Avis du contrôleur européen de la protection des données sur la communication de la Commission au Parlement européen et au Conseil intitulée «Renforcer la coopération dans le domaine de la répression au sein de l'UE: le modèle européen en matière d'échange d'informations (EIXM)»

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,[1]

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 28, paragraphe 2,[2]

vu la décision-cadre 2008/977/JAI du Conseil du 27 novembre 2008[3] 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:

1. INTRODUCTION

1.1. Consultation du CEPD

1. Le 7 décembre 2012, la Commission a adopté une communication intitulée «Renforcer la coopération dans le domaine de la répression au sein de l'UE: le modèle européen en matière d'échange d'informations (EIXM)» (ci-après la «communication»).[4] Ce même jour, la Commission a adopté un rapport sur la

[1] JO L 281, du 23.11.1995, p. 31.
[2] JO L 8, du 12.01.2001, p. 1.
[3] JO L 350, du 30.12.2008, p. 60.
[4] COM (2012) 735 final

mise en œuvre de la décision 2008/615/JAI du Conseil du 23 juin 2008 relative à l'approfondissement de la coopération transfrontalière, notamment en vue de lutter contre le terrorisme et la criminalité transfrontalière (la «Décision Prüm»).[5] Ce rapport ne fera pas l'objet d'observations distinctes dans le présent avis, mais il est mentionné ici pour mieux comprendre le contexte.

2. Préalablement à l'adoption de la communication, le CEPD a eu la possibilité de formuler des observations informelles. Le CEPD se félicite que certaines de ses observations aient été prises en compte dans la communication.

1.2. Contexte et objectifs de la communication

3. Le programme de Stockholm[6] vise à relever les futurs défis mais aussi à renforcer davantage le thème de la liberté, de la sécurité et de la justice par des mesures axées sur les intérêts et besoins des citoyens. Il établit les priorités de l'UE dans le domaine de la justice et des affaires intérieures pour la période 2010-2014 et définit les orientations stratégiques de la programmation législative et opérationnelle dans le domaine de la liberté, de la sécurité et de la justice conformément à l'article 68 du traité sur le fonctionnement de l'Union européenne (le «TFUE»)[7].

4. En particulier, le programme de Stockholm reconnaît que le développement de la gestion et des échanges d'informations doit se faire de manière cohérente et structurée dans le domaine de la sécurité intérieure de l'UE et invite le Conseil et la Commission à mettre en œuvre une stratégie de gestion de l'information pour la sécurité intérieure de l'Union, qui prévoie un dispositif renforcé de protection des données. Dans ce contexte, le programme de Stockholm invite également la Commission à évaluer la nécessité de mettre au point un modèle européen en matière d'échange d'informations (EIXM), à partir d'une évaluation des instruments existants dans le domaine des échanges d'informations de l'UE. Cette évaluation permettra de déterminer si ces instruments fonctionnent comme il était initialement prévu et s'ils répondent aux objectifs de la stratégie de gestion de l'information[8].

5. Dans le cadre du suivi du programme de Stockholm, la Commission a publié une communication en juillet 2010[9] (ci-après la «communication de 2010») qui présente un panorama complet des mesures qui, à l'échelle de l'UE, sont en place, en cours de mise en œuvre ou d'examen et qui régissent la collecte, le stockage ou l'échange transfrontalier d'informations à caractère personnel à des fins répressives ou de gestion des flux migratoires.

---

[5] COM (2012) 732 final

[6] Le programme de Stockholm – Une Europe ouverte et sûre qui sert et protège les citoyens, document 5731/10 du Conseil du 3.3.2010.

[7] Traité sur le fonctionnement de l'Union européenne, JO C 83/47, du 30.03.2010

[8] Le programme de Stockholm – Une Europe ouverte et sûre qui sert et protège les citoyens, document 5731/10 du Conseil du 3.3.2010, section 4.2.2

[9] Communication de la Commission du 20 juillet 2010 au Parlement européen et au Conseil intitulée «Présentation générale de la gestion de l'information dans le domaine de la liberté, de la sécurité et de la justice», COM(2010) 385 final.

6. Répondant à l'invitation du programme de Stockholm et sur la base de la communication de 2010, la présente communication a pour objectif de faire le point sur la façon dont l'échange transfrontalier d'informations dans l'UE fonctionne dans la pratique et de recommander d'éventuelles améliorations.

2. OBSERVATIONS

2.1. Observations générales

Nécessité d'améliorer l'échange d'informations tout en respectant les droits fondamentaux

7. Comme il a déjà été signalé dans des avis précédents[10], le CEPD reconnaît qu'un meilleur échange d'informations est un objectif politique essentiel pour l'Union européenne, dans le domaine de la liberté, de la sécurité et de la justice. L'importance de l'échange d'informations mérite d'autant plus d'être soulignée qu'il n'existe pas de force de police européenne, de système européen de justice pénale ou de contrôle aux frontières entièrement harmonisé. Les mesures relatives à l'information constituent donc une contribution essentielle de l'Union européenne, car elles permettent aux autorités nationales des États membres de lutter efficacement contre la criminalité transnationale et de protéger les frontières extérieures de manière effective.

8. Toutefois, ces mesures ne doivent pas seulement contribuer à assurer la sécurité des citoyens, mais elles sont également tenues, au sein de notre société européenne, de respecter pleinement les droits fondamentaux des citoyens, notamment le droit à la protection des données à caractère personnel. C'est d'autant plus important que l'échange d'informations dans le domaine de la coopération policière et judiciaire en matière pénale porte principalement sur les données à caractère personnel. Le traitement des données à caractère personnel dans ce domaine présente des risques spécifiques pour les personnes physiques et exige donc un niveau élevé de protection des données.

9. Le CEPD apprécie l'attention généralement portée à la protection des données dans la communication. Il se félicite que la communication évoque les principes matériels de i) sauvegarde des droits fondamentaux - en particulier le droit au respect de la vie privée et la protection des données à caractère personnel - et ii) l'exigence de la nécessité qui implique qu'une restriction du droit au respect de la vie privée ne peut être justifiée que si elle est prévue par la loi, si elle poursuit un but légitime et si elle est nécessaire dans une société démocratique. La communication rappelle également qu'il est essentiel de vérifier la nécessité de toute mesure adoptée et de respecter le principe de limitation des finalités.[11]

10. Le CEPD note avec satisfaction que la communication souligne la nécessité de garantir un niveau élevé de qualité, de sécurité et de protection des données et

[10] Voir, par exemple, l'avis du CEPD du 10 juillet 2009 sur la communication de la Commission au Parlement européen et au Conseil sur un espace de liberté, de sécurité et de justice au service des citoyens, JO 276, du 17.11.2009, p. 8, et l'avis du CEPD du 7 octobre 2009 sur les propositions relatives à l'accès à EURODAC à des fins répressives, JO C 92, du 10.04.2010, p. 1.
[11] Voir point 2.5 de la communication.

insiste sur le fait que «quelle que soit la combinaison ou la séquence utilisée pour échanger des informations, les règles relatives à la protection des données, à la sécurité et à la qualité des données, et aux fins pour lesquelles les instruments sont susceptibles d'être utilisés doivent être respectées».[12]

Le contexte des instruments déjà disponibles

11. La communication indique, dès le début, que l'échange d'informations fonctionne généralement bien, ajoutant qu'aucune nouvelle base de données dans le domaine de la répression ni aucun nouvel instrument d'échange d'informations n'est nécessaire à l'échelle de l'UE; toutefois, les instruments existants devraient bénéficier d'une meilleure mise en œuvre. Le CEPD se félicite de cette conclusion. La multiplicité des systèmes d'échange transfrontalier d'informations comportant des risques en termes de protection des données à caractère personnel et d'atteinte à la vie privée, le CEPD a préconisé dans plusieurs avis qu'avant de créer un nouvel instrument, une évaluation minutieuse et plus actuelle soit réalisée afin de déterminer si une mise en œuvre complète des instruments existants ne serait pas suffisante.[13]

12. La communication est essentiellement axée sur l'utilisation par les États membres de quatre instruments de l'UE: l'initiative suédoise[14], les décisions Prüm[15], Europol[16] et le système d'information Schengen[17]. Elle ne traite pas de tous les instruments de l'UE existants et envisagés dans le domaine de la coopération policière et judiciaire en matière pénale ni ne mentionne, par exemple, le système européen d'information sur les casiers judiciaires pour les ressortissants de l'UE.[18]

---

[12] Voir point 2.3 de la communication.

[13] Voir, par exemple, l'avis du CEPD du 5 septembre 2012 au sujet de l'accès des services répressifs à EURODAC, l'avis du CEPD du 30 septembre 2010 au sujet de la communication de la Commission au Parlement européen et au Conseil intitulée «Présentation générale de la gestion de l'information dans le domaine de la liberté, de la sécurité et de la justice», l'avis du CEPD du 24 novembre 2010 au sujet de la Communication de la Commission au Parlement européen et au Conseil concernant la politique antiterroriste de l'UE: principales réalisations et défis à venir, l'avis du CEPD du 20 décembre 2007 sur le projet de proposition de décision-cadre du Conseil relative à l'utilisation des données des dossiers passagers (Passenger Name Record — PNR) à des fins répressives, et l'avis du CEPD du 19 octobre 2005 sur trois propositions concernant le système d'information Schengen de deuxième génération (SIS II).

[14] Décision-cadre 2006/960/JAI du Conseil du 18 décembre 2006 relative à la simplification de l'échange d'informations et de renseignements entre les services répressifs des États membres de l'Union européenne, JO L 386, du 29.12.2006, p. 89

[15] Décision 2008/615/JAI du Conseil du 23 juin 2008 relative à l'approfondissement de la coopération transfrontalière, notamment en vue de lutter contre le terrorisme et la criminalité transfrontalière, JO L 210, du 06.08.2008, p. 1 et décision 2008/616/JAI du Conseil du 23 juin 2008 concernant la mise en œuvre de la décision 2008/615/JAI relative à l'approfondissement de la coopération transfrontalière, notamment en vue de lutter contre le terrorisme et la criminalité transfrontalière, JO L 210, du 06.08.2008, p. 12.

[16] Décision du Conseil 2009/371/JAI portant création de l'Office européen de police, JO L 121 du 15.05.2009, p. 37.

[17] Décision 2007/533/JAI du Conseil du 12 juin 2007 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen de deuxième génération (SIS II), JO 205, du 07.08.2007, p.63.

[18] 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, JO L 93, du 07.04.2009, p. 23, et décision 2009/316/JAI du Conseil du 6 avril 2009 relative à la création du système

En outre, bien que la communication mentionne d'autres instruments de l'UE dans le domaine de la liberté, de la sécurité et de la justice (par exemple, le système informatique douanier, le système d'information sur les visas, EURODAC, EUROSUR) ou initiatives (par exemple, les propositions pour un système entrée-sortie), elle ne les analyse pas.

13. Finalement, le CEPD attire l'attention sur le fait que les instruments juridiques dans des domaines autres que ceux de la liberté, de la sécurité et de la justice doivent également être pris en compte, puisqu'ils prennent une importance croissante (voir les instruments évoqués au point 16).

Tendances dans les moyens d'enquête

14. Les nouvelles technologies ont pour effet d'accroître le volume d'informations disponibles et d'élargir l'éventail des utilisations possibles de ces informations. Dans une société de l'information, il existe une tendance logique à ce que les services répressifs recourent plus largement aux informations disponibles dans des sources accessibles et combinent ces informations à l'aide d'outils informatiques sophistiqués. Les phénomènes technologiques, tels que l'informatique en nuage, les réseaux sociaux, le télépéage et les dispositifs de localisation géographique, ainsi que le couplage et le partage de données entre différentes bases de données ou l'utilisation d'outils d'analyse destinés à prévoir les comportements humains ont profondément modifié la façon dont chaque donnée peut être collectée et traitée ultérieurement. Les méthodes de travail des services répressifs, telles que l'extraction des données et le profilage, deviennent de plus en plus proactives, et des enquêtes sont en cours sur la base des développements généraux, quelquefois en l'absence de soupçon concret, mais à l'aide d'outils informatiques puissants.

15. Il existe une tendance générale et croissante à accorder aux services répressifs un accès aux données disponibles qui, initialement, ont été, sont ou seront collectées et traitées à des fins autres que la lutte contre la criminalité et qui concernent des personnes physiques qui, en principe, ne sont soupçonnées d'aucune infraction. Un accès élargi est plus souvent donné ou envisagé pour les services répressifs à plusieurs systèmes d'information et d'identification à grande échelle établis, par exemple, dans les domaines de l'immigration et des contrôles aux frontières[19].

---

européen d'information sur les casiers judiciaires (ECRIS), en application de l'article 11 de la décision-cadre 2009/315/JAI, JO L 93, du 07.04.2009, p. 33.

[19] Voir, par exemple, la décision 2008/633/JAI du Conseil du 23 juin 2008 concernant l'accès en consultation au système d'information sur les visas (VIS) par les autorités désignées des États membres et par l'Office européen de police (Europol) aux fins de la prévention et de la détection des infractions terroristes et des autres infractions pénales graves, ainsi qu'aux fins des enquêtes en la matière, JO L 218, du 13.08.2008, p. 129; la proposition modifiée de la Commission de règlement du Parlement européen et du Conseil relatif à la création du système «Eurodac» pour la comparaison des empreintes digitales aux fins de l'application efficace du règlement (EU) n° […/…] (établissant les critères et mécanismes de détermination de l'État membre responsable de l'examen d'une demande de protection internationale présentée dans l'un des États membres par un ressortissant de pays tiers ou un apatride) et pour les demandes de comparaison avec les données d'EURODAC présentées par les services répressifs des États membres et Europol à des fins répressives, et modifiant le règlement (UE) n° 1077/2011 portant création d'une Agence européenne pour la gestion opérationnelle des systèmes d'information à grande échelle dans le domaine de la liberté, de la sécurité et de la justice (refonte), COM (2012) 254 final, du 30.05.2012 et la proposition de la Commission de règlement du Parlement européen et du Conseil portant création d'un système d'entrée/sortie pour l'enregistrement des entrées

16. Jusqu'à présent, l'on constatait une séparation claire entre les activités répressives et celles du secteur privé, les missions répressives étant effectuées par des services ad hoc et le secteur privé étant sollicité au cas par cas pour communiquer des données à caractère personnel à ces services répressifs en cas de soupçons concrets. On assiste aujourd'hui à une tendance visant à obliger les acteurs privés à coopérer systématiquement avec les services répressifs. Cette tendance est, par exemple, liée aux données générées par l'utilisation des communications électroniques[20] et aux données des passagers aériens qui se rendent dans certains pays tiers[21], et elle se développe également dans le secteur financier[22].

17. Le volume croissant d'informations disponibles en dehors du domaine de la répression ainsi que l'utilisation de nouveaux outils informatiques puissants par les services répressifs contribuent, dans une certaine mesure, à ce que, actuellement, l'on passe d'une surveillance des personnes physiques soupçonnées d'avoir commis une infraction ou d'avoir participé à une infraction ou pour lesquelles des indices concrets donnent de bonnes raisons de croire qu'elles commettront des infractions, à une surveillance plus générale dans laquelle toutes les personnes physiques peuvent être considérées *a priori* comme des malfaiteurs potentiels et font l'objet d'une surveillance pour cette raison même.

Conséquences

18. En raison de cette évolution de grande ampleur, il est nécessaire de repenser et même de redéfinir le bon équilibre entre la répression et le respect des droits fondamentaux des personnes physiques. Il convient par exemple de noter que lorsque des informations sont recueillies par des méthodes de surveillance en dehors d'une affaire pénale concrète, le contexte même de la protection des droits fondamentaux change. L'on pourrait soutenir que, tant qu'aucune affaire n'est portée devant un tribunal, le principe d'un procès équitable (article 6 de la Convention européenne des droits de l'homme) ne peut être appliqué et que, par conséquent, les questions relatives à la protection des données et au respect de la vie privée devraient revêtir une plus grande importance.

19. Cela suppose en premier lieu une réflexion sur l'efficacité des principes de protection des données, compte tenu de l'évolution technologique ainsi que du

---

et sorties des ressortissants de pays tiers franchissant les frontières extérieures des États membres de l'Union européenne, COM (2013) 95 final, du 28.02.2013.

[20] Directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE, JO L 105, du 13.04.2006, p. 54.

[21] Voir la décision 2012/472/UE du Conseil du 26 avril 2012 relative à la conclusion de l'accord entre les États-Unis d'Amérique et l'Union européenne sur l'utilisation des données des dossiers passagers et leur transfert au ministère américain de la sécurité intérieure, JO L 215, du 11.08.2012, p 4.

[22] Directive 2005/60/CE du Parlement européen et du Conseil du 26 octobre 2005 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux et du financement du terrorisme, JO L 309, du 25.11.2005, p. 15 (actuellement à l'examen). Voir également la communication du 13 juillet 2011 de la Commission au Parlement européen et au Conseil intitulée «Options envisageables pour la création d'un système européen de surveillance du financement du terrorisme», COM(2011)429, final.

volume croissant de données collectées et utilisées à des fins répressives. Cela peut aboutir à des changements et/ou à des garanties supplémentaires.

20. En second lieu, aujourd'hui plus que jamais, une réflexion approfondie s'impose sur l'échange d'informations au sein de l'UE, compte tenu de l'évolution des systèmes d'information à grande échelle et de l'utilisation croissante des données collectées initialement à d'autres fins que la lutte contre la criminalité. Cette réflexion doit également porter sur les bénéfices pour la sécurité publique de la tendance actuelle à une surveillance généralisée, systématique et proactive des personnes non suspectes et sur son utilité réelle dans la lutte contre la criminalité.

21. Le CEPD se félicite de ce que la communication constitue une première étape vers un processus d'évaluation complet et encourage la Commission à mener ces réflexions approfondies, dont le résultat doit déboucher sur une politique globale, intégrée et bien structurée de l'UE sur la gestion de l'information et de l'échange dans ce domaine.

La relation avec le cadre actuel et le cadre proposé concernant la protection des données

22. Le CEPD souligne qu'il est capital de garantir un cadre légal cohérent et complet relatif à la protection des données. Une première étape importante a été franchie lors de l'adoption de la décision-cadre 2008/977/JAI du Conseil[23]. Toutefois, cet instrument juridique ne peut être considéré comme un cadre complet, notamment parce que ses dispositions n'ont pas une portée générale. Elles ne s'appliquent pas aux situations domestiques, lorsque les données à caractère personnel émanent de l'État membre qui les utilise[24]. Deuxièmement, les autres instruments de protection des données utilisables dans le domaine de la liberté, de la sécurité et de la justice doivent être davantage harmonisés et structurés.

23. Le CEPD aimerait souligner que les discussions en cours sur la proposition de la Commission du 25 janvier 2012 pour une directive s'appliquant au traitement des données à caractère personnel à des fins répressives[25] ne doivent pas empêcher la Commission de dresser, dès à présent, un inventaire des problèmes et risques en matière de protection des données et des améliorations possibles dans le contexte juridique actuel. En revanche, les discussions sur la directive proposée pourraient fournir une inspiration pour développer davantage le modèle européen en matière d'échange d'informations. Dans ce contexte, les discussions portant sur les différences claires de traitement des données relatives à des personnes suspectes et de celles relatives à des personnes non suspectes en sont un bon exemple. Le

[23] 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, JL L 350, 30.12.2008, p. 60.

[24] Voir également l'avis du CEPD du 19 décembre 2005 concernant la proposition de décision-cadre du Conseil relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale (COM (2005)475 final), JO C 47, 25.02.2006, p. 27.

[25] Proposition du 25 janvier 2012 concernant une directive 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, COM(2012) 10 final.

CEPD recommande d'analyser plus en profondeur ces notions dans le contexte du modèle européen en matière d'échange d'informations.

24. Le CEPD note que la communication se réfère à la proposition de directive de la Commission. En particulier, la communication mentionne la nécessité de réviser les instruments actuels pour les aligner sur la directive proposée. Le CEPD souscrit totalement à cette intention et encourage la Commission à prendre des mesures dans ce sens.

2.2. Observations spécifiques

Évaluation des instruments

25. La communication donne des exemples de réussites en matière d'échange d'informations dans le cadre de l'initiative suédoise et des décisions Prüm, tout en soulignant que la mise en œuvre des décisions Prüm présente un retard important et que l'initiative suédoise n'a pas atteint son plein potentiel. En ce qui concerne les canaux SIS et SIRENE, la communication signale qu'elle ne présente aucune recommandation en raison des changements d'envergure qui sont déjà en cours, notamment la migration vers le SIS II.[26]

26. Comme cela est mentionné dans la communication, les premiers résultats de l'échange d'informations basé sur l'initiative suédoise et les décisions Prüm sont positifs dans le cadre de la répression. Toutefois, le CEPD souhaite faire remarquer qu'une évaluation complète de ces instruments (y compris en cas d'insuffisances et de faiblesses avérées des systèmes, telles que le nombre de personnes arrêtées à tort ou mises dans l'embarras à la suite d'un faux résultat positif dans le système) ne peut être réalisée qu'après leur mise en œuvre complète. Il encourage la Commission à poursuivre l'évaluation de ces instruments durant et après leur mise en œuvre complète.

Choix des canaux

27. Dans sa communication, la Commission déclare que, indépendamment des obligations juridiques d'utiliser des canaux spécifiques, les États membres utilisent différents canaux à des degrés divers. Bien que rien dans la communication ne semble indiquer que l'utilisation de canaux différents soulève des problèmes particuliers, la Commission conclut qu'il est temps d'adopter une approche plus cohérente, qui attribue un rôle central à Europol. À cet égard, la communication invite les États membres à utiliser, pour les échanges lorsque le canal n'est pas défini par une exigence juridique, le canal Europol comme canal par défaut, par l'intermédiaire de l'outil SIENA, à moins que des raisons particulières n'exigent d'en utiliser un autre.

28. Le CEPD reconnaît la nécessité d'une approche cohérente et harmonisée concernant le choix des canaux. Toutefois, pour ce qui est de l'utilisation de l'un des canaux comme canal par défaut, il rappelle le principe de la limitation des

[26] Voir à ce sujet l'annonce de la Commission du 9 avril 2013: «Mise en service de SIS II»: http://ec.europa.eu/dgs/home-affairs/what-is-new/news/news/2013/20130409_01_en.htm

finalités, qui est un principe fondamental en matière de protection des données. Comme la communication le souligne, il existe une diversité d'instruments, de canaux et d'outils, chacun étant conçu à des fins particulières. L'utilisation d'un canal conçu à des fins particulières ne doit pas donner lieu à l'éventuelle utilisation ou collecte de données passant par ce canal à d'autres fins. Cela présente le risque de ce qui est souvent décrit comme un «détournement d'usage», c'est-à-dire un élargissement progressif de l'utilisation d'un système ou d'une base de données qui va au-delà de l'objet pour lequel il a été prévu au départ. En outre, l'utilisation d'un canal a également des effets directs sur les responsabilités en termes de protection des données et de sécurité de l'autorité/agence qui gère le canal. Le CEPD déplore que la communication ne souligne pas ces conséquences et recommande que les orientations que le Conseil est invité à donner prennent en compte ces perspectives.

29. Enfin, le CEPD attire l'attention sur le fait que les mécanismes conçus pour l'échange d'informations à des fins spécifiques ne sont pas nécessairement adaptés à d'autres fins. L'outil de communication SIENA développé par Europol a été adapté à l'échange spécifique d'informations entre les autorités compétentes des États membres et les tiers aux fins de coopération policière. Ainsi, les fonctionnalités spécifiques de SIENA ont été développées et mises en œuvre sur la base des besoins définis lors de la création de cet outil. Ces fonctionnalités exigent, entre autres choses, que les utilisateurs entrent certains types et certaines quantités d'informations. Le CEPD signale que les fonctionnalités de SIENA ne sont pas nécessairement appropriées pour l'échange d'informations dans un contexte différent et à d'autres fins. Par conséquent, en l'espèce, il encourage la Commission à justifier plus clairement le choix de ce canal et à évaluer la conformité de ce choix au principe de respect de la vie privée dès la conception.

Gestion des canaux - PCU

30. La communication invite les États membres à créer – ou à utiliser s'il existe déjà - un point de contact unique (PCU) comme un «guichet unique» pour la coopération internationale couvrant tous les principaux canaux, disponible 24 heures sur 24 et 7 jours sur 7, regroupant toutes les autorités répressives avec un accès à toutes les bases de données nationales pertinentes. Étant donné l'existence de différentes unités s'occupant de parties différentes de coopération policière au niveau national, le CEPD estime que l'accessibilité par l'intermédiaire d'un point de contact unique aidera le pays requérant puisqu'il n'aura pas à s'adresser à différentes autorités et contacts dans le pays sollicité.

31. La création de PCU peut présenter des avantages puisqu'elle facilite une vue d'ensemble du flux d'informations transfrontalier et permet un enregistrement supplémentaire des acteurs directement impliqués. Toutefois, la création de PCU doit prendre en compte les implications en matière de protection des données. Toutes les bases de données ont été créées à des fins bien définies et sont soumises à des règles spécifiques. Une base de données peut n'être accessible que par le personnel dûment habilité dans le cadre de l'exécution des tâches qui lui incombent et aux fins pour lesquelles la base de données a été créée. Par conséquent, la composition et les modalités des PCU doivent être analysées

attentivement et définies afin de garantir le respect des règles applicables à chaque base de données.

32. En l'absence de conditions harmonisées pour les PCU, il pourrait arriver que des entités représentées dans les PCU ne soient pas autorisées à accéder directement à la base de données mais facilitent l'accès et assurent la communication des informations demandées à l'autorité sollicitée d'un autre État membre. Le CEPD note que la communication spécifie que les PCU doivent avoir un accès direct aux bases de données nationales si la loi l'autorise. Le CEPD note avec satisfaction que la communication rappelle que les informations ne peuvent être effectivement échangées et utilisées que si la loi le permet, ce qui suppose de respecter les règles relatives à la protection des données. Toutefois, il invite la Commission à commencer à travailler sur l'harmonisation des conditions pour les PCU, afin de garantir que les exigences soient les mêmes dans tous les États membres et qu'elles protègent efficacement les personnes physiques.

Garantir la qualité, la sécurité et la protection des données

33. En ce qui concerne l'interopérabilité entre les différents systèmes nationaux et structures administratives dont il est question dans la communication, le CEPD souligne la nécessité de considérer la protection des données à caractère personnel comme une partie intégrante de l'établissement - ou de l'amélioration - de l'interopérabilité des systèmes correspondants.

34. Comme cela a déjà été souligné dans des observations et avis précédents[27], rendre techniquement possible l'accès à des données ou leur échange constitue, dans de nombreux cas, une puissante incitation à y accéder ou à les échanger de facto. Bien que l'introduction de l'interopérabilité ne donne pas lieu à la création de nouvelles bases de données, elle introduira nécessairement une nouvelle utilisation des bases de données existantes en fournissant de nouvelles possibilités d'accéder à ces bases de données.

35. À cet égard, le CEPD aimerait attirer l'attention sur le principe de base en matière de protection des données de la limitation des finalités, lequel exige que les données à caractère personnel ne peuvent pas être utilisées à des fins qui ne sont pas compatibles avec l'objet pour lequel les données ont été initialement collectées, à moins que cela ne soit spécifiquement permis dans certaines conditions strictes.

[27] Voir l'avis du CEPD du 26 février 2006 relatif à l'échange d'informations en vertu du principe de disponibilité; les observations du CEPD du 10 mars 2006 relatives à la communication de la Commission du 24 novembre 2005 sur le renforcement de l'efficacité et de l'interopérabilité des bases de données européennes dans le domaine de la justice et des affaires intérieures et sur la création de synergies entre ces bases, et l'avis du CEPD du 7 décembre 2009 sur l'agence pour les systèmes d'information à grande échelle.

Amélioration de la formation et de la sensibilisation

36. La communication se réfère à la préparation par la Commission d'un programme européen de formation des services répressifs qui comprendra une formation sur l'échange transfrontalier d'informations. Le CEPD note l'adoption récente de la communication de la Commission mettant en place un programme européen de formation des services répressifs[28] sur lequel il reviendra dans ses avis concernant la proposition de règlement relatif à Europol[29]. Considérant que, dans nombre de cas, l'échange transfrontalier d'informations impliquera des données à caractère personnel, le CEPD aimerait attirer l'attention sur la nécessité d'inclure des formations sur la sécurité de l'information et la protection des données dans le programme envisagé par la Commission ainsi que dans les formations que les États membres sont invités à assurer.

3. CONCLUSIONS

37. Le CEPD apprécie l'attention généralement portée à la protection des données dans la communication, qui souligne la nécessité de garantir un niveau élevé de qualité, de sécurité et de protection des données, et rappelle que, quelle que soit la combinaison ou la séquence utilisée pour échanger des informations, les règles sur la protection, la sécurité et la qualité des données ainsi que les fins pour lesquelles les instruments sont susceptibles d'être utilisés doivent être respectées.

38. En outre, le CEPD:

- se félicite de ce que la communication conclut qu'aucune nouvelle base de données dans le domaine de la répression ni aucun nouvel instrument d'échange d'informations n'est nécessaire à l'échelle de l'UE;

- souligne la nécessité d'un processus d'évaluation complet des instruments et initiatives dans le domaine de la justice et des affaires intérieures, dont le résultat doit déboucher sur une politique globale, intégrée et bien structurée de l'UE sur la gestion de l'information et de l'échange, et encourage la Commission à poursuivre l'évaluation des autres instruments existants;

- encourage la Commission à mener des réflexions sur i) l'efficacité des principes de protection des données compte tenu de l'évolution technologique, de l'évolution des systèmes d'information à grande échelle et de l'utilisation croissante des données collectées initialement à d'autres fins que la lutte contre la criminalité, ainsi que sur ii) les bénéfices pour la sécurité publique de la tendance actuelle à une surveillance généralisée, systématique et proactive des personnes non suspectes et son utilité réelle dans la lutte contre la criminalité; les résultats de ces réflexions doivent aboutir à une politique globale, intégrée et

[28] Communication du 27 mars 2013 de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions intitulée «Création d'un programme européen de formation des services répressifs», COM(2013) 172 final.
[29] Proposition du 27 mars 2013 de règlement du Parlement européen et du Conseil relatif à l'Agence de l'Union européenne pour la coopération et la formation des services répressifs (Europol) et abrogeant les décisions 2009/371/JAI et 2005/681/JAI, COM(2013) 173 final.

bien structurée de l'UE sur la gestion de l'information et de l'échange dans ce domaine;

- souligne que les discussions en cours sur la proposition de directive ne doivent pas empêcher la Commission de dresser un inventaire des problèmes et risques en matière de protection des données et des éventuelles améliorations dans le contexte juridique actuel, et recommande d'utiliser ces discussions, notamment en matière de distinction sur le traitement des données relatives à des personnes suspectes et celles relatives à des personnes non suspectes, pour poursuivre le développement du modèle européen en matière d'échange d'informations;

- souscrit totalement à la nécessité de réviser les instruments actuels pour les aligner sur la directive proposée et encourage la Commission à prendre des mesures dans ce sens;

- encourage la Commission à poursuivre l'évaluation des instruments actuels durant et après leur mise en œuvre complète;

- recommande que les orientations que le Conseil est invité à donner relativement au choix de canal tiennent compte des conséquences en termes de principe de limitation des finalités et de responsabilités;

- encourage la Commission à justifier plus clairement le choix du canal Europol par l'intermédiaire de l'outil SIENA comme canal par défaut et à déterminer si ce choix est conforme au principe de respect de la vie privée dès la conception;

- note avec satisfaction que la communication rappelle que l'information ne peut être effectivement échangée et utilisée que si la loi le permet, ce qui suppose de respecter les règles relatives à la protection des données, et invite la Commission à commencer à travailler sur l'harmonisation des conditions pour les PCU, pour garantir que les exigences soient les mêmes dans tous les États membres et qu'elles protègent efficacement les personnes physiques;

- recommande d'inclure des formations sur la sécurité de l'information et la protection des données dans le programme envisagé par la Commission ainsi que dans les formations que les États membres sont invités à assurer.

Fait à Bruxelles, le 29 avril 2013

(signé)

Peter HUSTINX
Contrôleur européen de la protection des données