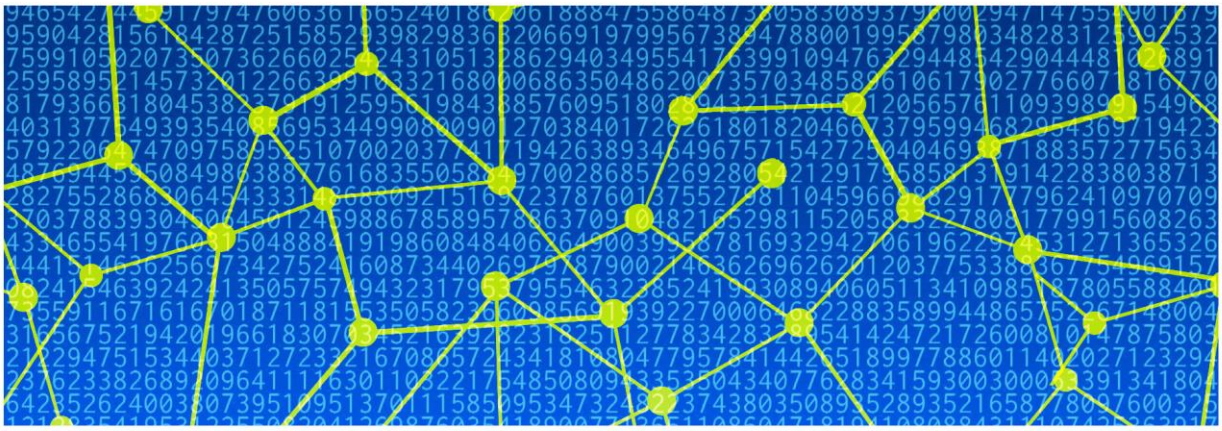

EUROPEAN DATA PROTECTION SUPERVISOR

Avis nº 3/2016

Avis sur les échanges d'informations relatives aux ressortissants de pays tiers dans le cadre du système européen d'information sur les casiers judiciaires (ECRIS)

EDPS

13 avril 2016

Le contrôleur européen de la protection des données (CEPD) est une institution indépendante de l'UE chargée en vertu de l'article 41, paragraphe 2, du règlement nº 45/2001 «[e]n ce qui concerne le traitement de données à caractère personnel, [...] de veiller à ce que les libertés et droits fondamentaux des personnes physiques, notamment leur vie privée, soient respectés par les institutions et organes communautaires», et «[...] de conseiller les institutions et organes communautaires et les personnes concernées pour toutes les questions concernant le traitement des données à caractère personnel». Conformément à l'article 28, paragraphe 2, du règlement nº 45/2001, la Commission a l'obligation, lorsqu'elle adopte une proposition de législation relative à la protection des droits et libertés des personnes à l'égard du traitement de données à caractère personnel, de consulter le CEPD.

Le CEPD et le contrôleur adjoint ont été nommés en décembre 2014 avec comme mission spécifique d'être plus constructifs et proactifs. Le CEPD a publié en mars 2015 une stratégie quinquennale exposant la manière dont il entend mettre en œuvre ce mandat et en rendre compte.

Le présent avis se rapporte à la mission du CEPD de conseil des institutions de l'UE sur les implications de leurs politiques en matière de protection des données et de promotion d'une élaboration responsable des politiques, conformément à l'action nº 9 de la stratégie du CEPD: «Faciliter l'élaboration responsable et éclairée de politiques». Le CEPD considère que la conformité aux exigences en matière de protection des données sera un élément clé de la réussite des échanges d'informations sur les casiers judiciaires de ressortissants de pays tiers au moyen de l'ECRIS.

Résumé

Le législateur de l'UE envisage depuis longtemps d'étendre les échanges d'informations concernant les casiers judiciaires au sein de l'UE aux ressortissants de pays tiers (RPT) dans le cadre de l'ECRIS (système européen d'information sur les casiers judiciaires). Le programme européen en matière de sécurité, dans lequel il était mentionné que l'ECRIS «ne fonctionne pas de façon satisfaisante pour les ressortissants de pays tiers ayant fait l'objet d'une condamnation dans l'UE», a accéléré l'adoption de la proposition d'extension de l'ECRIS aux RPT.

Dans le cadre actuel de l'ECRIS, la nationalité d'un État membre des personnes ayant fait l'objet d'une condamnation constitue un point central dans les échanges d'informations. C'est le motif pour lequel la création d'un système parallèle pour les ressortissants de pays tiers est justifiée. La Commission a choisi de mettre en œuvre les échanges d'informations concernant les casiers judiciaires de ressortissants de pays tiers dans un système décentralisé, au moyen de l'utilisation d'un index-filtre pour chacun des États membres participants. L'index-filtre sera mis à jour avec des informations spécifiques à chaque fois qu'un ressortissant de pays tiers fera l'objet d'une condamnation, puis il sera communiqué aux autres États membres.

Le CEPD a analysé avec soin la proposition législative et formule des recommandations en vue d'apporter son assistance au législateur et d'assurer la conformité des nouvelles mesures à la législation de l'UE en matière de protection des données, et en particulier aux articles 7 et 8 de la Charte des droits fondamentaux de l'UE.

Le CEPD se félicite de la proposition de mise en place d'un système décentralisé de l'UE pour traiter les données relatives aux casiers judiciaires de RPT qui serait fondé sur une fonctionnalité de recherche utilisant un système de concordance/non-concordance *(«hit/no hit»)* et ferait usage de mesures techniques destinées à limiter les atteintes aux droits que sont le respect de la vie privée et la protection des données à caractère personnel; cependant, le CEPD soulève trois préoccupations principales et formule plusieurs recommandations supplémentaires, exposées de manière plus détaillée dans le présent avis.

Premièrement, il conviendrait de mettre en place un régime pour les RPT correspondant à celui existant pour les ressortissants de l'UE, qui tienne compte de la spécificité des systèmes pénaux nationaux et réponde ainsi aux exigences de nécessité et de proportionnalité des traitements de données à caractère personnel.

Deuxièmement, le texte de la proposition évoque de manière erronée les informations contenues dans l'index-filtre comme étant des informations «anonymes». Le CEPD recommande de préciser que les informations traitées aux fins de l'ECRIS-RPT sont des données à caractère personnel, qui ont fait l'objet d'une procédure de pseudonymisation, et non pas des données anonymes.

Troisièmement, le CEPD considère que la création d'un autre type de système visant à traiter les données des ressortissants de l'UE, qui serait différent de celui mis en place pour les ressortissants de l'UE possédant la nationalité d'un pays tiers, ne répond pas aux exigences de proportionnalité prévues par la législation de l'UE en matière de protection des données et pourrait conduire à une discrimination. En conséquence, le CEPD recommande que les mesures prévues dans la proposition se réfèrent uniquement aux RPT, et non pas également aux ressortissants de l'UE possédant également la nationalité d'un pays tiers.

TABLE DES MATIÈRES

LE CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES,

vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 16,

vu la Charte des droits fondamentaux de l'Union européenne, et notamment ses articles 7 et 8,

vu la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données,

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 ses articles 28, paragraphe 2, 41, paragraphe 2, et 46, point d),

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

A ADOPTÉ L'AVIS SUIVANT:

I. INTRODUCTION ET CONTEXTE

I.1 Consultation du CEPD

1. Le 19 janvier 2016, la Commission européenne a publié une proposition de directive du Parlement européen et du Conseil modifiant la décision-cadre 2009/315/JAI du Conseil en ce qui concerne les échanges d'informations relatives aux ressortissants de pays tiers ainsi que le système européen d'information sur les casiers judiciaires (ECRIS), et remplaçant la décision 2009/316/JAI du Conseil (la «proposition»).[1] Le CEPD a été consulté de manière informelle préalablement à la publication de la proposition. Cependant, le CEPD regrette de ne pas avoir reçu de demande d'avis après la publication de la proposition.

I.2 Objectif de la proposition

2. L'ECRIS est un système électronique d'échange d'informations sur les condamnations antérieures prononcées par des juridictions pénales dans l'UE à l'encontre d'une personne déterminée, aux fins d'une procédure pénale à l'encontre d'une personne et, si la législation nationale l'autorise, à d'autres fins. Le système est fondé sur la décision-cadre 2009/315/JAI du Conseil (la «décision-cadre») et sur la décision 2009/316/JAI du Conseil.[2]

3. Conformément à l'exposé des motifs qui accompagne la décision-cadre, le principe qui sous-tend l'ECRIS est de permettre l'obtention d'informations complètes sur les

[1] COM(2016) 7 final, 2016/0002 (COD), Strasbourg, 19.1.2016.

[2] Décision-cadre 2009/315/JAI du Conseil du 26 février 2009 concernant l'organisation et le contenu des échanges d'informations extraites du casier judiciaire entre les États membres (la «décision-cadre»), JO L 93, 7.4.2009, p. 23; et décision du Conseil 2009/316/JAI du 6 avril 2009 relative à la création du système européen d'information sur les casiers judiciaires (ECRIS), en application de l'article 11 de la décision-cadre 2009/315/JAI, JO L 93, 7.4.2009, p. 33.

condamnations antérieures infligées à un ressortissant de l'UE auprès de l'État membre de nationalité de la personne en question, lequel est en mesure de fournir, sur demande, des informations exhaustives et à jour sur le casier judiciaire de ses ressortissants, quel que soit le lieu où les condamnations ont été prononcées dans l'Union européenne. En raison de cette architecture, à l'heure actuelle, les autorités se heurtent à des difficultés lorsqu'elles souhaitent échanger des informations sur des condamnations concernant des ressortissants de pays tiers et des apatrides (ci-après: RPT) au moyen de l'ECRIS, étant donné que «les RPT n'ont pas d'État membre de nationalité» et qu'«il faut, pour obtenir une vue d'ensemble complète des antécédents judiciaires d'une personne donnée, envoyer des demandes à tous les États membres de condamnation».[3]

4. Dès lors, l'objectif de la proposition consiste à renforcer l'efficacité de l'ECRIS en ce qui concerne les échanges d'informations sur des casiers judiciaires de RPT.

5. L'exposé des motifs décrit le système qui a été choisi pour réaliser cet objectif. Le système sera organisé d'une manière décentralisée, ce qui signifie qu'il n'existera pas de base de données de l'UE unique contenant les informations pertinentes, mais que chaque État membre tiendra à jour un fichier de données. Les États membres devront extraire les éléments d'identification de leur casier judiciaire national et les enregistrer dans un fichier distinct, l'«index-filtre», dès qu'un RPT fera l'objet d'une condamnation. Les données seront converties en «clés et verrous». L'index-filtre sera distribué à tous les autres États membres, leur permettant de faire des recherches de manière indépendante dans leurs propres locaux. Le système permettra aux États membres de comparer leurs propres données par rapport à celui-ci et de découvrir s'il existe d'autres inscriptions au casier judiciaire dans d'autres États membres (système de «concordance/non-concordance»).

II. IMPLICATIONS EN MATIÈRE DE PROTECTION DES DONNÉES

6. Le CEPD se félicite d la référence faite au considérant 12 de la proposition à la décision-cadre 2008/977/JAI du Conseil[4] relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale et à son application dans le contexte des échanges informatisés d'informations extraites des casiers judiciaires des États membres, en assurant un niveau suffisant de protection des données lorsque des informations sont échangées entre États membres, tout en permettant aux États membres de prévoir des normes plus élevées de protection en matière de traitement national des données. En outre, le CEPD relève que la proposition de directive sur la protection des données en matière pénale[5] (DPD) sera pleinement applicable au traitement de données à caractère personnel envisagé par la proposition, et ce dès son entrée en vigueur. **Dès lors, le CEPD recommande d'inclure dans le préambule de la proposition une référence à la DPD précisant la relation qui existe entre les instruments.**

[3] Exposé des motifs de la proposition, p. 3.
[4] 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 350/60, 30.12.2008.
[5] Proposition de directive du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, approuvée par le Conseil le 18 décembre 2015.

7. Les mesures prévues dans la proposition supposent le traitement de données à caractère personnel et, dès lors, elles constituent une atteinte au droit fondamental à la vie privée, inscrit à l'article 7 de la Charte des droits fondamentaux de l'UE (la «Charte de l'UE»), ainsi qu'au droit fondamental à la protection des données à caractère personnel, garanti par l'article 8 de la Charte de l'UE.[6] En ce sens, le CEPD se félicite de la référence contenue dans l'exposé des motifs à la jurisprudence de la Cour de justice de l'UE appliquant les articles 7 et 8 de la Charte de l'UE en ce qui concerne l'accès des autorités aux données à caractère personnel à des fins répressives, et en particulier à l'affaire *Digital Rights Ireland («DRI»)*.

8. Conformément à l'article 52, paragraphe 1, de la Charte, toute limitation de l'exercice des droits et des libertés consacrés par celle-ci doit être prévue par la loi, respecter leur contenu essentiel et, dans le respect du principe de proportionnalité, des limitations ne peuvent être apportées à ces droits et libertés que si elles sont nécessaires et répondent effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et libertés d'autrui.[7]

9. La lutte contre le terrorisme et contre la grande criminalité en vue d'assurer la sécurité publique est reconnue comme un objectif d'intérêt général en droit de l'UE.[8] Comme il est indiqué dans le préambule de la proposition, «l'échange d'informations sur les condamnations pénales est un aspect important de toute stratégie visant à lutter contre la criminalité et le terrorisme» (considérant 7). Dès lors, les mesures proposées répondent à un objectif d'intérêt général et peuvent être justifiées, dans le respect du principe de proportionnalité. Dans l'analyse ci-après, le CEPD se concentre sur plusieurs aspects relatifs à la proportionnalité des mesures proposées; il soulignera également la nécessité d'une meilleure définition du champ d'application matériel de la proposition, au regard du type de traitement de données concerné (anonymisation/pseudonymisation).

II.1 Champ d'application matériel de la mesure proposée

A. Traitement des empreintes digitales

10. Conformément à la proposition, d'une part, les États membres auront l'obligation inconditionnelle (sauf dans les cas où le prélèvement des empreintes est impossible pour des motifs d'ordre factuel[9]) de conserver les empreintes digitales des RPT qui ont été condamnés (article 1er, paragraphe 4, de la proposition). En outre, les empreintes digitales des RPT doivent être conservées *dans l'index-filtre*. D'autre part, les États membres ne sont tenus de conserver les empreintes digitales des citoyens de l'UE qui ont été condamnés que lorsque l'autorité centrale a accès à ces empreintes (article 11, paragraphe 1, point c), ii), de la décision-cadre). Il est entendu que l'autorité centrale peut ainsi avoir accès ou non aux empreintes digitales des citoyens de l'UE, en application de la législation nationale.

11. La collecte, la conservation et l'utilisation obligatoires des empreintes digitales aux fins du système de l'ECRIS-RPT qui sont proposées constituent des atteintes au titre des articles 7

[6] CJUE, C-293/12 et C-594/12, Digital Rights Ireland et Seitlinger e.a., 8.4.2014, points 33 et 36.
[7] Voir également l'arrêt *Digital Rights Ireland*, point 38.
[8] CJUE, C-402/05 P et C-415/05 P, Kadi et Al Barakaat International Foundation/Conseil et Commission, ECLi:EU:C:2008:461, point 383; C-539/10 P et C-550/10 P, Al-Aqsa/Conseil, ECLi:EU:C:2012:711, point 130; et C-145/09, Tsakouridis, ECLi:EU:C:2010:708, points 46 et 47.
[9] La formulation utilisée à l'article 4 bis, paragraphe 1, pour définir cette exception est la suivante: «à moins que, dans certains cas exceptionnels, cela ne soit pas possible».

et 8 de la Charte de l'UE. En ce sens, la Cour de justice de l'Union européenne (CJUE) a considéré dans son arrêt *Schwartz* qu'«il convient de constater que le prélèvement et la conservation d'empreintes digitales par les autorités nationales [...] constituent une atteinte aux droits au respect de la vie privée et à la protection des données à caractère personnel».[10] Si l'utilisation et la conservation d'empreintes digitales aux fins de l'ECRIS-RPT poursuivent effectivement un intérêt légitime, comme il est exigé à l'article 52, paragraphe 1, de la Charte, à savoir la lutte contre le terrorisme et contre la grande criminalité en vue d'assurer la sécurité publique, il convient d'apprécier si la mesure est nécessaire et proportionnée.

12. À titre préliminaire, il convient de relever que «les conditions en application desquelles les États membres conservent les empreintes digitales pendant les enquêtes et procédures pénales ne sont pas harmonisées par le droit de l'UE».[11] En pratique, cela signifie qu'à l'heure actuelle, les États membres disposent de règles différentes concernant la conservation des empreintes digitales à des fins répressives, ces règles variant selon la gravité des crimes et infractions. Le fait que chaque État membre dispose de sa propre politique pénale, avec des différences en ce qui concerne le niveau de gravité des infractions à partir duquel cet État est tenu de conserver les empreintes digitales des personnes qui ont été condamnées dans sa propre base de données judiciaire, est un facteur dont il doit être tenu compte lors de l'appréciation du caractère nécessaire de l'obligation d'utilisation des empreintes digitales.[12] En conséquence, on pourrait aboutir à une situation dans laquelle un État membre pourrait être tenu, conformément à la proposition, de collecter et de conserver les empreintes digitales d'une personne ayant commis une infraction mineure (ce qui représente une atteinte au droit à la vie privée dont dispose cette personne), alors que son droit national ne prévoirait pas d'obligation de conservation des empreintes digitales en lien avec le casier judiciaire de cette personne.

13. Le législateur justifie l'obligation faite aux États membres de conserver dans l'index-filtre les empreintes digitales de tous les RPT ayant été condamnés par la nécessité de «garantir l'identification»[13], eu égard au fait qu'il s'agit du «seul moyen de s'assurer de l'identité de la personne».[14] Il convient de reconnaître la valeur ajoutée que présente l'utilisation des empreintes digitales, en particulier pour l'identification de RPT, dans la mesure où l'on peut concevoir des situations dans lesquelles des RPT n'auraient pas de pièce d'identité ou porteraient des noms écrits dans des alphabets autres que ceux utilisés par les langues officielles de l'Union, ce qui pourrait donner lieu à des erreurs d'identification.

14. Cependant, selon l'exposé des motifs, actuellement, les autorités centrales de nombreux États membres ne stockent pas les empreintes digitales dans leurs casiers judiciaires nationaux et ne sont pas connectées au fichier automatisé d'empreintes digitales (FAED) national.[15] Certains États membres ont également fait part de «préoccupations d'ordre

[10] Voir, à cet égard, CJUE, C-291/12, Schwartz, 17.10.2013, point 30.
[11] Analyse d'impact, p. 15 (disponible en anglais uniquement).
[12] Comme la Commission l'a reconnu dans l'une de ses communications, «[l]e droit pénal constitue certainement un champ d'action politique sensible dans lequel les différences entre systèmes nationaux restent importantes, par exemple concernant les types et niveaux de sanctions de même que le classement de certains comportements comme infractions administratives ou pénales» - Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions, *«Vers une politique de l'UE en matière pénale: assurer une mise en œuvre efficace des politiques de l'UE au moyen du droit pénal»*, COM(2011) 573 final, 20.9.2011, p. 2.
[13] Considérant 10 du préambule.
[14] Exposé des motifs, p. 7.
[15] Exposé des motifs, p. 7.

constitutionnel»[16] soulevées par l'obligation de conserver les empreintes digitales de tous les RPT qui ont été condamnés, indépendamment du type d'infraction ou de crime commis.

15. Dès lors, on ne saurait considérer qu'il n'existe pas d'autre moyen, pour assurer l'identification des personnes, que l'utilisation des empreintes digitales et, en conséquence, la nécessité de l'obligation d'utilisation des empreintes digitales pour les RPT dans l'ECRIS n'a pas été démontrée.

16. Eu égard à l'ensemble des considérations qui précèdent, il ne semble ni nécessaire, ni proportionné d'imposer à tous les États membres une obligation de conservation des empreintes digitales des RPT, indépendamment des seuils de sanction et de la nature des infractions dans leur propre système national. **Le CEPD recommande au législateur d'étudier la création d'un régime pour les RPT correspondant à celui existant pour les ressortissants de l'UE concernant le traitement des empreintes digitales, en étendant aux RPT le champ d'application *rationae personae* de l'article 11 de la décision-cadre 2009/315/JAI en vigueur. Ceci permettrait de conférer un caractère facultatif à la conservation d'empreintes digitales au niveau national, en conformité avec les systèmes constitutionnels des États membres, tout en maintenant l'obligation d'intégrer les empreintes digitales de RPT dans l'index-filtre dans tous les cas dans lesquels ces empreintes sont effectivement conservées au niveau national.**

17. Le CEPD a souligné dans de précédents avis relatifs à des bases de données contenant des données biométriques que «le caractère par définition sensible des données biométriques nécessite des garanties spécifiques»[17], et notamment de réaliser une analyse d'impact ciblée en ce qui concerne l'utilisation de la biométrie, d'accorder de l'importance à la procédure d'enrôlement (la manière dont ces données seront recueillies), de mettre l'accent sur le niveau de précision et de mettre en place une procédure de secours afin de respecter la dignité des personnes qui auraient pu être identifiées par erreur et d'éviter de leur faire supporter la charge des imperfections du système.[18]

18. En ce qui concerne la mesure en cause en l'espèce, l'analyse d'impact de la proposition comporte des parties consacrées spécifiquement à l'analyse de l'utilisation des empreintes digitales, dans lesquelles plusieurs options sont prises en considération: conservation centralisée/décentralisée, utilisation obligatoire/facultative. En outre, la proposition législative comporte des garanties spécifiques qui tiennent compte du caractère sensible des données biométriques. Le mécanisme de pseudonymisation des données dans l'index-filtre et la mise en œuvre d'un système décentralisé de l'UE de «concordance-non-concordance» constituent des garanties dont le CEPD se félicite en ce qui concerne le traitement des empreintes digitales dans le fichier de données. En outre, **le CEPD recommande d'inclure, dans les actes d'exécution à venir qui seront proposés à la Commission, des garanties supplémentaires concernant la procédure d'enrôlement, la nécessité de mettre l'accent sur le niveau de précision et la nécessité de mettre en place une procédure de secours**.

[16] Exposé des motifs, p. 7.
[17] Avis du 19 octobre 2005 sur trois propositions concernant le système d'information Schengen de deuxième génération (SIS II) [COM(2005) 230 final, COM(2005) 236 final et COM(2005) 237 final], JO C 91, 19.4.2006, p. 43.
[18] Avis du CEPD sur le SIS II, 2005, p. 44.

B. Anonymisation/pseudonymisation

19. La proposition renvoie à un index-filtre «anonyme» permettant aux États membres de vérifier si d'autres États membres détiennent des informations concernant un RPT déterminé. Eu égard aux informations fournies, le CEPD considère que les informations fournies ne peuvent pas être qualifiées d'«anonymes» en raison de la nature du système, qui vise à permettre l'identification de personnes physiques disposant d'un casier judiciaire dans un autre État membre. En vue d'apprécier la terminologie utilisée dans la proposition, il convient de reprendre les définitions pertinentes:

- les «données à caractère personnel» sont définies comme suit dans l'ordre juridique de l'UE: «toute information concernant une personne physique identifiée ou identifiable, "personne concernée"; est réputée identifiable une personne qui peut être identifiée, directement ou indirectement».[19] L'expression recouvre donc également l'identification indirecte, par exemple au moyen d'un numéro de référence;
- la «pseudonymisation» est définie dans la DPD comme «le traitement de données à caractère personnel de telle façon qu'elles ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que celles-ci soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir cette non-attribution à une personne identifiée ou identifiable».[20] Partant, les données pseudonymisées demeurent des données à caractère personnel et, à ce titre, elles relèvent du champ d'application de la législation en matière de protection des données;
- le fait de «rendre anonyme» est défini à l'article 2, point k), de la décision-cadre 2008/977/JAI du Conseil comme «le fait de modifier des données à caractère personnel d'une façon telle que des données particulières sur des situations personnelles ou matérielles ne puissent plus être rattachées à une personne physique identifiée ou identifiable, ou alors seulement au prix d'un effort démesuré en termes de temps, de coût et de main-d'œuvre». Le groupe de travail «Article 29» a considéré que «[l]es "données anonymisées" sont donc des données anonymes qui concernaient auparavant une personne identifiable, mais ne permettent plus cette identification».[21] Étant donné que les «données anonymes» ne se rapportent pas à des personnes physiques identifiées ou identifiables, elles ne relèvent pas du champ d'application de la législation en matière de protection des données.

C'est au regard de ces définitions établies qu'il convient d'apprécier le libellé de la proposition.

20. La proposition autorise deux opérations différentes de traitement de données à caractère personnel concernant des RPT, outre les échanges d'informations en tant que tels. La première opération de traitement de données à caractère personnel est la «conservation» d'un ensemble de 11 éléments de données à caractère personnel[22] (au nombre desquels les

[19] Article 3, point 1, de la DPD.
[20] Article 3, point 4 bis, de la DPD.
[21] À cet égard, voir la conclusion énoncée par le groupe de travail «Article 29» dans son avis 4/2007 sur le concept de données à caractère personnel, selon laquelle «[l]es "données anonymisées" sont donc des données anonymes qui concernaient auparavant une personne identifiable, mais ne permettent plus cette identification» (p. 21). Voir également les «Observations complémentaires du CEPD sur le paquet de mesures pour une réforme de la protection des données», pages 1 à 4, publiées le 13 mars 2013.
[22] *Article 4 bis, paragraphe 1*: a) personne faisant l'objet de la condamnation [nom complet, date de naissance, lieu de naissance (ville et pays), sexe, nationalité et, le cas échéant, noms précédents]; b) forme de la condamnation (date de condamnation, nom de la juridiction, date à laquelle la décision est passée en force de chose jugée); c) infraction ayant donné lieu à la condamnation (date de l'infraction ayant entraîné la

empreintes digitales de la personne) par les États membres «dans le[s]quel[s] une condamnation est prononcée à l'encontre d'un ressortissant d'un pays tiers [...], à moins que, dans certains cas exceptionnels, cela ne soit pas possible».[23]

21. La seconde opération de traitement de données à caractère personnel est la création et l'utilisation de l'index-filtre. L'article 1, paragraphe 4, de la proposition, en application duquel il est inséré un *article 4 bis, paragraphe 2*, dans la directive ECRIS, prévoit que «[l]'autorité centrale crée un index-filtre contenant, *sous une forme anonymisée*, [des] informations» [caractères italiques ajoutés], lesquelles doivent contenir cinq des éléments de données conservés par les États membres[24], au nombre desquels les empreintes digitales. Selon l'exposé des motifs, l'index-filtre décrit ci-dessus *«ne contiendra pas de données à caractère personnel»*[25], étant donné que les informations qui seront conservées dans l'index-filtre seront *«anonymisée[s]»*.[26] En outre, il est également indiqué dans le préambule que «[l]es données à caractère personnel *devraient être rendues anonymes* pour que la personne concernée *ne puisse pas être identifiée*»[27] [caractères italiques ajoutés].

22. En conséquence, il est manifeste que la finalité même de l'existence de l'index-filtre contenant des empreintes digitales est en réalité l'identification précise des RPT qui possèdent un casier judiciaire dans d'autres États membres, en identifiant ces États membres et en leur demandant ensuite de communiquer toutes les informations disponibles concernant le RPT spécifique faisant l'objet de la recherche. Étant donné que, conformément aux définitions établies, toutes les informations concernant une personne physique identifiée ou identifiable constituent des données à caractère personnel, celles-ci englobent les informations contenues dans l'index-filtre. Il est précisé dans l'exposé des motifs de la proposition lui-même que «[p]our assurer l'*identification* correcte des ressortissants de pays tiers, il conviendrait d'inclure les empreintes digitales dans les données d'identification à conserver dans le casier judiciaire d'une personne et dans l'index-filtre».[28]

23. Même si la procédure utilisée pour enregistrer les données dans l'index-filtre est décrite comme «irréversible»[29], il demeure qu'il ne fait aucun doute que la finalité du traitement des données dans l'index-filtre est l'identification de RPT spécifiques qui possèdent un casier judiciaire dans d'autres États membres, par la production d'un résultat de type «concordance/non-concordance». Le résultat de type «concordance/non-concordance», associé aux éléments d'identification utilisés pour effectuer la recherche dans l'index-filtre, aboutit à l'identification de personnes physiques et à l'obtention d'informations supplémentaires les concernant (à savoir, possession ou non d'un casier judiciaire dans un ou plusieurs des autres États membres).

---

condamnation, nom ou qualification juridique de l'infraction et référence aux dispositions légales applicables); d) contenu de la condamnation (notamment la peine prononcée, les peines complémentaires éventuelles, les mesures de sûreté et les décisions ultérieures modifiant l'exécution de la peine); e) nom des parents de la personne condamnée; f) numéro de référence de la condamnation; g) lieu de l'infraction; h) le cas échéant, déchéances consécutives à une condamnation; i) numéro d'identité de la personne condamnée ou type et numéro de sa pièce d'identité; j) empreintes digitales de la personne; k) le cas échéant, pseudonyme et/ou alias.

[23] Article 1, paragraphe 4, de la proposition (nouvel article 4 bis, paragraphe 1, de la décision-cadre).

[24] Points a), e), i), j) et k) de la liste indiquée dans la note de bas de page 22.

[25] Exposé des motifs de la proposition, p. 5.

[26] Considérant 11 du préambule de la proposition.

[27] Considérant 11 du préambule de la proposition.

[28] Exposé des motifs, p. 10.

[29] Exposé des motifs, p. 5.

24. Dès lors, les données traitées dans l'index-filtre ne peuvent pas être définies comme des données «anonymes». Il apparaît qu'en réalité, ces données sont pseudonymisées - il s'agit donc de données à caractère personnel qui ont été soumises à la procédure de pseudonymisation, comme il est décrit au paragraphe 9 ci-dessus.

25. Si nous considérons que la technique envisagée[30] pour transformer les données figurant dans l'index-filtre en «clés et verrous» constitue une garantie appropriée pour limiter les atteintes au droit à la vie privée et au droit à la protection des données à caractère personnel des personnes physiques concernées[31], nous soulignons que la législation en matière de protection des données s'applique aux données figurant dans l'index-filtre. En conséquence, nous recommandons, à des fins de clarté et de sécurité juridique, de mettre en conformité le texte de la proposition et celui de la DPD[32], dans la mesure où il conviendrait de **supprimer de la proposition les références aux données anonymes et de les remplacer par des références précises à la procédure de pseudonymisation**.

C. Catégories de données à caractère personnel qui seront traitées

26. L'article 1, paragraphe 4, de la proposition, qui introduit un nouvel article 4 bis, paragraphe 1, dans la directive ECRIS, dresse une liste spécifique des données qui seront conservées par l'autorité centrale d'un État membre en cas de condamnation d'un RPT. Une liste similaire est énoncée à l'article 11 de la décision-cadre en vigueur pour les ressortissants de l'UE qui ont été condamnés. L'article 11 de la décision-cadre est plus limité que le nouvel article 4 bis en ce qui concerne l'atteinte à la vie privée de ressortissants de l'UE. Il établit trois catégories différentes de données qui seront traitées aux fins de l'ECRIS: les informations obligatoires, les informations facultatives (à titre d'exemple, les noms des parents de la personne condamnée) et les informations supplémentaires. Cette distinction n'existe pas pour les données de RPT qui seront traitées aux fins de l'ECRIS.

27. En pratique, lorsque l'on compare les deux listes, il apparaît que les informations concernant «le nom des parents de la personne condamnée», «le numéro de référence de la condamnation» et «le lieu de l'infraction», dont la transmission est facultative dans le cas de ressortissants de l'UE, doivent obligatoirement être transmises dans le cas de RPT. Le fait de disposer dans la proposition de directive de deux articles différents précisant les informations qui seront échangées, l'un de ces articles étant applicable aux ressortissants de l'UE et l'autre aux RPT, ne semble pas justifié. Il existe des informations supplémentaires qui ont un caractère obligatoire concernant les RPT, mais qui constituent uniquement des informations facultatives pour les ressortissants de l'UE. Cette distinction ne peut se justifier que si elle est fondée sur un raisonnement juridique solide et précis, qui semble faire défaut. Le CEPD recommande de s'abstenir d'insérer dans la directive un nouvel article qui dresserait spécifiquement la liste des informations relatives aux RPT qui seront traitées et, en lieu et

[30] Il apparaît que la Commission européenne a déjà prévu une solution technique pour la mise en œuvre de l'ECRIS-RPT et que le texte de la proposition a été rédigé de manière à correspondre à cette solution technique. À titre de remarque générale, la procédure devrait consister à commencer par définir les exigences auxquelles une solution technique doit répondre, puis, dans un second temps, à mettre à disposition ou élaborer une solution satisfaisant à ces exigences.

[31] Comparativement à un système de fichier-index pleinement centralisé.

[32] La DPD se trouve à l'étape finale de la procédure d'adoption. Le 18 décembre 2015, le Comité des représentants permanents (Coreper) a entériné les textes de compromis qui avaient fait l'objet d'un accord avec le Parlement européen dans le cadre de la réforme de la protection des données. L'accord entre le Conseil, le Parlement et la Commission était intervenu le 15 décembre. L'adoption formelle devrait intervenir au cours du premier semestre de 2016.

place, d'étendre aux RPT le champ d'application *rationae personae* de l'article 11 («Format et autres modalités d'organisation et de facilitation des échanges d'informations concernant les condamnations») de la décision-cadre 2009/315/JAI du Conseil.

II.2 Champ d'application personnel de la mesure

28. La proposition établit deux distinctions concernant le champ d'application personnel de la mesure proposée: l'une entre les ressortissants de l'UE et les RPT, et l'autre entre les ressortissants de l'UE qui sont uniquement citoyens d'un État membre de l'UE et les ressortissants de l'UE qui sont également citoyens d'un pays tiers. Les deux distinctions semblent découler de la création de l'index-filtre, lequel contiendra des données de RPT, y compris des données de citoyens de l'UE qui ont également la nationalité d'un autre État membre de l'UE. À cet effet, il est précisé à l'article 1, paragraphe 4, de la proposition (nouvel *article 4 bis, paragraphe 4*, de la future directive ECRIS) que la création de l'index-filtre «s'appliqu[e] également [...] pour les ressortissants de pays tiers qui ont la nationalité d'un État membre». La même distinction est établie au nouvel article 4 ter, paragraphe 2, relatif à l'«utilisation des index-filtres».

29. Le CEPD rappelle que l'article 8, paragraphe 2, de la Charte exige que le traitement de données à caractère personnel soit loyal. En outre, comme il a été démontré plus haut, le traitement de données à caractère personnel représente une atteinte au droit à la protection des données à caractère personnel[33], et l'article 52, paragraphe 1, de la Charte exige que toute atteinte aux dispositions de l'article 8 soit nécessaire et proportionnée.

30. La distinction établie entre les RPT et les ressortissants de l'UE en ce qui concerne les modalités différentes du traitement de leurs données à caractère personnel semble nécessaire, car elle est justifiée par des éléments objectifs se rapportant à la finalité des mesures proposées, comme il est décrit au paragraphe 3 du présent avis. En particulier, la création de l'index-filtre concernant les RPT est justifiée par le fait que, dès lors que les RPT n'ont pas d'État membre de nationalité, il n'est pas possible de leur appliquer la procédure normale de l'ECRIS concernant les échanges d'informations.[34]

31. En ce qui concerne la distinction établie entre les ressortissants de l'UE qui sont uniquement des ressortissants de l'UE et les ressortissants de l'UE qui sont également citoyens d'un pays tiers, la nécessité de cette mesure n'est pas démontrée. Si une opération de traitement déterminée, comme le traitement de données dans l'index-filtre, n'est pas nécessaire pour les ressortissants de l'UE, elle ne le sera pas non plus pour les ressortissants de l'UE qui sont également des RPT.

32. Dans l'arrêt Huber, la Cour de justice a considéré que l'ancien article 12, paragraphe 1, CE prévoyant le droit à l'absence de discrimination fondée sur la nationalité au sein de l'UE (actuel article 18, paragraphe 1, TFUE) doit être «interprét[é] en ce sens qu'il s'oppose à l'instauration par un État membre d'un système de traitement de données à caractère personnel spécifique aux citoyens de l'Union non-ressortissants de cet État membre dans l'objectif de lutter contre la criminalité».[35] La Cour a rappelé que «des situations comparables ne [doivent] pas [être] traitées de manière différente et que des situations différentes ne [doivent] pas [être] traitées de manière égale. *Un tel traitement ne pourrait être justifié que*

[33] À cet égard, voir paragraphe 7 ci-dessus et la référence qu'il contient.
[34] Exposé des motifs, p. 3.
[35] C-524/06, Huber, 16.12.2008, point 81.

s'il se fondait sur des considérations objectives indépendantes de la nationalité des personnes concernées et proportionnées à l'objectif légitimement poursuivi»[36] [caractères italiques ajoutés].

33. La différence de traitement prévue dans la proposition ne semble pas nécessaire pour atteindre l'objectif poursuivi, étant donné que, pour les ressortissants de l'UE, les autorités peuvent appliquer les procédures de l'ECRIS existantes pour partager des informations. L'exposé des motifs de la proposition ne comporte aucune explication concernant le motif pour lequel cette distinction serait nécessaire. La différence de traitement pourrait conduire à une discrimination, ce qui constituerait une violation de l'article 21, paragraphe 1, de la Charte de l'UE. Cet article prévoit l'interdiction, dans le champ d'application du TFUE, de «toute discrimination», quel qu'en soit le fondement, qui ne pourrait pas être justifiée conformément à l'article 52, paragraphe 1, de la Charte.

34. Enfin, le but de l'adoption d'une législation en matière de protection des données dans quelque domaine que ce soit (affaires commerciales ou pénales) est «de garantir [...] un niveau élevé de protection des droits et libertés fondamentaux des personnes physiques, [...], en ce qui concerne le traitement des données à caractère personnel»[37], ces droits incluant le droit à la non-discrimination. En conséquence, une situation dans laquelle le traitement de données à caractère personnel violerait les droits fondamentaux de la personne dont les données sont traitées, comme le droit à la non-discrimination consacré à l'article 21 de la Charte de l'UE, ne serait pas conforme à la législation de l'UE en matière de protection des données.

35. **Le CEPD recommande en conséquence de limiter strictement l'index-filtre aux informations se rapportant aux RPT, à l'exclusion des ressortissants de l'UE qui sont également citoyens d'un pays tiers.**

II.3 Qualité des données

36. Le CEPD se félicite du fait que la proposition prévoit, à l'article 4 bis, paragraphe 3, la mise à jour automatique des données à caractère personnel figurant dans l'index-filtre à la suite d'une modification ou d'une suppression des informations; cette obligation est similaire à celle consacrée à l'article 4, paragraphe 3, de la décision-cadre 2009/315/JAI du Conseil concernant les casiers judiciaires de ressortissants de l'UE. L'exactitude des informations est particulièrement importante lors des échanges d'informations dans le cadre d'affaires pénales, dans lesquelles une personne peut faire l'objet de décisions produisant des effets juridiques ou des effets négatifs en conséquence du traitement de données.

III. CONCLUSION

37. Comme il a déjà été indiqué dans l'avis du CEPD de 2006 concernant la proposition ECRIS, «[u]n autre système pourrait s'avérer nécessaire pour les ressortissants des pays tiers», étant donné que «[p]our des raisons évidentes, le système proposé ne peut s'appliquer

[36] C-524/06, Huber, point 75.
[37] Voir article 1er, paragraphe 1, de la décision-cadre 2008/977/JAI du Conseil et article 1er, paragraphe 1, de la directive 95/46/CE 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, JO L 281, 23.11.1995, p. 31 à 50.

dans de tels cas».[38] En conséquence, nous nous félicitons de la proposition actuelle et nous reconnaissons l'importance d'échanges d'informations extraites du casier judiciaire de personnes ayant été condamnées qui soient efficaces, particulièrement dans le contexte de l'adoption du programme européen en matière de sécurité.[39]

38. Le CEPD a analysé avec soin la proposition et formule les recommandations ci-après, en vue d'assurer la conformité à la législation de l'UE en matière de protection des données:

1) en ce qui concerne l'utilisation obligatoire des empreintes digitales concernant les RPT, **il conviendrait de créer un régime pour les RPT correspondant à celui existant pour les ressortissants de l'UE**, conforme aux règles existantes en matière de collecte des empreintes digitales au niveau national;

2) les références aux données anonymes devraient être supprimées de la proposition et remplacées par des **références précises à la procédure de pseudonymisation**;

3) les **données qui seront conservées au niveau national concernant les ressortissants de l'UE ayant été condamnés et les RPT ayant été condamnés ne devraient pas se voir appliquer des classifications différentes**. À cette fin, il conviendrait d'étendre le régime existant en vigueur pour les ressortissants de l'UE (à titre d'exemple, «données facultatives», «données supplémentaires») aux RPT;

4) **l'utilisation de l'index-filtre devrait être strictement limitée aux données à caractère personnel des RPT**, cette catégorie de personnes ne devant pas inclure les ressortissants de l'UE qui sont également citoyens d'un pays tiers.

39. En outre, le CEPD formule les recommandations ci-après, dont la mise en œuvre permettrait de renforcer le niveau de protection des données à caractère personnel traitées aux fins de l'ECRIS-RPT:

1) le préambule de la proposition devrait **envoyer à la DPD**, en précisant la relation qui existe entre les instruments;

2) il conviendrait de fournir des garanties supplémentaires en ce qui concerne le traitement des empreintes digitales dans les actes d'exécution qui seront proposés par la Commission, **concernant la procédure d'enrôlement, la nécessité de mettre l'accent sur le niveau de précision et la nécessité de mettre en place une procédure de secours**.

Fait à Bruxelles, le 13 avril 2016

Giovanni BUTTARELLI

Contrôleur européen de la protection des données

[38] Avis du CEPD concernant la proposition de décision-cadre du Conseil relative à l'organisation et au contenu des échanges d'informations extraites du casier judiciaire entre les États membres [COM(2005) 690 final], JO C 313/26, 20.12.2006, points 15 et 18.

[39] «Programme européen en matière de sécurité» - Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions du 28 avril 2015, COM(2015) 185 final.