des États membres (les points d'accès nationaux au réseau) et non l'échange d'informations au sein des États membres.

30. Confier cette responsabilité supplémentaire à la Commission n'affecterait pas le caractère décentralisé de l'architecture informatique, et permettrait par ailleurs d'optimiser l'efficacité de l'échange. Il est important d'accroître l'efficacité du point de vue de la protection des données, pour des raisons de qualité des données: seules les données essentielles doivent être échangées, et il faudrait éviter de devoir procéder à des échanges d'informations complémentaires qui seraient rendus nécessaires par des imperfections du système. Regrouper entre les mêmes mains les responsabilités exercées à l'égard de l'infrastructure de communication commune et du logiciel d'interconnexion permettrait en outre un meilleur contrôle du système.

31. Cela est d'autant plus important compte tenu de la fonction d'outil d'échange qu'exerce le logiciel. Parmi les caractéristiques importantes du logiciel d'interconnexion, celui-ci doit être capable de vérifier l'identité de l'expéditeur, ainsi que la compatibilité et l'intégrité des demandes, et, par conséquent, d'autoriser la validation des demandes. L'interopérabilité des logiciels utilisés par les États membres est donc une condition sine qua non. Tous les États membres ne doivent pas nécessairement utiliser le même logiciel (ce qui serait néanmoins la solution la plus pratique), mais le logiciel doit être totalement interopérable.

32. La proposition reconnaît la nécessité d'harmoniser les aspects relatifs au logiciel d'interconnexion. Les mesures d'exécution énumérées à l'article 6 — à arrêter conformément à une procédure de comité — comprennent par exemple «les procédures de vérification de la conformité des applications informatiques avec les spécifications techniques». L'article 6 mentionne également un ensemble commun de protocoles. Cependant, un tel ensemble commun de protocoles n'est pas prescrit pour le logiciel d'interconnexion. L'article 6 ne prévoit pas non plus de désigner un type de logiciel.

33. Pour les raisons qui précèdent, le CEPD recommande ce qui suit, afin d'améliorer l'efficacité et la sécurité des échanges:

— au minimum, il convient d'arrêter des mesures d'exécution garantissant l'interopérabilité des logiciels,

— le texte devrait — il s'agit-là de l'option à privilégier — prévoir, par le biais probablement d'une procédure de comité, que la Commission et les États membres sont tenus de mettre au point ou désigner un type de logiciel répondant à toutes les exigences susmentionnées,

— le texte devrait prévoir que la Commission sera responsable du logiciel d'interconnexion.

V. AUTRES QUESTIONS

Le manuel

34. L'article 6, point b), prévoit qu'un manuel, destiné à être arrêté conformément à la procédure de comité, déterminera la procédure à suivre pour l'échange d'informations, «portant notamment sur les modalités de l'identification des auteurs d'infractions». Le CEPD se demande ce que ce manuel contiendra précisément et si, par exemple, il prévoira que l'identification s'effectue au moyen de la biométrie.

35. Le CEPD souligne que l'identification des auteurs d'infractions ne devrait pas entraîner un échange de données à caractère personnel qui ne sont pas expressément visées par la décision-cadre. De plus, le manuel devrait établir des garanties appropriées pour le traitement et la transmission de catégories spéciales de données, telles que les données biométriques.

Collecte de données statistiques

36. L'article 6, point c) et l'article 8 font référence à la collecte de données statistiques, qui constituent un élément essentiel non seulement pour évaluer l'efficacité du système d'échange de données mais également pour contrôler le respect des garanties relatives à la protection des données. Dans ce contexte, le CEPD recommande que, comme c'est le cas dans d'autres instruments juridiques portant sur l'échange de données à caractère personnel⁽¹⁾, les éléments statistiques à collecter soient définis avec plus de précision et prennent dûment en compte la nécessité d'assurer un contrôle de la protection des données. Par exemple, les données statistiques pourraient explicitement inclure des éléments tels que le nombre de demandes d'accès ou de rectification des données à caractère personnel, la durée et l'achèvement du processus de mise à jour, la qualité des personnes ayant accès à ces données ainsi que les cas de violations de la sécurité. En outre, les données statistiques et les rapports basés sur celles-ci devraient être intégralement mis à la disposition des autorités compétentes en matière de protection des données.

Coordination du contrôle du traitement des données

37. Le CEPD a déjà souligné, dans son avis du 29 mai 2006 sur la décision cadre relative à l'échange d'informations extraites des casiers judiciaires, que la proposition ne devrait pas porter uniquement sur la coopération entre les autorités centrales, mais aussi sur la coopération entre les différentes autorités compétentes en matière de protection des données. Cette nécessité est devenue encore plus impérieuse depuis que les négociations sur la DCDT ont entraîné la suppression de la disposition établissant un groupe réunissant les autorités chargées de la protection des données au sein de l'UE et coordonnant leurs activités à l'égard du traitement des données dans le cadre de la coopération policière et judiciaire en matière pénale.

⁽¹⁾ Voir par exemple l'article 3, paragraphes 3 et 4, du règlement (CE) n° 2725/2000 du Conseil du 11 décembre 2000 concernant la création du système «Eurodac» pour la comparaison des empreintes digitales aux fins de l'application efficace de la convention de Dublin.

38. Par conséquent, en vue d'assurer un contrôle efficace ainsi qu'une circulation transfrontière satisfaisante des données extraites de casiers judiciaires, il serait nécessaire d'établir des mécanismes de coordination appropriés entre les autorités compétentes en matière de protection des données. Ces mécanismes devraient également tenir compte du pouvoir de contrôle du CEPD à l'égard de l'infrastructure S-TESTA. Ces mécanismes pourraient figurer dans une disposition spécifique ou être ajoutés aux mesures d'exécution à arrêter conformément à l'article 6 de la proposition.

Traductions

39. Les considérants 6 et 8, ainsi que l'exposé des motifs de la Commission, font référence au recours intensif à la traduction automatique. Si le CEPD se félicite de toute mesure visant à améliorer la compréhension mutuelle des informations transmises, il souligne également qu'il est important de bien définir et circonscrire le recours à la traduction automatique. En effet, une fois que des pré-traductions fidèles des catégories d'infractions figurant à l'annexe de la décision auront été établies, l'utilisation des codes communs permettra aux autorités nationales de lire la traduction automatique de ces catégories dans leur langue nationale. Ce recours à la traduction automatique est un instrument utile et de nature à favoriser la compréhension mutuelle des infractions en question.

40. Toutefois, le recours à la traduction automatique pour la transmission d'informations qui n'ont pas été fidèlement pré-traduites, telles que des observations ou des précisions supplémentaires, ajoutées dans des cas particuliers, est susceptible de nuire à la qualité des informations transmises — et, par là même, à celle des décisions prises sur leur base — et devrait en principe être exclu. Le CEPD recommande de préciser ce point dans les considérants de la décision du Conseil.

VI. CONCLUSIONS

41. Le CEPD recommande qu'il soit fait référence, dans les considérants de la proposition, à la consultation ayant donné lieu au présent avis.

42. Il est suggéré de profiter des circonstances présentes pour remanier le formulaire afin de le mettre en conformité avec l'article 11 de la décision-cadre du Conseil sur les casiers judiciaires, qui établit une distinction entre les informations obligatoires, les informations facultatives, les informations complémentaires et toute autre information.

43. Le CEPD appuie la proposition de création de l'ECRIS faisant l'objet du présent avis, sous réserve que soient prises en compte les observations qui y sont formulées, notamment les recommandations suivantes:

- la responsabilité de la Commission à l'égard de l'infrastructure de communication commune devrait être clarifiée dans le texte, pour des motifs tenant à la sécurité juridique,
- il convient d'ajouter à la décision une disposition indiquant que le règlement (CE) n° 45/2001 s'applique au traitement de données à caractère personnel relevant de la responsabilité de la Commission,
- l'article 6 doit faire référence à un niveau élevé de protection des données comme condition préalable à l'adoption de toutes les mesures d'exécution,
- un considérant devrait souligner le rôle exercé, en relation avec les mesures d'exécution, par les autorités compétentes en matière de protection des données, et devrait également encourager lesdites autorités à coopérer entre elles,
- il convient d'arrêter des mesures d'exécution garantissant l'interopérabilité des logiciels,
- il convient de prévoir, par le biais probablement d'une procédure de comité, que la Commission et les États membres sont tenus de mettre au point ou désigner un type de logiciel répondant à toutes les exigences,
- il devrait être précisé dans le texte que la Commission sera responsable du logiciel d'interconnexion.

44. Les éléments statistiques à collecter devraient être définis avec plus de précision et prendre dûment en compte la nécessité d'assurer un contrôle de la protection des données.

45. Il convient d'établir des mécanismes de coordination appropriés entre les autorités compétentes en matière de protection des données, en tenant compte du pouvoir de contrôle du CEPD à l'égard de l'infrastructure S-TESTA.

46. Il devrait être précisé, dans les considérants de la décision du Conseil, que le recours à la traduction automatique ne devrait pas être étendu à la transmission d'informations qui n'ont pas été fidèlement pré-traduites.

Fait à Bruxelles, le 16 septembre 2008.

Peter HUSTINX

Contrôleur européen de la protection des données