Résumé de l'avis du contrôleur européen de la protection des données sur les propositions de deux règlements portant établissement d'un cadre pour l'interopérabilité des systèmes d'information à grande échelle de l'Union européenne

(Le texte complet de l'avis en anglais, français et allemand est disponible sur le site internet du CEPD www.edps.europa.eu)

(2018/C 233/07)

Les défis urgents qui se posent aujourd'hui en matière de sécurité et de gestion des frontières imposent d'utiliser plus intelligemment les informations dont disposent déjà les autorités publiques compétentes. Cela a incité la Commission européenne à lancer un processus devant déboucher sur l'interopérabilité des systèmes d'information à grande échelle de l'Union européenne (existants et futurs) dans les domaines de la migration, de l'asile et de la sécurité. En décembre 2017, la Commission a publié deux propositions de règlements visant à établir un cadre juridique pour l'interopérabilité des systèmes d'information à grande échelle de l'Union européenne.

L'interopérabilité, pour autant qu'elle soit mise en œuvre de manière réfléchie et dans le strict respect des droits fondamentaux, et notamment des droits au respect de la vie privée et à la protection des données, peut être un outil utile pour répondre aux besoins légitimes des autorités compétentes à l'aide des systèmes d'information à grande échelle et pour contribuer au développement d'un partage de l'information effectif et efficace. L'interopérabilité n'est pas seulement ou principalement un choix technique, mais plutôt un choix politique susceptible d'avoir des conséquences juridiques et sociétales profondes, qui ne peuvent pas être masquées derrière des changements prétendument techniques. La décision du législateur de l'Union européenne de rendre les systèmes d'information à grande échelle interopérables non seulement aurait une incidence profonde et durable sur leur structure et leur mode de fonctionnement, mais modifierait également la façon dont les principes juridiques ont été interprétés dans ce domaine jusqu'à présent, marquant ainsi un «point de non-retour».

Si l'interopérabilité a pu être envisagée dans un premier temps comme un outil ayant pour seul but de faciliter l'utilisation des systèmes, les propositions introduiraient de nouvelles possibilités d'accès et d'utilisation des données stockées dans les différents systèmes afin de lutter contre la fraude à l'identité, de faciliter les contrôles d'identité et de simplifier l'accès des services répressifs aux systèmes d'information à finalité non répressive.

En particulier, les propositions créent une nouvelle base de données centralisée qui contiendrait des informations sur des millions de ressortissants de pays tiers, y compris leurs données biométriques. En raison de l'ampleur de cette base de données et de la nature des données à stocker dans celle-ci, les conséquences d'une violation de données pourraient porter gravement atteinte à un nombre potentiellement très élevé d'individus. Si de telles informations venaient à tomber entre de mauvaises mains, la base de données pourrait devenir un outil dangereux contre les droits fondamentaux. Il est donc essentiel de mettre en place des garanties juridiques, techniques et organisationnelles solides. Une vigilance particulière s'impose également en ce qui concerne les finalités de la base de données ainsi que ses conditions et modalités d'utilisation.

Dans ce contexte, le CEPD souligne l'importance de clarifier davantage l'ampleur du problème de la fraude à l'identité parmi les ressortissants de pays tiers, afin de s'assurer que la mesure proposée est appropriée et proportionnée. La possibilité de consulter la base de données centralisée pour faciliter les contrôles d'identité sur le territoire des États membres devrait être formulée de manière plus précise.

Le CEPD reconnaît qu'il est nécessaire que les services répressifs aient à leur disposition les meilleurs outils possibles pour identifier rapidement les auteurs d'actes terroristes et d'autres infractions pénales graves. Cependant, faciliter l'accès des services répressifs aux systèmes à finalité non répressive (c'est-à-dire aux informations obtenues par les autorités pour des finalités autres que répressives), même de manière limitée, est loin d'être anodin du point de vue des droits fondamentaux. En effet, un accès systématique représenterait une violation grave du principe de limitation de la finalité. Le CEPD appelle donc à la mise en place de garanties réelles pour préserver les droits fondamentaux des ressortissants de pays tiers.

Enfin, le CEPD tient à rappeler que, tant sur le plan juridique que sur le plan technique, les propositions ajoutent à la complexité des systèmes existants et de ceux qui sont toujours en cours d'élaboration, avec des implications précises qu'il est difficile d'évaluer à ce stade. Cette complexité aura des répercussions non seulement sur la protection des données, mais aussi sur la gouvernance et la surveillance des systèmes. Les conséquences précises pour les droits et libertés, qui sont au cœur du projet de l'Union européenne, sont difficiles à évaluer pleinement à ce stade. Pour ces raisons, le CEPD appelle à un débat plus large sur le futur de l'échange d'informations au sein de l'Union européenne, sur sa gouvernance et sur les moyens de sauvegarder les droits fondamentaux dans ce contexte.

1. **INTRODUCTION**

1.1. **Contexte**

1. En avril 2016, la Commission a adopté une communication *sur des systèmes d'information plus robustes et plus intelligents au service des frontières et de la sécurité* ([1]), amorçant une discussion sur la façon dont les systèmes d'information au sein de l'Union européenne pouvaient améliorer la gestion des frontières et la sécurité interne.

2. En juin 2016, dans le cadre du suivi de cette communication, la Commission a créé un groupe d'experts de haut niveau sur les systèmes d'information et l'interopérabilité (le «HLEG»). Le HLEG a été chargé d'examiner les défis juridiques, techniques et opérationnels posés par la réalisation de l'interopérabilité des systèmes centraux de l'Union européenne en matière de frontières et de sécurité. ([2])

3. Le HLEG a tout d'abord présenté des recommandations dans son rapport intérimaire de décembre 2016 ([3]), puis dans son rapport final de mai 2017 ([4]). Le CEPD a été invité à participer aux travaux du HLEG et a émis une déclaration sur le concept d'interopérabilité dans le domaine de la migration, de l'asile et de la sécurité, qui a été consignée dans le rapport final du HLEG.

4. Sur la base de la communication de 2016 et des recommandations du HLEG, la Commission a proposé une nouvelle approche de la sécurité, des frontières et de la gestion des migrations, selon laquelle tous les systèmes d'information centralisés de l'Union européenne en la matière seraient interopérables ([5]). La Commission a annoncé son intention de poursuivre ses travaux en vue de la création d'un portail de recherche européen, d'un service partagé d'établissement de correspondances biométriques ainsi que d'un répertoire commun de données d'identité.

5. Le 8 juin 2017, le Conseil s'est félicité de la position de la Commission et de la voie à suivre qu'elle proposait afin d'atteindre, d'ici à 2020, l'interopérabilité des systèmes d'information ([6]). Le 27 juillet 2017, la Commission a lancé une consultation publique sur l'interopérabilité des systèmes d'information de l'Union européenne au service des frontières et de la sécurité ([7]). La consultation était accompagnée d'une analyse d'impact initiale.

6. Le 17 novembre 2017, à titre de contribution supplémentaire, le CEPD a publié un document de réflexion sur l'interopérabilité des systèmes d'information dans les domaines de la liberté, de la sécurité et de la justice ([8]). Dans ce document, il a reconnu que, lorsqu'elle est mise en œuvre de manière réfléchie et dans le respect des exigences fondamentales de nécessité et de proportionnalité, l'interopérabilité peut être un outil utile pour répondre aux besoins légitimes des autorités compétentes à l'aide de systèmes d'information à grande échelle, y compris pour améliorer le partage de l'information.

7. Le 12 décembre 2017, la Commission a publié deux propositions législatives (les «propositions»):

   — de règlement du Parlement européen et du Conseil portant établissement d'un cadre pour l'interopérabilité des systèmes d'information de l'Union européenne (frontières et visas) et modifiant la décision 2004/512/CE du Conseil, le règlement (CE) n° 767/2008, la décision 2008/633/JAI du Conseil, le règlement (UE) 2016/399 et le règlement (UE) 2017/2226 (ci-après la «proposition sur les frontières et visas»),

   — de règlement du Parlement européen et du Conseil portant établissement d'un cadre pour l'interopérabilité des systèmes d'information de l'Union européenne (coopération policière et judiciaire, asile et migration) (ci-après la «proposition sur la coopération policière et judiciaire, l'asile et la migration»).

([1]) Communication de la Commission au Parlement européen et au Conseil sur des systèmes d'information plus robustes et plus intelligents au service des frontières et de la sécurité, 6.4.2016, COM(2016) 205 final.
([2]) Ibidem, p. 15.
([3]) Rapport intérimaire du président du groupe d'experts de haut niveau sur les systèmes d'information et l'interopérabilité institué par la Commission européenne, rapport intérimaire du président du groupe d'experts de haut niveau, décembre 2016, consultable à l'adresse suivante: http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3435
([4]) Rapport final du groupe d'experts de haut niveau sur les systèmes d'information et l'interopérabilité institué par la Commission européenne, 11 mai 2017, consultable à l'adresse suivante: http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3435
([5]) Communication du 16.5.2017 de la Commission au Parlement européen, au Conseil européen et au Conseil, septième rapport sur les progrès accomplis dans la mise en place d'une union de la sécurité réelle et effective, COM(2017) 261 final.
([6]) Conclusions du Conseil sur la voie à suivre pour améliorer l'échange d'informations et assurer l'interopérabilité des systèmes d'information de l'Union européenne, 8 juin 2017: http://data.consilium.europa.eu/doc/document/ST-10151-2017-INIT/fr/pdf
([7]) La consultation publique et l'analyse d'impact sont consultables à l'adresse suivante: https://ec.europa.eu/home-affairs/content/consultation-interoperability-eu-information-systems-borders-and-security_en
([8]) https://edps.europa.eu/sites/edp/files/publication/17-11-16_opinion_interoperability_en.pdf

1.2. **Objectifs des propositions**

8. Les propositions visent en général à améliorer la gestion des frontières extérieures de l'espace Schengen et à contribuer à la sécurité intérieure de l'Union européenne. À cet effet, elles créent un cadre visant à garantir l'interopérabilité entre les systèmes d'information à grande échelle de l'Union européenne, existants et futurs, dans les domaines des contrôles aux frontières, de l'asile et de l'immigration, ainsi que de la coopération policière et judiciaire en matière pénale.

9. Les éléments d'interopérabilité établis par les propositions couvriraient les systèmes suivants:

— les trois systèmes existants: le système d'information Schengen (SIS), le système Eurodac et le système d'information sur les visas (VIS),

— trois systèmes proposés qui sont toujours en cours d'élaboration ou de développement:

— un système qui a été récemment approuvé par les législateurs de l'Union européenne et qui doit encore être développé: le système d'entrée/de sortie (EES) ([1]), et

— deux systèmes qui sont toujours en cours de négociation: la proposition de système européen d'information et d'autorisation concernant les voyages (ETIAS) ([2]), et la proposition de système européen d'information sur les casiers judiciaires pour les ressortissants de pays tiers (ECRIS-TCN) ([3]),

— la base de données d'Interpol sur les documents de voyage volés et perdus (SLTD) et

— les données d'Europol. ([4])

10. L'interopérabilité entre ces systèmes s'articule autour de quatre éléments:

— un portail de recherche européen («ESP»),

— un service partagé d'établissement de correspondances biométriques («BMS partagé»),

— un répertoire commun de données d'identité («CIR»), et

— un détecteur d'identités multiples («MID»).

11. L'ESP ferait office de courtier de messages. Il a pour objet de fournir une interface simple qui donnerait des résultats de recherche rapidement et de manière transparente. Il permettrait d'interroger simultanément les différents systèmes utilisant des données d'identité (biographiques et biométriques). En d'autres termes, plutôt que d'interroger chaque système séparément, l'utilisateur final pourrait interroger tous les systèmes auxquels il est autorisé à accéder en une seule recherche.

12. Le BMS partagé serait un outil technique facilitant l'identification d'une personne pouvant être enregistrée dans différentes bases de données. Il stockerait des modèles des données biométriques (empreintes digitales et images faciales) contenues dans les systèmes d'information centralisés de l'Union européenne (c'est-à-dire le SIS, le système Eurodac, l'EES, le VIS et l'ECRIS-TCN). Il permettrait, d'une part, de rechercher simultanément des données biométriques stockées dans les différents systèmes et, d'autre part, de comparer ces données.

13. Le CIR faciliterait l'identification des personnes, y compris sur le territoire des États membres, et contribuerait également à simplifier l'accès des services répressifs aux systèmes d'information à finalité non répressive. Le CIR stockerait des données biographiques et biométriques enregistrées dans le VIS, l'ECRIS-TCN, l'EES, le système Eurodac et l'ETIAS. Il stockerait les données (séparées logiquement) en fonction du système dont elles proviennent.

([1]) règlement (UE) 2017/2226 du Parlement européen et du Conseil du 30 novembre 2017 portant création d'un système d'entrée/de sortie (EES) pour enregistrer les données relatives aux entrées, aux sorties et aux refus d'entrée concernant les ressortissants de pays tiers qui franchissent les frontières extérieures des États membres et portant détermination des conditions d'accès à l'EES à des fins répressives, et modifiant la convention d'application de l'accord de Schengen et les règlements (CE) nº 767/2008 et (UE) nº 1077/2011 (JO L 327 du 9.12.2017, p. 20).

([2]) Proposition de règlement du Parlement européen et du Conseil portant création d'un système européen d'information et d'autorisation concernant les voyages (ETIAS) et modifiant les règlements (UE) nº 515/2014, (UE) 2016/399, (UE) 2016/794 et (UE) 2016/1624, COM(2016) 731 final, 16.11.2016.

([3]) Proposition de règlement du Parlement européen et du Conseil portant création d'un système centralisé permettant d'identifier les États membres détenant des informations relatives aux condamnations concernant des ressortissants de pays tiers et des apatrides, qui vise à compléter et à soutenir le système européen d'information sur les casiers judiciaires (système ECRIS-TCN), et modifiant le règlement (UE) nº 1077/2011, COM(2017) 344 final, 29.6.2017.

([4]) Règlement (UE) 2016/794 du Parlement européen et du Conseil du 11 mai 2016 relatif à l'Agence de l'Union européenne pour la coopération des services répressifs (Europol) et remplaçant et abrogeant les décisions du Conseil 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI et 2009/968/JAI (JO L 135 du 24.5.2016, p. 53).

14. Le MID constituerait un outil qui permettrait de relier des identités au sein du CIR et du SIS et qui stockerait les liens entre les fiches. Il stockerait des liens fournissant des informations lorsqu'une ou plusieurs correspondance(s) confirmée(s) ou éventuelle(s) est (sont) détectée(s) et/ou lorsqu'une identité frauduleuse est utilisée. Il vérifierait si les données recherchées ou introduites existent dans plus d'un des systèmes pour détecter des identités multiples (par exemple, des données biométriques identiques liées à des données biographiques différentes ou des données biographiques identiques/similaires liées à des données biométriques différentes). Le MID montrerait les fiches d'identité biographique ayant un lien dans les différents systèmes.

15. Grâce aux quatre éléments d'interopérabilité, les propositions visent à:

— garantir que les utilisateurs autorisés disposent d'un accès rapide, continu, systématique et contrôlé aux systèmes d'information pertinents,

— faciliter les contrôles d'identité des ressortissants de pays tiers effectués sur le territoire des États membres,

— détecter les identités multiples liées à un même ensemble de données, et

— simplifier l'accès des services répressifs aux systèmes d'information à finalité non répressive.

16. En outre, les propositions établiraient un répertoire central des rapports et statistiques («CRRS»), le format universel pour les messages («UMF»), et elles instaureraient des mécanismes automatisés de contrôle de la qualité des données.

17. La publication de deux propositions législatives au lieu d'une seule résulte de la nécessité de respecter la distinction entre les systèmes qui concernent:

— l'acquis de Schengen en matière de frontières et de visas [c'est-à-dire le VIS, l'EES, l'ETIAS et le SIS tel que régi par le règlement (CE) nº 1987/2006],

— l'acquis de Schengen en matière de coopération policière ou les systèmes qui ne sont pas liés à l'acquis de Schengen (le système Eurodac, l'ECRIS-TCN et le SIS tel que régi par la décision du Conseil 2007/533/JAI).

18. Les deux propositions sont des «propositions complémentaires» qui doivent être lues conjointement. La numérotation des articles est essentiellement similaire dans les deux propositions, tout comme l'est leur contenu. Par conséquent, sauf indication contraire, lorsqu'un article spécifique est mentionné, cet article fait référence à celui des deux propositions.

5. **CONCLUSIONS**

142. Le CEPD reconnaît que, lorsqu'elle est mise en œuvre de manière réfléchie et dans le strict respect des exigences fondamentales de nécessité et de proportionnalité, l'interopérabilité peut être un outil utile pour répondre aux besoins légitimes des autorités compétentes à l'aide de systèmes d'information à grande échelle, y compris pour améliorer le partage de l'information.

143. Il souligne que l'interopérabilité n'est pas essentiellement un choix technique, c'est avant tout un choix politique à faire, qui aura des implications juridiques et sociétales importantes dans les années à venir. Dans le contexte d'une tendance claire consistant à mélanger des objectifs législatifs et politiques communautaires distincts (c'est-à-dire contrôles aux frontières, asile et immigration, coopération policière et, désormais aussi, judiciaire en matière pénale), ainsi qu'à assurer aux services répressifs un accès systématique aux bases de données à finalité non répressive, la décision du législateur de l'Union européenne de rendre les systèmes informatiques à grande échelle interopérables aurait non seulement une incidence profonde et durable sur leur structure et leur mode de fonctionnement, mais modifierait également la façon dont les principes juridiques ont été interprétés dans ce domaine jusqu'à présent, marquant ainsi un «point de non-retour». Pour ces raisons, le CEPD appelle à un débat plus large sur l'avenir de l'échange d'informations au sein de l'Union européenne, sur sa gouvernance et sur les moyens de sauvegarder les droits fondamentaux dans ce contexte.

144. Bien que les propositions telles qu'elles sont présentées puissent donner l'impression que l'interopérabilité est l'élément final de systèmes d'information déjà pleinement opérationnels (ou, tout au moins, de systèmes dont les actes juridiques fondateurs sont déjà «stables» et en phase finale du processus législatif), le CEPD tient à rappeler que ce n'est pas le cas. En réalité, trois des six systèmes d'information de l'Union européenne que les propositions cherchent à interconnecter n'existent pas à l'heure actuelle (ETIAS, ECRIS-TCN et EES), deux sont en cours de révision (SIS et Eurodac) et un doit être révisé plus tard cette année (VIS). Il est impossible d'évaluer les implications précises, pour le respect de la vie privée et la protection des données, d'un système extrêmement complexe qui compte autant d'«éléments mobiles». Le CEPD rappelle l'importance de garantir une cohérence entre les textes juridiques qui sont déjà en cours de négociation (ou à venir) et les propositions, afin de créer un environnement juridique, organisationnel et technique unifié pour l'ensemble des activités de traitement de données au sein de l'Union. Dans ce contexte, il tient à souligner que le présent avis est sans préjudice d'autres interventions qui pourraient se produire au fur et à mesure que les différents instruments juridiques interconnectés passent par les différentes étapes du processus législatif.

145. Le CEPD relève que si l'interopérabilité a pu être envisagée dans un premier temps comme un outil ayant pour seul but de faciliter l'utilisation des systèmes, les propositions introduisent de nouvelles possibilités d'accès et d'utilisation des données stockées dans les différents systèmes afin de lutter contre la fraude à l'identité, de faciliter les contrôles d'identité et de simplifier l'accès des services répressifs aux systèmes d'information à finalité non répressive.

146. Comme il l'a déjà souligné dans son document de réflexion, le CEPD souligne l'importance, tout d'abord, de clarifier davantage l'ampleur du problème de la fraude à l'identité parmi les ressortissants de pays tiers, afin de s'assurer que la mesure proposée est appropriée et proportionnée.

147. En ce qui concerne l'utilisation des données stockées dans les différents systèmes pour faciliter les contrôles d'identité sur le territoire des États membres, le CEPD souligne que les objectifs d'une telle utilisation, à savoir combattre la migration irrégulière et favoriser un niveau élevé de sécurité, sont formulés de façon trop générale et devraient être «strictement limités» et «définis avec précision» dans les propositions, afin de se conformer à la jurisprudence de la Cour de justice de l'Union européenne. Il estime en particulier que l'accès au CIR pour établir l'identité d'un ressortissant d'un pays tiers afin de garantir un niveau élevé de sécurité ne devrait être autorisé que s'il est possible d'accéder à des bases de données nationales similaires (par exemple un registre de ressortissants/résidents) pour les mêmes finalités et dans les mêmes conditions. Il recommande de clarifier ce point dans les propositions. Dans le cas contraire, les propositions sembleraient établir une présomption selon laquelle les ressortissants de pays tiers constituent par définition une menace pour la sécurité. Il recommande également de veiller à ce que l'accès aux données permettant d'identifier une personne lors d'un contrôle d'identité soit autorisé:

— en principe, en présence de la personne et

— lorsqu'elle n'est pas en mesure de coopérer et n'est pas en possession d'un document établissant son identité, ou

— lorsqu'elle refuse de coopérer, ou

lorsqu'il existe des motifs justifiés ou fondés de croire que les documents présentés sont faux ou que la personne ne dit pas la vérité sur son identité.

148. Le CEPD reconnaît qu'il est nécessaire que les services répressifs aient à leur disposition les meilleurs outils possibles pour identifier rapidement les auteurs d'actes terroristes et autres infractions pénales graves. Toutefois, il serait inacceptable de supprimer des garanties réelles, qui ont été introduites pour préserver les droits fondamentaux, dans le but principal d'accélérer une procédure. Dès lors, il recommande d'ajouter à l'article 22, paragraphe 1, des propositions les conditions relatives à l'existence de motifs raisonnables, à la réalisation d'une recherche préalable dans les bases de données nationales et au lancement d'une interrogation du système automatisé d'identification des empreintes digitales des autres États membres en vertu de la décision 2008/615/JAI, avant toute recherche dans le répertoire commun de données d'identité. En outre, il considère que le respect des conditions d'accès à des informations même limitées (comme une concordance/non-concordance) devrait toujours être vérifié, indépendamment de tout accès ultérieur aux données stockées dans le système ayant déclenché le résultat positif.

149. Le CEPD estime que la nécessité et la proportionnalité de l'utilisation des données stockées dans l'ECRIS-TCN pour détecter les identités multiples et pour faciliter les contrôles d'identité devraient être démontrées plus clairement, et qu'il convient également de clarifier sa compatibilité avec le principe de limitation de la finalité. Il recommande donc de veiller, dans les propositions, à ce que les données stockées dans l'ECRIS-TCN puissent être consultées et utilisées uniquement aux fins de l'ECRIS-TCN, telles qu'elles sont définies dans l'instrument juridique y afférent.

150. Le CEPD se félicite du fait que les propositions visent à créer un environnement technique harmonisé de systèmes qui fonctionneront ensemble pour fournir un accès rapide, continu, contrôlé et systématique aux informations dont les différentes parties prenantes ont besoin pour accomplir leurs missions. Il rappelle que les principes fondamentaux de protection des données devraient être pris en compte à tous les stades de la mise en œuvre des propositions, et recommande donc d'inclure dans les propositions l'obligation pour l'eu-LISA et les États membres de suivre les principes de protection des données dès la conception et par défaut.

151. Au-delà des observations générales et des questions clés identifiées ci-dessus, le CEPD formule des recommandations supplémentaires concernant les aspects suivants des propositions:

— la fonctionnalité de l'ESP, du BMS partagé, du CIR et du MID,

— les périodes de conservation des données dans le CIR et le MID,

— la vérification manuelle des liens,

— le répertoire central des rapports et statistiques,

— la répartition des rôles et des responsabilités entre l'eu-LISA et les États membres,

— la sécurité des éléments d'interopérabilité,

— les droits des personnes concernées,

— l'accès du personnel de l'eu-LISA,

— la période de transition,

— les registres et

— le rôle des autorités de contrôle nationales et du CEPD.

152. Le CEPD reste disponible pour apporter des conseils supplémentaires concernant les propositions, ainsi que tout acte délégué ou d'exécution adopté portant sur les règlements proposés qui serait susceptible d'avoir une incidence sur le traitement de données à caractère personnel.

Bruxelles, le 19 mars 2018.

Giovanni BUTTARELLI

Contrôleur européen de la protection des données