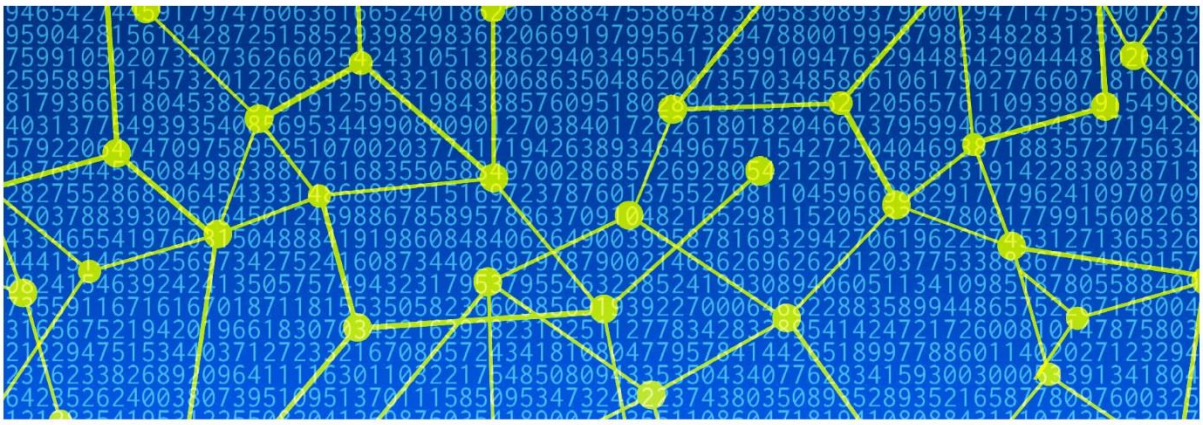

EUROPEAN DATA PROTECTION SUPERVISOR

Avis 4/2018 sur les propositions de deux règlements portant établissement d'un cadre pour l'interopérabilité des systèmes d'information à grande échelle de l'UE

EDPS

16 avril 2018

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, «En 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'adopter une approche constructive et proactive. 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 conseiller les institutions de l'UE sur les implications de leurs politiques en matière de protection des données et de promouvoir une élaboration responsable des politiques, conformément à l'action nº 9 de la stratégie du CEPD: «Faciliter l'élaboration responsable et éclairée de politiques». Il fait suite au document de réflexion publié par le CEPD le 17 novembre 2017. Le CEPD considère que le respect des exigences en matière de protection des données est essentiel pour une interopérabilité réussie des systèmes d'information à grande échelle de l'UE au sein de l'espace de liberté, de sécurité et de justice.

Synthèse

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'UE (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'UE.

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'UE 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'UE, 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'UE, sur sa gouvernance et sur les moyens de sauvegarder les droits fondamentaux dans ce contexte.

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[1], et vu le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (le «règlement général sur la protection des données»)[2],

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[3], et notamment son article 28, paragraphe 2, son article 41, paragraphe 2, et son article 46, point d),

vu la décision-cadre du Conseil 2008/977/JAI, du 27 novembre 2008, sur la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale[4], et vu la directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 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, et abrogeant la décision-cadre 2008/977/JAI du Conseil[5],

A ADOPTÉ L'AVIS SUIVANT:

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,*[6] 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'UE en matière de frontières et de sécurité.[7]

3 Le HLEG a tout d'abord présenté des recommandations dans son rapport intérimaire de décembre 2016[8], puis dans son rapport final de mai 2017[9]. 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'UE en la matière seraient interopérables[10]. 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[11]. Le 27 juillet 2017, la Commission a lancé une consultation publique sur l'interopérabilité des systèmes d'information de l'UE au service des frontières et de la sécurité[12]. 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[13]. 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'UE (frontières et visas) et modifiant la décision 2004/512/CE du Conseil, le règlement (CE) nº 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'UE (coopération policière et judiciaire, asile et migration) (ci-après la «proposition sur la coopération policière et judiciaire, l'asile et la migration»).

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'UE, 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'UE et qui doit encore être développé: le système d'entrée/de sortie (EES)[14] et
- deux systèmes qui sont toujours en cours de négociation: la proposition de système européen d'information et d'autorisation concernant les voyages (ETIAS)[15], et la proposition de système européen d'information sur les casiers judiciaires pour les ressortissants de pays tiers (ECRIS-TCN)[16];

- la base de données d'Interpol sur les documents de voyage volés et perdus (SLTD) et
- les données d'Europol.[17]

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'UE (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.

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.

2 Observations générales

19 Les défis urgents qui se posent aujourd'hui en matière de sécurité et de gestion des frontières imposent d'utiliser plus intelligemment les informations qui sont déjà à la disposition des autorités. Lorsqu'elle est mise en œuvre de manière réfléchie, l'interopérabilité peut contribuer au développement d'un partage de l'information effectif et efficace. Dans ce contexte, le CEPD a soutenu l'initiative de la Commission consistant à lancer la réflexion sur une vision stratégique globale sur la manière de rendre la gestion et l'utilisation des données plus effectives et plus efficaces dans le strict respect de la protection des données[18]. Il a reconnu que l'interopérabilité, lorsqu'elle est développée en pleine conformité avec les droits fondamentaux, peut être un outil utile pour répondre aux besoins légitimes des autorités compétentes à l'aide de systèmes d'information à grande échelle.

20 Le CEPD a observé, au cours des dernières années, une tendance croissante à aborder conjointement les objectifs de sécurité et de gestion des migrations. Parmi les exemples de cette tendance, on peut citer l'octroi de l'accès aux systèmes d'information sur les migrations existants à finalité répressive[19], la création de systèmes d'information de l'UE à double finalité[20], ou encore l'extension des mandats des agences de l'UE[21]. En instaurant l'interopérabilité entre les outils liés à la migration, la coopération policière et la coopération judiciaire, les propositions s'inscrivent dans cette tendance. Comme il l'a

déjà souligné dans son document de réflexion, le CEPD craint que les références répétées à la migration, à la sécurité intérieure et à la lutte contre le terrorisme, utilisées de manière quasiment interchangeable, risquent d'estomper les distinctions entre la gestion des flux migratoires et la lutte contre la criminalité et le terrorisme. Cela pourrait même contribuer à assimiler terroristes, criminels et étrangers.

21 En outre, il relève que si trois des six systèmes d'information de l'UE que les propositions visent 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).

22 Il est impossible d'évaluer les implications précises, pour le respect de la vie privée et la protection des données, d'un système doté d'autant d'«éléments mobiles». Les propositions ajoutent à la complexité, tant juridique que technique, des systèmes existants et de ceux qui sont encore en cours de développement. L'interopérabilité ainsi mise en œuvre donne lieu à une plus grande complexité plutôt qu'à une simplification. Bien que le CEPD comprenne les raisons qui sous-tendent les propositions, ajouter à la complexité pourrait aller à l'encontre de l'objectif même des propositions, tel qu'il est énoncé à leur article 2, paragraphe 2, point e), à savoir renforcer, simplifier et rendre plus uniformes les conditions de sécurité des données et de protection des données régissant les différents systèmes d'information de l'UE.

23 Cette complexité aura des implications non seulement pour la protection des données, mais aussi pour la gouvernance et la surveillance des systèmes. Dans ce contexte, le CEPD rappelle que les systèmes d'information à grande échelle de l'UE au sein de l'espace de liberté, de sécurité et de justice ont un impact considérable sur les droits fondamentaux des personnes, y compris leurs droits à la protection des données, et exigent donc une surveillance indépendante, efficace et forte. Dès lors, il met l'accent sur la nécessité de fournir aux autorités chargées de la protection des données, y compris le CEPD, les ressources financières et humaines supplémentaires nécessaires pour leur permettre de s'acquitter comme il convient de leur mission de surveillance.

24 Les propositions présentées donnent l'impression que l'interopérabilité est l'élément final de systèmes d'information déjà pleinement opérationnels (ou bénéficiant, tout au moins, d'instruments juridiques fondateurs stables selon le processus législatif). Or, comme mentionné ci-dessus, tel n'est pas le cas; il aurait été préférable, par souci de cohérence et au regard du processus démocratique, de présenter les propositions après l'adoption des différents instruments juridiques pendants ou, tout au moins, de présenter ensemble toutes les propositions législatives pertinentes en même temps. Il est important 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, le CEPD 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.

25 Le CEPD reconnaît qu'il est, aujourd'hui plus que jamais, nécessaire de mieux partager l'information et d'utiliser plus efficacement les systèmes d'information à grande échelle

de l'UE, afin de gérer les défis migratoires, d'un côté, et de lutter contre les problèmes de terrorisme et de criminalité, de l'autre. Toutefois, la nécessité de mieux exploiter les données ne devrait jamais donner lieu à la violation du droit fondamental à la protection des données. L'interopérabilité n'est pas essentiellement un choix technique, c'est avant tout un choix politique à faire. Dans le contexte d'une tendance claire qui consiste 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'UE 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'UE, sur sa gouvernance et sur les moyens de sauvegarder les droits fondamentaux dans ce contexte.

26 Enfin, le CEPD tient à rappeler que la protection des droits fondamentaux, y compris des droits au respect de la vie privée et à la protection des données, consacrés par la charte des droits fondamentaux de l'UE, n'est pas limitée aux seuls ressortissants de l'UE. L'UE et les États membres sont liés par celle-ci lorsqu'ils appliquent le droit de l'UE à une personne, qu'il s'agisse ou non d'un citoyen de l'UE, d'un ressortissant d'un pays tiers, d'un migrant (en situation irrégulière ou non) ou d'un demandeur d'asile. La charte doit servir de boussole pour toutes les politiques et législations de l'UE. Le CEPD est prêt à aider le législateur de l'UE à veiller à ce qu'il en soit ainsi.

3 Recommandations principales

3.1 Introduction

27 Comme il l'a déjà souligné dans son document de réflexion, le CEPD est d'avis que l'interopérabilité ne devrait pas être une fin en soi, mais qu'elle devrait toujours être mise au service d'un objectif d'intérêt général réel. Par conséquent, il se félicite du fait que les propositions énumèrent les objectifs d'intérêt général qu'elles poursuivent, ainsi que les objectifs plus spécifiques que l'interopérabilité vise à atteindre.

28 Il estime que l'interopérabilité, telle qu'elle est exposée dans les propositions, est plus que la somme de ses parties, dans la mesure où, en définitive, les éléments qui la composent contribuent ensemble à établir une base de données centrale des ressortissants de pays tiers, et en particulier un registre central des données biométriques des ressortissants de pays tiers. Contrairement aux bases de données décentralisées, une base de données centrale augmente implicitement le risque d'abus et suscite plus facilement le désir d'utiliser le système au-delà des finalités pour lesquelles il a été conçu à l'origine. Il convient donc d'examiner attentivement les propositions, en prêtant une attention particulière à l'existence de toutes les garanties nécessaires.

29 En particulier, les propositions introduisent de nouvelles utilisations des données déjà collectées dans d'autres systèmes et apportent des modifications aux droits et conditions actuels d'accès à ces données, ainsi qu'à l'architecture des systèmes. Elles supposent

donc de nouveaux traitements des données qui ne sont pas couverts par les bases juridiques existantes. Cela a un impact sur les droits fondamentaux au respect de la vie privée et à la protection des données qu'il convient d'évaluer soigneusement.

3.2 Utilisation des données pour de nouvelles finalités

30 Les propositions créent un CIR qui contiendra un dossier individuel pour chaque personne enregistrée dans au moins un des systèmes suivants: l'EES, le VIS, l'ETIAS, Eurodac et l'ECRIS-TCN. Le dossier individuel compilera les données enregistrées dans les différents systèmes concernant cette personne (à l'exception, pour des raisons techniques, de celles stockées dans le SIS). Ces données seront constituées de données biographiques (prénoms, noms, lieu et date de naissance, sexe, nationalité, titres de voyage) et de données biométriques (empreintes digitales et images faciales). Pour chaque ensemble de données, le CIR comportera une référence aux systèmes d'information auxquels appartiennent les données. Le BMS partagé et le MID permettront de recouper les données stockées dans le CIR ainsi que celles stockées dans le SIS.

31 À titre liminaire, le CEPD tient à souligner que le CIR stockera des données concernant tous les ressortissants de pays tiers qui ont franchi ou envisagent de franchir les frontières de l'UE (à quelques exceptions près), autrement dit des millions de personnes. Ces données incluent des données biométriques qui sont, par nature, très sensibles. En effet, à la différence des autres données à caractère personnel, les données biométriques ne sont ni communiquées par un tiers, ni choisies par la personne; elles sont immanentes à l'organisme lui-même et se réfèrent de façon distinctive et définitive à une personne. Par ailleurs, une base de données est d'autant plus vulnérable, convoitée et soumise à de multiples usages qu'elle est importante, reliée à des milliers de points d'accès et qu'elle stocke des données sensibles telles que des données biométriques.

32 En raison de l'ampleur d'une base de données centralisée et de la nature des données qui y sont stockées, les conséquences d'une violation de données concernant le CIR pourraient porter gravement atteinte à un nombre potentiellement élevé de personnes. Si ces données venaient à tomber entre les mauvaises mains, le CIR pourrait devenir un outil dangereux contre les droits fondamentaux s'il n'était pas entouré de garanties juridiques, techniques et organisationnelles strictes et suffisantes. Il est donc essentiel de faire preuve d'une vigilance particulière en ce qui concerne les finalités ainsi que les conditions et modalités d'utilisation du CIR.

33 Le CEPD tient à rappeler que si les systèmes qui alimenteront le CIR ont été développés pour appuyer la gestion des frontières et/ou la répression[22], chacun d'entre eux a été conçu pour une finalité bien précise (par exemple l'EES, pour identifier les personnes qui dépassent la durée de séjour autorisée, le système Eurodac, pour déterminer l'État membre responsable de l'examen d'une demande d'asile, etc.).

34 Le CEPD note que les propositions prévoient la possibilité d'utiliser les systèmes plus largement, c'est-à-dire d'étendre leur utilisation au-delà des finalités spécifiques pour lesquelles ils ont été établis. En particulier, les données stockées dans les différents systèmes seront rassemblées pour lutter contre la fraude à l'identité, mais aussi pour faciliter et permettre les contrôles d'identité sur le territoire des États membres.

3.2.1 Lutter contre la fraude à l'identité

35 L'un des principaux objectifs des propositions, selon leur analyse d'impact, est la lutte contre la fraude à l'identité. Le CEPD reconnaît que la lutte contre la fraude à l'identité est un objectif légitime d'intérêt général. Toutefois, comme cela a déjà été souligné ci-dessus, la solution proposée, c'est-à-dire la création d'une base de données contenant des informations relatives à des millions de ressortissants de pays tiers, y compris leurs données biométriques, semble très intrusive au regard des droits fondamentaux au respect de la vie privée et à la protection des données. Comme l'indique le considérant 38, les nouvelles opérations de traitement des données ayant pour but d'identifier correctement les personnes concernées constituent une atteinte aux droits fondamentaux protégés par les articles 7 et 8 de la charte. Par conséquent, elles doivent satisfaire aux critères de nécessité et de proportionnalité (article 52, paragraphe 1, de la charte).

36 Comme l'a rappelé le CEPD dans son document de réflexion, les problèmes auxquels les propositions visent à remédier doivent être suffisamment et clairement décrits et accompagnés de preuves. Le CEPD relève que l'analyse d'impact se contente de mentionner que les informations fournies par les systèmes de l'UE ne sont pas toujours complètes, exactes et fiables. Elle associe cela (sans autres explications) à l'absence de liens entre les données enregistrées dans les différents systèmes, ce qui rend très difficile la détection d'identité multiples ou la lutte contre la fraude à l'identité[23]. L'analyse d'impact se concentre sur le risque de fraude à l'identité et sur les difficultés à détecter les éventuelles fraudes, mais elle ne fournit pas la moindre explication ou estimation de l'ampleur du problème, pas plus qu'elle n'évoque les cas de fraude à l'identité auxquels les autorités compétentes sont confrontées. En l'absence d'autres indications sur l'existence de la fraude à l'identité, il est difficile de s'assurer que la mesure proposée est appropriée et proportionnée.

3.2.2 Faciliter l'identification d'une personne lors de contrôles d'identité (article 20)

37 L'article 20 des propositions dispose que l'autorité de police d'un État membre peut interroger le CIR à l'aide des données biométriques d'une personne relevées lors d'un contrôle d'identité, uniquement aux fins de l'identification de cette personne. Un tel accès doit être prévu par des mesures législatives nationales, qui indiqueront les finalités précises des contrôles d'identité dans le but de prévenir et de combattre la migration irrégulière et/ou de favoriser un niveau élevé de sécurité. Elles désigneront également les autorités de police compétentes et fixeront les procédures, les conditions et les critères relatifs aux contrôles.

38 Pour justifier la nécessité d'une telle utilisation, l'analyse d'impact souligne que, bien que les autorités des États membres tiennent des registres des ressortissants et des résidents de l'UE, elles ne peuvent pas tenir des registres complets des ressortissants de pays tiers présents pour un court séjour. En effet, ces derniers peuvent entrer dans différents États membres, voyager au sein de ceux-ci et les quitter. Le CIR pourrait combler cette lacune en autorisant les autorités des États membres à accéder au système Eurodac, au VIS, à l'EES, à l'ETIAS ainsi qu'à l'ECRIS-TCN, dans le but d'identifier les personnes présentes sur le territoire de l'UE et de permettre aux autorités de s'acquitter correctement et efficacement de leurs diverses missions et obligations.[24]

39 Le CEPD aimerait souligner une fois de plus que l'identification d'une personne n'est pas une fin en soi mais doit répondre à un objectif bien précis, par exemple, vérifier si la personne est recherchée par la police ou est habilitée à séjourner dans l'UE (si elle est en possession d'un visa en cours de validité, par exemple).

40 Il note que, conformément à l'article 20, l'identification de la personne doit contribuer à prévenir et combattre la migration irrégulière ou favoriser un niveau élevé de sécurité au sein de l'espace de liberté, de sécurité et de justice, y compris la préservation de la sécurité et de l'ordre publics et la sauvegarde de la sécurité sur les territoires des États membres. En d'autres termes, l'utilisation des données figurant dans le CIR pour identifier une personne serait autorisée lorsqu'elle est nécessaire pour combattre la migration irrégulière et favoriser un niveau élevé de sécurité.

41 Le CEPD met l'accent sur le fait que la formulation «combattre la migration irrégulière et favoriser un niveau élevé de sécurité» est une description très générale des finalités (par ailleurs légitimes). Il relève que l'article 20 prévoit l'adoption de mesures législatives nationales censées préciser ces finalités. Il tient néanmoins à rappeler que la Cour de justice de l'Union européenne («CJUE»), dans son arrêt Digital Rights Ireland, a considéré que la directive 2006/24 «*ne prévoit aucun critère objectif permettant de délimiter l'accès des autorités nationales compétentes aux données et leur utilisation ultérieure à des fins de prévention, de détection ou de poursuites pénales concernant des infractions*», se bornant à renvoyer «*de manière générale aux infractions graves telles qu'elles sont définies par chaque État membre dans son droit interne*[25]». La Cour a également considéré que l'accès et l'utilisation des données n'étaient pas «*strictement restreints à des fins de prévention et de détection d'infractions graves précisément délimitées ou de poursuites pénales afférentes à celles-ci*»[26].

42 **Le CEPD considère que les finalités consistant à combattre la migration irrégulière et favoriser un niveau élevé de sécurité, dans le contexte de l'article 20, sont trop générales et ne répondent pas aux exigences de finalités «*strictement restreintes*» et «*précisément délimitées*» dans les propositions, comme l'exige la Cour. Il recommande donc de les définir plus précisément dans les propositions.** Ainsi, par exemple, «migration irrégulière» pourrait renvoyer aux conditions d'entrée et de séjour telles qu'elles sont visées à l'article 6 du règlement (UE) 2016/399 du Parlement européen et du Conseil. En ce qui concerne la sécurité, le CEPD recommande de cibler les infractions pénales qui sont susceptibles en particulier de menacer un niveau élevé de sécurité, par exemple en renvoyant aux infractions pénales énumérées à l'article 2, paragraphe 2, de la décision-cadre 2002/584/JAI si elles sont passibles, en vertu du droit national, d'une peine ou d'une mesure de sûreté privatives de liberté pour une période maximale d'au moins trois ans.

43 S'agissant des conditions d'accès aux données stockées dans le CIR, le CEPD souligne que, dans son arrêt Digital Rights Ireland, la Cour a également critiqué le fait que la «*directive 2006/24 ne contient pas les conditions matérielles et procédurales relatives à l'accès des autorités nationales compétentes aux données et à leur utilisation ultérieure*», étant donné qu'«*elle se borne à prévoir que chaque État membre arrête la procédure à suivre et les conditions à remplir pour avoir accès aux données conservées dans le respect des exigences de nécessité et de proportionnalité*.»[27]

44 Le CEPD note que l'article 20 prévoit certains critères et conditions dans la mesure où il limite l'accès aux autorités de police et uniquement aux fins de l'identification d'une personne lors d'un contrôle d'identité. Toutefois, il considère que ces conditions devraient être définies plus précisément dans les propositions afin de satisfaire aux exigences de la Cour. **Le CEPD estime 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 des conditions équivalentes. Il recommande de clarifier ce point dans les propositions.** Dans le cas contraire, les propositions sembleraient clairement établir une présomption selon laquelle les ressortissants de pays tiers constituent par définition une menace pour la sécurité.

45 En outre, le CEPD souligne qu'un contrôle d'identité consiste généralement en ce qu'une autorité de police demande à des individus, dans le cadre des exigences légales définies dans le droit national, de prouver leur identité par tout moyen approprié, tel qu'une carte d'identité ou tout autre document en cours de validité.

46 Dans ce contexte, il relève que l'article 20, paragraphe 1, dispose que lorsque les données biométriques de la personne ne peuvent pas être utilisées ou lorsque la recherche effectuée avec ces données échoue, la recherche est effectuée à l'aide des données d'identité de cette personne, combinées aux données du document de voyage, ou à l'aide des données d'identité fournies par cette personne. Cela signifie que le contrôle d'identité serait d'abord effectué à l'aide des données biométriques puis, uniquement en cas d'échec, à l'aide d'autres données telles que les noms ou le document de voyage. D'après le CEPD, la consultation du CIR pour identifier une personne lors d'un contrôle d'identité ne devrait être effectuée sur la base des données biométriques qu'en dernier recours, c'est-à-dire:

- lorsque la personne n'est pas en mesure de coopérer (par exemple, elle ne comprend pas ce qu'on lui demande de présenter) et n'est pas en possession d'un document établissant son identité, ou
- lorsqu'elle refuse de coopérer, ou
- lorsqu'il existe des soupçons justifiés ou fondés que les documents sont faux ou que la personne ne dit pas la vérité sur son identité.

47 Le fait de relever systématiquement les données biométriques d'une personne lors d'un contrôle d'identité créerait le risque de stigmatiser certains individus (ou groupes d'individus) en raison de leur apparence et donnerait lieu à une différence de traitement injustifiée entre les citoyens de l'UE et les ressortissants de pays tiers.

48 **Par conséquent, le CEPD recommande de modifier l'article 20 de façon à ce qu'il dispose que l'accès au CIR sera 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 penser que les documents présentés sont faux ou que la personne ne dit pas la vérité sur son identité.**

3.2.3 Utilisation de l'ECRIS-TCN proposé

49 À titre liminaire, le CEPD tient à souligner que l'ECRIS-TCN n'existe pas encore. La proposition établissant l'ECRIS-TCN[28] est en cours d'examen par les législateurs de l'UE.

50 Le CEPD note que, conformément aux articles 17 et 18 de la proposition sur la coopération policière et judiciaire, l'asile et la migration, le CIR contiendrait les données suivantes stockées dans l'ECRIS-TCN: nom de famille; prénom(s); sexe; date de naissance; lieu et pays de naissance; nationalité(s); genre et, s'il y a lieu, nom et prénoms précédents, pseudonyme(s) et/ou nom(s) d'emprunt; image faciale; empreintes digitales, ainsi que la référence au numéro des données relatives aux empreintes digitales de la personne condamnée, y compris le code de l'État membre de condamnation. Par conséquent, il serait possible d'accéder à ces données et de les utiliser aux fins du CIR, à savoir la facilitation des contrôles d'identité et la détection d'identités multiples.

51 Le CEPD considère 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. L'argument selon lequel le CIR devrait contenir les données figurant dans le système ECRIS-TCN proposé au motif que les identités des ressortissants de pays tiers stockées dans ce système sont vérifiées par une autorité judiciaire[29] – et sont donc plus fiables – ne paraît pas suffisant pour satisfaire aux critères de nécessité et de proportionnalité visés à l'article 52, paragraphe 1, de la charte.

52 En outre, le CEPD rappelle que l'ECRIS-TCN vise à renforcer la coopération judiciaire en matière pénale en améliorant l'échange de l'information sur les casiers judiciaires dans l'ensemble de l'UE. L'article 22 de la proposition établissant l'ECRIS-TCN[30] dispose spécifiquement que les données contenues dans le système ne sont traitées qu'aux fins de l'identification de l'(des) État(s) membre(s) qui détien(nen)t l'information sur les casiers judiciaires des ressortissants de pays tiers. L'utilisation des données stockées dans l'ECRIS-TCN proposé pour détecter les identités multiples et faciliter les contrôles d'identité semble aller bien au-delà des finalités de l'ECRIS-TCN telles qu'elles sont définies dans l'instrument juridique proposé, et soulève la question de sa compatibilité avec le principe de limitation de la finalité.

53 **Le CEPD recommande donc de veiller à ce que les propositions n'autorisent l'accès aux données stockées dans l'ECRIS-TCN et leur utilisation que pour les finalités de l'ECRIS-TCN telles qu'elles sont définies dans l'acte juridique fondateur de ce système.**

3.3 Faciliter l'accès aux données à des fins répressives (article 22)

54 La possibilité d'utiliser les données d'identité enregistrées dans l'EES, le VIS, l'ETIAS ou le système Eurodac pour prévenir, détecter et enquêter sur les infractions terroristes et autres infractions pénales graves n'est pas nouvelle. Cette possibilité est prévue dans les instruments fondateurs (existants ou en cours de négociation) de ces systèmes. Toutefois, les propositions apportent des modifications significatives aux conditions d'accès à ces données prévues dans ces instruments.

55 Le CEPD a fait part à plusieurs reprises de ses inquiétudes au sujet de la tendance générale observée ces dernières années au sein de l'UE qui consistant à autoriser les services répressifs à accéder à des systèmes conçus pour des finalités autres que répressives. Lorsque la nécessité d'un tel accès est démontrée, le CEPD a insisté sur le fait que celui-ci ne devrait pas être accordé systématiquement, mais uniquement dans des circonstances particulières, au cas par cas et dans le respect de conditions strictes. Parmi ces conditions figure, notamment, le fait que les demandes d'accès aux données doivent être étroitement ciblées et fondées sur des suspicions portant sur des personnes en particulier.[31]

56 L'article 22 , paragraphe 1, des propositions dispose qu'aux fins de la prévention et de la détection des infractions terroristes ou d'autres infractions pénales graves, et des enquêtes en la matière, dans un cas particulier et pour savoir si des données sur une personne en particulier sont présentes dans l'EES, le VIS, l'ETIAS ou le système Eurodac, les autorités répressives et Europol peuvent consulter le CIR.

57 L'interrogation du CIR suivrait une approche de consultation en deux étapes: dans un premier temps, seule une référence indiquant un système («concordance/non-concordance») est fournie, l'accès complet n'étant accordé que dans un second temps. Si les données recherchées correspondent à des données enregistrées dans au moins l'un des systèmes, un indicateur de concordance apparaîtra indiquant quel est (sont) le(s) système(s) concerné(s). (Article 22, paragraphe 3, recherche de premier niveau). Toutefois, l'accès complet aux données resterait soumis aux conditions et procédures prévues dans les instruments législatifs respectifs régissant cet accès (article 22, paragraphe 4, recherche de deuxième niveau).

58 Le CEPD reconnaît qu'un «indicateur de concordance» est une information limitée. Cependant, contrairement à ce qu'affirme le considérant 33, un «indicateur de concordance» consiste en une information relative à une personne identifiée (ou identifiable) et constitue donc une donnée à caractère personnel. Comme il l'a déjà souligné dans son document de réflexion, le CEPD rappelle que l'existence (ou l'absence) d'un «résultat positif» doit toujours être considérée comme une donnée à caractère personnel. En effet, même avec le minimum absolu d'informations (par exemple, connu ou inconnu dans un système donné), une «concordance» ou «non-concordance» constitue une information relative à une personne (par exemple, la personne est ou n'est pas un demandeur d'asile). En conséquence, le traitement de ces données constitue une atteinte aux droits fondamentaux protégés par les articles 7 et 8 de la charte et doit respecter l'article 52, paragraphe 1, de la charte en termes de nécessité et de proportionnalité.

59 En ce qui concerne les différentes conditions d'accès et garanties régissant chaque système, l'exposé des motifs souligne que certaines des règles actuelles pourraient ralentir l'utilisation légitime des systèmes par les services répressifs. Grâce à la recherche de premier niveau, les propositions permettraient effectivement d'assouplir les conditions et les modalités de l'accès accordé aux services répressifs à des fins répressives.

60 Le CEPD souligne qu'à l'heure actuelle, tous les instruments fondateurs (existants et proposés) des systèmes concernés prévoient les conditions d'accès cumulatives suivantes:

- l'accès doit être nécessaire pour la prévention et la détection des infractions terroristes et autres infractions pénales graves, et les enquêtes à ce sujet,

- l'accès doit être nécessaire dans un cas particulier,
- il existe des motifs raisonnables de considérer que la consultation contribuera de manière substantielle à la prévention et à la détection des infractions pénales graves en question, ainsi qu'aux enquêtes en la matière.

Par ailleurs, les différents instruments exigent également la vérification, par une autorité indépendante, du respect des conditions d'accès précitées avant l'accès. Dans le cas de l'ETIAS, de l'EES et du système Eurodac, les services répressifs sont également tenus de consulter d'abord les autres systèmes pertinents (comme les bases de données nationales, les données d'Europol, Prüm, le VIS).

61 L'analyse d'impact dispose que ce «mécanisme en cascade» (c'est-à-dire l'obligation de vérification et de consultation préalables) crée une charge administrative considérable et se traduit par des retards ainsi que des occasions manquées de découvrir les informations nécessaires. Elle indique que le mécanisme en cascade oblige le service répressif à mettre fin à sa recherche une fois que l'information a été trouvée dans un système. Toutefois, cela ne signifie pas que le deuxième système dans la cascade, ou même les systèmes suivants, ne pourrait pas également contenir des informations utiles à des fins répressives[32].

62 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. Cependant, faciliter l'accès des services répressifs aux systèmes à finalité non répressive (même à des informations limitées comme une concordance/non-concordance) est loin d'être anodin du point de vue des droits fondamentaux. Il convient de ne pas perdre de vue que ces systèmes ont été mis en place et développés aux fins de l'application de politiques spécifiques et non comme un instrument de répression. Un accès systématique constituerait une violation du principe de limitation de la finalité. Il entraînerait une ingérence disproportionnée dans la vie privée, par exemple, de voyageurs qui ont accepté que leurs données fassent l'objet d'un traitement en vue d'obtenir un visa et qui s'attendent à ce que leurs données soient collectées, consultées et communiquées pour cette finalité. En outre, 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. S'il est nécessaire d'améliorer la procédure, cela ne devrait pas se faire au détriment des garanties.

63 Le CEPD relève qu'il ressort de l'article 22 des propositions que l'une des principales conditions d'accès aux systèmes n'est plus applicable, à savoir les motifs raisonnables de considérer que la consultation contribuera de manière substantielle à la prévention et à la détection des infractions terroristes ou autres infractions pénales graves, ainsi qu'aux enquêtes en la matière. Un motif raisonnable pourrait être, par exemple, un faux document de voyage retrouvé sur les lieux d'un crime. Le CEPD considère que l'obligation d'avoir des motifs raisonnables est une condition préalable fondamentale de tout accès des services répressifs à des systèmes à finalité non répressive. Il s'agit en effet d'une garantie essentielle contre les éventuelles «pêches aux informations» [*fishing expeditions*].

64 En outre, le CEPD n'est pas convaincu qu'une recherche préalable dans la base de données nationale soit un obstacle en soi. On peut raisonnablement penser que les

services répressifs vérifieront d'abord leurs propres bases de données nationales (pénales), auxquelles ils ont un accès direct. Si la personne est formellement identifiée comme un citoyen de l'UE, le CEPD considère qu'il n'y a pas lieu de procéder à une interrogation supplémentaire du CIR. La recherche préalable dans les bases de données nationales devrait demeurer une condition préalable à l'accès au CIR; de même, si les autres conditions sont remplies (c'est-à-dire, cas particulier, fins répressives et motifs raisonnables), elle ne s'opposerait pas nécessairement à un accès ultérieur au CIR.

65 Le CEPD se demande également pourquoi la consultation du système automatisé d'identification des empreintes digitales des autres États membres en vertu de la décision 2008/615/JAI (la «décision Prüm»)[33] ne s'appliquerait plus. Il rappelle qu'en vertu de la décision Prüm[34], il existe aujourd'hui un système répressif spécifique, qui vise à permettre l'échange d'informations policières, y compris de données relatives aux empreintes digitales, afin d'intensifier la coopération transfrontalière entre les autorités policières et judiciaires des États membres pour lutter contre le terrorisme et la criminalité transfrontalière. Les problèmes liés à l'efficacité de ce système, en raison (entre autres) de l'absence de mise en œuvre complète ou d'utilisation du système par les États membres, ne sauraient être considérés comme un motif valable pour faciliter l'accès des services répressifs aux systèmes à finalité non répressive. D'après le CEPD, la consultation d'autres systèmes en vertu de la décision Prüm devrait rester une condition d'accès au CIR et être effectuée au moins parallèlement à la consultation du CIR.

66 Par conséquent, le CEPD considère que l'accès au CIR pour détecter si les données relatives à une personne particulière sont présentes dans l'un des systèmes reliés au CIR (information sur la «concordance/non-concordance») ne devrait être autorisé que dans les conditions suivantes:

- aux fins de la prévention et de la détection des infractions terroristes et autres infractions pénales graves, et aux fins d'enquêtes en la matière,
- dans un cas particulier,
- lorsqu'il existe des motifs raisonnables de croire que la consultation contribuera de manière substantielle à la prévention et à la détection des infractions terroristes ou autres infractions pénales graves, ainsi qu'aux enquêtes en la matière; en particulier, lorsqu'il y a lieu de soupçonner que le suspect, l'auteur ou la victime d'une infraction terroriste ou autre infraction pénale grave appartient à la catégorie des ressortissants de pays tiers dont les données sont stockées dans l'EES, le VIS, l'ETIAS et le système Eurodac et,
- une recherche préalable dans les bases de données nationales a été effectuée et une interrogation du système automatisé d'identification des empreintes digitales des autres États membres en vertu de la décision 2008/615/JAI a été lancée.

67 Le CEPD considère que toutes ces conditions devraient être mentionnées dans l'article 22 des propositions. Il note que l'article 22, paragraphe 1, ne fait référence qu'aux conditions de finalité répressive et de cas particulier. **Par conséquent, il recommande d'ajouter à l'article 22, paragraphe 1, 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.** Le CEPD relève également que, conformément à l'article 22, paragraphe 4, en cas de «résultat positif», l'accès complet aux données contenues dans le

système reste soumis aux conditions et procédures prévues dans les instruments législatifs respectifs régissant cet accès.

68 Par ailleurs, étant donné qu'un «résultat positif» constitue une donnée à caractère personnel, le CEPD considère que le respect des conditions d'accès devrait toujours être vérifié, indépendamment de tout accès ultérieur aux données stockées dans le système ayant déclenché le résultat positif. **En d'autres termes, l'autorité répressive qui obtient un résultat positif devrait toujours en référer à l'autorité chargée de la vérification, laquelle s'assurera que les conditions d'accès au CIR ont été respectées. Si la vérification indépendante ex post détermine que la consultation du CIR n'était pas justifiée, l'autorité effacera toutes les données provenant du CIR. Nous recommandons de modifier l'article 22 des propositions en conséquence.**

3.4 Protection de la vie privée dès la conception et par défaut

69 Le CEPD se félicite de ce 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 souligne toutefois que les principes de protection des données devraient être pris en compte à tous les stades de la mise en œuvre des propositions.

70 À cet égard, le CEPD tient à attirer l'attention sur l'entrée en vigueur imminente du règlement 2016/679[35], et en particulier sur l'introduction du concept de protection des données dès la conception et par défaut en son article 25. Le CEPD rappelle que ce concept sera également introduit à l'article 27 du nouveau règlement (CE) 45/2001[36].

71 Ce concept impose à l'eu-LISA et aux États membres de mettre en œuvre des mesures techniques et organisationnelles appropriées pour garantir efficacement le respect des principes de protection des données et pour intégrer les garanties nécessaires afin de satisfaire aux exigences du RGPD et, en particulier, de protéger les droits des personnes concernées. En outre, l'eu-LISA et les États membres devraient veiller à ce que ne soient traitées par défaut que les données à caractère personnel qui sont nécessaires pour chaque finalité spécifique du traitement.

72 Le CEPD recommande d'inclure dans les propositions une référence à l'obligation incombant à l'eu-LISA et aux États membres de suivre les principes de protection des données dès la conception et par défaut.

4 Recommandations spécifiques

4.1 Référence à la législation applicable en matière de protection des données

73 À titre liminaire, le CEPD fait observer que certains articles des propositions renvoient à certaines dispositions de la législation applicable en matière de protection des données (à savoir le règlement 2016/679, la directive 2016/680 et le règlement 45/2001), par exemple les articles 46 et 47 des propositions. De l'avis du CEPD, ces dispositions visent à préciser davantage les articles correspondants des actes législatifs susmentionnés. Toutefois, afin d'indiquer clairement que ces références sont sans préjudice de l'application des autres dispositions pertinentes de ces actes législatifs, **le CEPD**

recommande de prévoir une disposition dans les propositions concernant l'applicabilité du règlement 2016/679, de la directive 2016/680 ainsi que du règlement 45/2001.

4.2 Profils d'utilisateur de l'ESP

74 Le CEPD se réjouit de ce que les propositions prévoient une gestion centralisée de la création des profils d'utilisateur, avec attribution des droits d'accès légaux. Toutefois, il souligne que **ces profils devraient être régulièrement réexaminés et, au besoin, mis à jour. Le CEPD recommande d'ajouter cette obligation au texte des propositions.**

75 L'article 7, paragraphe 4, des propositions définit quels organes de l'UE peuvent accéder à l'ESP. **Le CEPD recommande d'ajouter, après organes de l'UE, le texte suivant: «visés au paragraphe 1».**

76 L'article 8, paragraphe 1, des propositions dispose que chaque catégorie de profil d'utilisateur est liée à trois éléments: les champs de données à utiliser pour la recherche, les systèmes qui peuvent être consultés et les données qui peuvent être fournies dans chaque réponse. Le CEPD est d'avis que la finalité de la recherche est tout aussi importante. Or, elle n'est pas mentionnée dans l'article. Par conséquent, **le CEPD recommande d'ajouter également à l'article 8 des propositions une référence à la finalité de la recherche**.

4.3 Le BMS partagé - Catégories de données

77 Le CEPD considère que, conformément au considérant 17 des propositions, le BMS partagé a pour objet de regrouper et de stocker tous les modèles biométriques à un seul endroit, facilitant ainsi les comparaisons de données biométriques entre les systèmes afin de détecter les identités multiples, notamment via le CIR. Dans ce contexte, l'article 13 des propositions énumère toutes les données biométriques pertinentes qui devraient être stockées dans le BMS partagé.

78 En ce qui concerne le VIS, l'article 13, paragraphe 1, point b), des propositions dispose que le BMS partagé ne devrait conserver que le modèle biométrique issu des empreintes digitales des demandeurs VIS. Toutefois, l'article 18, paragraphe 1, point b), de la proposition sur les frontières et visas dispose également que la photographie du demandeur VIS devrait être stockée. Le CEPD estime que la photographie du demandeur VIS constitue une donnée biométrique pertinente aux termes de l'article 13, ce qui ajouterait une amélioration importante à la détection d'identités multiples. Par conséquent, **le CEPD se demande pourquoi la photographie du demandeur VIS n'est pas incluse dans l'article 13, paragraphe 1, point b), des propositions**.

79 En ce qui concerne le SIS, l'article 13, paragraphe 1, point c), des propositions renvoie à l'article 20, paragraphe 2, points w) et x), de la proposition de règlement sur le SIS II dans le domaine de la répression. Cependant, la définition de données dactylographiques figurant dans la proposition relative au SIS englobe également les empreintes palmaires. Le CEPD recommande de préciser dans les propositions que la référence aux données dactylographiques dans le SIS ne devrait inclure que les empreintes digitales et pas les empreintes palmaires. En outre, il constate que, dans le contexte de la proposition de règlement SIS dans le domaine de la répression, l'article 13, paragraphe 1, point d), des

propositions renvoie à l'article 20, paragraphe 3, points w) et x), de la proposition de règlement sur le SIS II dans le domaine de la répression. Le CEPD relève que l'article 20, paragraphe 3, point x), de la proposition de règlement dans le domaine de la répression fait explicitement référence aux données ADN. **Par conséquent, le CEPD recommande de modifier l'article 13, paragraphe 1, points c) et d), des propositions afin de s'assurer que ni les données ADN, ni les empreintes palmaires ne seront stockées dans le BMS partagé.**

80 **S'agissant de l'article 16, paragraphe 1, point d), des propositions, le CEPD recommande de prévoir une définition de la durée de la recherche, car le terme utilisé n'est pas explicite en tant que tel.**

4.4 Le CIR - Duplication des fiches

81 Il est indiqué dans l'exposé des motifs que l'une des propositions vise à garantir la simplicité et à réduire la duplication[37]. Le CEPD attend donc du CIR qu'il favorise un point d'entrée unique des données relatives à une personne, lorsque des données à caractère personnel identiques sont enregistrées ou corrigées dans les différents systèmes. Toutefois, cela ne ressort pas clairement d'une lecture conjointe des articles 17 et 18 des propositions.

82 En effet, si l'article 17 des propositions dispose qu'un dossier individuel est créé dans le CIR pour chaque personne enregistrée dans l'un des systèmes, l'article 18 des propositions ne fournit qu'une liste des données pertinentes qui devraient être stockées dans le CIR. Cela signifie que lorsqu'une personne fait l'objet de plusieurs fiches identiques dans l'un des systèmes sous-jacents, le CIR récupérera également ces données identiques. En outre, l'article 23, paragraphe 2, des propositions dispose qu'un dossier individuel est stocké dans le CIR tant que les données correspondantes sont stockées dans au moins un des systèmes d'information sous-jacents.

83 Par conséquent, **le CEPD craint que les propositions n'empêchent pas suffisamment la possibilité de duplication des données à caractère personnel. Il recommande donc d'être plus précis dans les articles correspondants et d'apporter les modifications nécessaires.**

4.5 Période de conservation des données dans le CIR et le MID

84 L'article 23, paragraphe 2, et l'article 35 des propositions définissent la période de conservation des données stockées dans le CIR et le MID, respectivement. Un dossier individuel n'est supprimé du CIR que lorsque les données correspondantes sont supprimées de tous les systèmes d'information. Les dossiers de confirmation d'identité et les données y afférentes sont stockés avec les liens dans le MID tant que les données liées sont stockées dans deux ou plusieurs systèmes d'information.

85 Toutefois, les propositions ne précisent pas la méthode de suppression des données après leur expiration. Il y a un risque que lorsque des informations sont introduites dans un système pour une période déterminée - à moins que la période de conservation et la suppression automatique ne soient techniquement mises en œuvre par le système -, les données à caractère personnel puissent être conservées dans le système au-delà de la date à laquelle elles auraient dû être supprimées. **Par conséquent, le CEPD recommande de**

préciser, dans les articles pertinents, que la suppression automatique des données sera applicable.

4.6 Vérification manuelle des liens

4.6.1 Décisions automatisées

86 Le CEPD tient à souligner que le processus automatisé de création de liens aux fins de la détection d'identités multiples constituerait une décision automatisée au sens de la législation relative à la protection des données. Les règles en matière de protection des données accordent traditionnellement aux personnes un niveau élevé de protection dans ces circonstances, en raison de l'absence d'intervention humaine et du risque d'intrusion dans la sphère privée. Ainsi, par exemple, l'article 22 du règlement 2016/679 et l'article 19 du règlement (CE) nº 45/2001 disposent à cet égard que la personne concernée a le droit de ne pas être soumise à une décision susceptible de comporter une mesure destinée à évaluer certains aspects de sa personnalité, prise sur le seul fondement d'un traitement automatisé de données produisant des effets juridiques à son égard ou l'affectant de manière significative, sans aucune intervention humaine.

87 Bien que l'article 22, paragraphe 2, du règlement 2016/679 et l'article 19 du règlement (CE) nº 45/2001 disposent que ce droit peut être limité par la loi, le CEPD tient à rappeler qu'une telle loi doit, dans le même temps, «prévoir des mesures appropriées garantissant la sauvegarde des droits et libertés ainsi que de l'intérêt légitime des personnes concernées». Afin de garantir, dans de telles circonstances, un traitement loyal et transparent à l'égard des personnes concernées, la logique de la décision et ses éventuelles conséquences doivent être clairement expliquées aux personnes concernées [voir article 13, paragraphe 2, point f), et article 14, paragraphe 2, point g), du règlement 2016/679]. Le responsable du traitement devrait également utiliser des procédures mathématiques ou statistiques adéquates aux fins du profilage, appliquer les mesures techniques et organisationnelles appropriées pour faire en sorte, en particulier, que les facteurs qui donnent lieu à des erreurs dans les données à caractère personnel soient corrigés et que le risque d'erreur soit réduit au minimum, et sécuriser les données à caractère personnel d'une manière qui tienne compte des risques susceptibles de peser sur les intérêts et les droits de la personne concernée et qui prévienne, entre autres, les effets discriminatoires à l'égard des personnes physiques fondées sur l'origine raciale ou ethnique, les opinions politiques, la religion ou les convictions, l'appartenance syndicale, le statut génétique ou l'état de santé, ou l'orientation sexuelle, ou qui se traduisent par des mesures produisant un tel effet[38].

88 Dès lors, **le CEPD considère que le processus de création de liens aux fins de la détection d'identités multiples constituerait une décision automatisée. Par conséquent, la transparence à l'égard des personnes concernées et les garanties nécessaires pour ce traitement devraient être prévues dans les propositions.**

4.6.2 Vérification manuelle

89 Les propositions instaurent un détecteur d'identités multiples («MID») qui sera en mesure d'indiquer si une personne est connue sous différentes identités dans les différents systèmes d'information (c'est-à-dire le SIS, le VIS, l'ETIAS, l'ECRIS, l'EES ou Eurodac). Le MID stockera les liens entre les personnes présentes dans plus d'un système

ainsi que la référence au système auquel appartiennent les données. Ces liens seront classés dans quatre catégories: blanc, jaune, vert et rouge:

- un lien blanc signifie que les différentes identités biographiques appartiennent à une même personne;
- un lien jaune signifie qu'il existe une possibilité d'identités biographiques différentes pour une même personne;
- un lien vert confirme que différentes personnes se trouvent partager la même identité biographique, ou
- un lien rouge signifie qu'il existe des soupçons qu'une même personne utilise illicitement différentes identités biographiques.

90 L'article 28, paragraphe 4, des propositions dispose qu'un lien jaune est créé lorsqu'une recherche de données biométriques ou de données d'identité génère un ou plusieurs résultats positifs et que les données d'identité des dossiers liés ne peuvent pas être considérées comme similaires. Toutefois, l'article 30, paragraphe 1, point b), des propositions affirme qu'un lien jaune est créé lorsque les données liées comportent des données d'identité différentes et qu'aucune vérification manuelle n'a été effectuée. Cette définition prête à confusion car elle suppose qu'un lien jaune serait créé entre les différentes données de deux ou plusieurs systèmes d'information. Cela signifierait aussi qu'aucun lien vert ne pourrait être créé par l'autorité responsable puisqu'aucun lien jaune n'aurait été créé au préalable. **Le CEPD présume que l'expression «données différentes» devrait se lire «données similaires» et recommande donc de modifier l'article 30 en conséquence. Par souci de clarté, il recommande en outre de prévoir à l'article 28, paragraphe 4, ainsi qu'à l'article 30 des propositions, une définition uniforme de «lien jaune».**

91 La création d'un lien jaune déclenche la procédure de vérification manuelle prévue à l'article 29 des propositions. L'article 29, paragraphe 1, des propositions dispose que la vérification manuelle devrait être effectuée par l'autorité qui a créé ou mis à jour le dossier correspondant. En revanche, l'article 29, paragraphe 2, des propositions prévoit une responsabilité exclusive du bureau SIRENE lorsqu'un lien jaune fait référence à un signalement SIS. Étant donné que le bureau SIRENE n'intervient pas nécessairement dans la création ou la mise à jour d'un dossier au sens de l'article 29, paragraphe 1, des propositions, il est difficile de savoir si et comment le bureau SIRENE pourrait être informé de sa responsabilité de vérifier les différentes identités. **Le CEPD recommande d'ajouter à l'article 29 des propositions que le bureau SIRENE responsable est immédiatement informé lorsqu'il doit vérifier manuellement un lien jaune.**

92 À cet égard, le CEPD constate que si l'article 29 des propositions dispose que les autorités responsables doivent mettre à jour sans délai les liens pertinents, il n'existe aucune disposition relative au cas où une autorité responsable ne s'acquitte pas de ses responsabilités. **Le CEPD recommande donc d'introduire un calendrier fixe assorti de délais spécifiques et d'établir une procédure claire afin de garantir une vérification en temps voulu, dans la mesure où ces liens pourraient potentiellement avoir des conséquences négatives pour la (les) personne(s) concernée(s).**

93 Conformément à l'article 29, paragraphe 3, des propositions, l'autorité responsable devrait avoir accès au dossier de confirmation d'identité pertinent figurant dans le MID et, conformément à l'article 21 des propositions, aux données d'identité liées figurant

dans le CIR, afin de vérifier l'identité d'une personne. En ce qui concerne le CIR, l'article 21 des propositions précise que l'accès ne devrait être accordé qu'aux données d'identité connectées à un lien jaune. L'autorité responsable devra ensuite évaluer les différentes identités et décider si le lien peut être considéré comme un lien vert, rouge ou blanc. Lorsque la décision de l'autorité responsable débouche sur un lien blanc ou rouge, les nouvelles données sont ajoutées au dossier individuel dans le CIR, conformément à l'article 19, paragraphe 2, des propositions.

94 Conformément à l'article 27, paragraphe 1, point e), des propositions, le MID est lancé lorsqu'un signalement de personne est créé ou mis à jour dans le SIS. Toutefois, l'article 26, paragraphe 1, point e), et l'article 29, paragraphe 1, point e), des propositions disposent que le bureau SIRENE n'a accès au MID que lors de la mise à jour d'un signalement, mais pas lors de la création d'un signalement. **Le CEPD considère qu'il s'agit d'une erreur de rédaction et recommande de modifier les articles 26 et 29 des propositions en conséquence.**

95 En outre, le CEPD remarque que les propositions parlent souvent de différentes identités désignant de manière licite ou illicite une personne [article 32, paragraphe 1, points a) et b)]. **Dans la mesure où les propositions n'indiquent pas quand une identité désigne de manière licite ou illicite une personne, le CEPD recommande de clarifier davantage la signification de ces termes dans les dispositions pertinentes ou, tout au moins, dans un considérant.**

96 Enfin, le CEPD constate que les propositions prévoient la possibilité pour une personne concernée de corriger un lien erroné dans les faits, mais que les États membres n'ont pas la possibilité de rectifier eux-mêmes de tels liens[39]. Le CEPD est d'avis qu'un tel mécanisme permettrait d'améliorer encore davantage la qualité des données au sein des systèmes pertinents, répondant ainsi à l'objectif d'interopérabilité visé. Par conséquent, **il recommande d'adopter dans les propositions un mécanisme pertinent permettant aux États membres de rectifier eux-mêmes un lien incorrectement établi.**

4.7 Répertoire central des rapports et statistiques - CRRS

97 Conformément à l'article 39 des propositions, l'agence eu-LISA devrait établir, mettre en œuvre et héberger un répertoire central des rapports et statistiques. Le CEPD rappelle, dans ce contexte, ses avis précédents sur l'EES[40], l'ETIAS[41], le SIS[42] et l'agence eu-LISA[43]. Dans ces avis, le CEPD a vivement mis en garde contre le fait que la solution proposée pour la fourniture de statistiques imposerait une lourde charge à l'eu-LISA et au CEPD, puisque l'eu-LISA devrait maintenir et sécuriser un deuxième répertoire, tandis que le CEPD devrait superviser ce deuxième répertoire.

98 Le CEPD serait donc favorable à une solution qui, au lieu de rendre nécessaire un répertoire central supplémentaire, imposerait à l'eu-LISA de développer des fonctions permettant aux États membres, à la Commission, à elle-même ainsi qu'aux agences autorisées d'extraire automatiquement et directement les statistiques demandées du système.

99 À cet égard, le CEPD souligne que l'agence eu-LISA devrait également procéder à une évaluation approfondie des risques en matière de sécurité de l'information avant la mise en œuvre du CRRS et qu'elle devrait aussi aborder la question des points d'accès

sécurisés. Il est important que des mesures de sécurité adéquates soient mises en place avant l'établissement du CRRS.

100 Le CEPD comprend la nécessité pour le personnel dûment autorisé des autorités compétentes des États membres, de la Commission et de l'eu-LISA d'avoir accès aux données contenues dans le CIR et le MID à des fins d'établissement de rapports et de statistiques, et, pour l'Agence européenne des gardes-frontières et des garde-côtes, à des fins d'analyse des risques et d'évaluation de la vulnérabilité. Toutefois, il convient de noter que, contrairement au libellé de l'article 56, paragraphes 2 et 3, des propositions, la combinaison de la nationalité, du sexe et de l'année de naissance d'une personne pourrait conduire à une identification individuelle.

101 **Le CEPD recommande donc de reformuler l'article 56, paragraphes 2 et 3, des propositions et de reconnaître que les données énumérées à l'article 56, paragraphe 2, points a) à d), et paragraphe 3, points a) à c), pourraient conduire à l'identification de personnes et doivent donc être protégées. Cette protection implique encore une fois de procéder à une évaluation approfondie des risques dans le domaine de la sécurité de l'information, et de mettre en œuvre des mesures de sécurité adéquates avant de créer ce répertoire central supplémentaire. Le CEPD recommande en outre que le respect de la vie privée dès la conception soit également appliqué lors de la conception du CRRS.**

4.8 Qualification de l'eu-LISA en tant que sous-traitant

102 À plusieurs reprises, le CEPD a souligné les conséquences de la répartition des rôles entre divers acteurs dans les bases de données à grande échelle de l'UE et a recommandé que lorsqu'un acteur définit indépendamment les finalités ou les méthodes du traitement de données, il devrait être considéré comme un responsable du traitement plutôt que comme un sous-traitant[44]. Dans le même ordre d'idées, lorsque plusieurs entités contribuent aux finalités et/ou aux moyens de traitement, comme c'est le cas dans la présente proposition de règlement, elles devraient être considérées comme des responsables conjoints du traitement.

103 L'article 4, paragraphe 7, du règlement 2016/679 définit le responsable du traitement comme une personne physique ou morale, une autorité publique, un service ou tout autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel. L'article 26 du règlement 2016/679 précise la notion de contrôle conjoint et dispose que, lorsque deux ou plusieurs entités déterminent conjointement les finalités et les moyens de traitement, elles sont considérées comme des responsables conjoints du traitement. Ces responsables conjoints du traitement devraient définir clairement qui est responsable de quoi entre eux lorsque cela n'est pas déjà défini par la loi.

104 En 2010, le groupe de travail «Article 29» a rendu un avis sur les concepts de responsable du traitement, de sous-traitant et de responsabilité conjointe du traitement[45]. Dans cet avis, il a conclu que la notion de responsable du traitement est autonome, en ce sens qu'elle doit être interprétée principalement selon le droit de l'Union en matière de protection des données, et fonctionnelle, en ce sens qu'elle est destinée à répartir les responsabilités lorsque l'influence factuelle est, et donc fondée sur une analyse factuelle plutôt que sur une analyse formelle.

105 L'article 40 des propositions dispose que les autorités des États membres qui sont les responsables du traitement des systèmes sources concernés restent responsables du BMS partagé et du CIR. Pour le traitement des données dans la directive MID, l'Agence européenne des garde-frontières et des garde-côtes et les autorités de l'État membre qui ajoutent ou modifient les données du fichier de confirmation d'identité sont considérés comme des responsables du traitement conformément au règlement (UE) 2016/679. L'article 41 de la proposition de règlement dispose que l'eu-LISA doit être considérée comme le sous-traitant conformément au règlement (CE) n° 45/2001 pour le traitement des données à caractère personnel dans le CIR.

106 Selon l'article 52 des propositions, l'agence eu-LISA est responsable du développement des éléments d'interopérabilité et de toutes les adaptations nécessaires pour établir l'interopérabilité entre les systèmes centraux et le portail de recherche européen, le BMS partagé, le CIR et le MID. En outre, l'eu-LISA définit l'architecture physique, y compris ses spécifications techniques, les représentants des États membres réunis au sein d'un conseil de gestion du programme assurant la gestion adéquate de la phase de conception et de développement (article 52, paragraphe 4). La gestion technique de l'infrastructure centrale incombe à l'eu-LISA, qui est également responsable de la sécurité des éléments d'interopérabilité et de l'infrastructure de communication correspondante (article 53, paragraphe 1, et article 42, paragraphe 2). L'eu-LISA veille, en coopération avec les États membres, à ce que la meilleure technologie disponible soit utilisée en permanence (article 53, paragraphe 1), et elle élabore et gère un mécanisme de contrôle de la qualité des données (article 53, paragraphe 3). Cela montre que l'eu-LISA jouera un rôle important dans la détermination des moyens de traitement, tant pendant le développement initial que pendant les opérations.

107 Comme expliqué ci-dessus, le concept de responsabilité du traitement est basé sur une analyse factuelle. L'attribution des rôles dans la proposition de règlement conduit à une situation où les États membres sont responsables des questions qu'ils contrôlent (par exemple, comment l'eu-LISA gère la sécurité de l'information et la transmission sécurisée des données vers et depuis les bases de données). En outre, l'eu-LISA se voit confier des tâches (développer le système, assurer sa sécurité pendant les opérations, etc.) que, selon les propositions, elle est censée accomplir avec une plus grande autonomie que celle d'un sous-traitant. Par conséquent, **nous recommandons de désigner l'agence eu-LISA et les autorités compétentes des États membres en tant que responsables conjoints du traitement, chacun ayant des tâches et des responsabilités clairement définies.**

4.9 Sécurité

108 Le CEPD note que les propositions réuniraient des bases de données à grande échelle de l'UE et des données sensibles. Il est donc extrêmement important que ces données soient protégées contre d'éventuels attaquants et incidents de sécurité. Le CEPD recommande fortement que l'agence eu-LISA et les États membres tiennent compte du principe de la protection des données dès la conception et par défaut pendant la phase de développement et de mise en œuvre de chaque nouveau système et élément d'interopérabilité, et, en outre, qu'ils mettent en œuvre un processus complet de gestion des risques en matière de sécurité de l'information (ISRM).

109 Le CEPD souligne l'importance de procéder à une gestion complète des risques liés à la sécurité de l'information suivant l'article 22 du règlement (CE) nº 45/2001 et les orientations du CEPD. Il recommande que toute référence à la sécurité de l'information ou aux plans de sécurité dans la proposition soit remplacée par «la mise en œuvre d'un processus complet de gestion des risques en matière de sécurité de l'information (ISRM)».

110 Conformément à l'article 37 des propositions, les contrôles automatisés de la qualité des données garantissent un niveau minimal de qualité des données pour toutes les données stockées dans les systèmes. Le CEPD se félicite de la mise en place de ces contrôles. Toutefois, il résulte d'une lecture conjointe des paragraphes 1 et 3 de l'article 53 des propositions que l'eu-LISA ne développera un mécanisme pour effectuer de tels contrôles de qualité qu'après la mise en service des nouveaux systèmes.

111 **Le CEPD recommande vivement que des contrôles automatisés de la qualité des données soient mis en place dès que possible et testés de préférence avant l'entrée en service.**

112 Le CEPD est d'avis que l'eu-LISA devrait également se pencher sur la question de la gouvernance de la sécurité pendant la phase de développement des éléments d'interopérabilité, car cela permettra d'assurer l'application de mesures de sécurité de pointe.

113 L'article 42 des propositions définit la sécurité du traitement tant pour l'eu-LISA que pour les États membres. Le CEPD est d'avis que les responsabilités techniques relatives à la sécurité des éléments d'interopérabilité devraient être partagées entre l'eu-LISA et les États membres, compte tenu de la conception architecturale spécifique du système. **Si les autorités des États membres ne peuvent pas être responsables du système central, elles peuvent être responsables de la sécurité aux points finaux en ce qui concerne l'accès aux systèmes (sécurité des lignes de communication nationales, contrôles d'accès, autorisations, traitement de données, etc.). Le CEPD recommande de modifier l'article 42, paragraphe 1, des propositions pour refléter cette distinction.**

114 Le CEPD rappelle qu'un plan de sécurité adéquat, tel que défini à l'article 42, paragraphe 3, des propositions, devrait être le résultat d'une évaluation approfondie des risques en matière de sécurité de l'information, raison pour laquelle une référence pertinente devrait être faite audit article. Ce plan de sécurité devrait également définir exactement les responsabilités et les exigences en matière de sécurité pour chaque partie prenante. En général, il importe de rappeler qu'une sécurité de l'information efficace ne peut être atteinte que par une analyse approfondie des risques auxquels un système d'information est soumis en matière de sécurité de l'information.

115 Comme le reflète l'article 42, paragraphe 3, point i), des propositions, les mesures de sécurité doivent être contrôlées par l'agence eu-LISA, qui doit également prendre les mesures organisationnelles nécessaires. **Le CEPD suggère de renforcer cette disposition afin de permettre la mise en place d'un système de gouvernance de la sécurité qui évaluera les mesures de sécurité appliquées en tenant compte également des nouveaux développements technologiques.**

4.10 Droits des personnes concernées

116 Le CEPD note que les propositions font référence, en ce qui concerne les droits des personnes concernées, aux dispositions pertinentes du règlement (CE) 45/2001 et du règlement (UE) 2016/679. Néanmoins, l'objectif premier de l'ECRIS et en partie du SIS est l'application de la loi et la coopération judiciaire, domaines auxquels s'applique la directive 2016/680. À cet égard, le CEPD recommande d'inclure, à l'article 46 des propositions, une référence à l'article 13 de la directive 2016/680 et, à l'article 47 des propositions, une référence aux articles 14 et 16 de la directive 2016/680.

117 L'article 46 des propositions dispose que les autorités compétentes informent les personnes concernées du traitement des données à caractère personnel les concernant dans le BMS partagé, le CIR et le MID, de la finalité du traitement, de l'identité et des coordonnées du responsable du traitement, des procédures pour exercer leurs droits en matière de protection des données, ainsi que des coordonnées du CEPD et des autorités de contrôle nationales. Le CEPD se félicite que les personnes concernées soient informées de la présence d'identités multiples illicites (cf. article 32, paragraphe 4, des propositions). Toutefois, il prend note du fait que les limitations proposées du droit à l'information des personnes concernées ne sont pas conformes à l'article 13, paragraphe 3, de la directive (UE) 680/2016. **Il recommande donc d'aligner l'article 32, paragraphe 4, des propositions sur l'article 13, paragraphe 3, de la directive (UE) 680/2016.**

118 Le CEPD estime qu'il est impératif que les personnes concernées soient également informées de la période de conservation de leurs données, c'est-à-dire que la période de conservation soit soumise aux règlements pertinents, comme le prévoient l'article 13, paragraphe 2, point a), du règlement 2016/679 et l'article 13, paragraphe 2, point b), de la directive 680/2016. Étant donné que le processus automatisé de création de liens aux fins de la détection d'identités multiples constitue une décision automatisée, les personnes concernées devraient également en être informées [cf. article 13, paragraphe 2, point f), du règlement 2016/679]. En outre, le CEPD est d'avis que les personnes concernées devraient également être informées des destinataires de leurs données et, conformément à l'article 48 des propositions, que les données les concernant stockées dans les éléments d'interopérabilité ou auxquelles ceux-ci ont accès ne sont pas transférées ou mises à la disposition de pays tiers, d'organisations internationales ou de parties privées, à l'exception des transferts à Interpol, comme le prévoient l'article 13, paragraphe 1, point f), du RGPD et l'article 13, paragraphe 2, point c), de la directive 680/2016.

119 **Le CEPD recommande donc d'ajouter à l'article 46 des propositions que les personnes concernées devraient également être informées des périodes de conservation pertinentes, des décisions automatisées et du fait que les données à caractère personnel ne sont pas transférées ou mises à la disposition de pays tiers, d'organisations internationales ou de parties privées, à l'exception des transferts à Interpol.**

120 Le CEPD constate que l'article 47, paragraphe 1, des propositions prévoit, en ce qui concerne les droits d'accès, de rectification, d'effacement et de limitation des personnes concernées, que la personne concernée peut adresser sa demande à tout État membre, qui examine la demande et y répond.

121 À cet égard, le CEPD fait observer que lorsqu'une personne soumet une demande à un État membre, comme prévu à l'article 47, paragraphe 1, des propositions, cet État membre doit déterminer quel est l'État membre responsable de la vérification manuelle. Toutefois, étant donné que l'article 13, paragraphe 2, et l'article 18, paragraphe 2, des propositions se réfèrent simplement au système pertinent mais pas à l'État membre responsable, l'article 26, paragraphe 2, limite l'accès de l'État membre au dossier de confirmation d'identification à cet égard. Dès lors, **le CEPD recommande d'ajouter à l'article 13, paragraphe 2, et à l'article 18, paragraphe 2, des propositions une référence à l'État membre responsable et, en ce qui concerne l'article 26, paragraphe 2, des propositions, une référence à l'article 34, point d), ce qui permettrait de garantir que la personne concernée peut effectivement exercer ses droits.**

122 En ce qui concerne l'article 47, paragraphe 3, des propositions, le CEPD constate que ce paragraphe ne fait référence qu'au droit de rectification et d'effacement, mais pas au droit à la limitation. **Le CEPD recommande d'ajouter le droit à la limitation à l'article 47, paragraphe 3, des propositions.**

123 Si l'article 47, paragraphe 3, des propositions prévoit qu'une demande de correction et d'effacement doit être transmise par un État membre à l'État membre responsable, il n'existe néanmoins aucune disposition de ce type en ce qui concerne le droit d'accès. **Le CEPD recommande d'ajouter à l'article 47 des propositions un paragraphe pertinent qui devrait comporter l'obligation pour l'État membre de transmettre la demande d'accès à l'État membre responsable.**

124 En outre, **le CEPD recommande d'ajouter à l'article 47 des propositions l'obligation pour les États membres d'informer la personne concernée que sa demande a été transmise, tout en indiquant les coordonnées de l'autorité compétente de l'État membre concerné.** Cela permettrait à la personne concernée d'identifier plus facilement l'autorité compétente et d'adresser d'autres demandes directement à l'autorité responsable.

125 **En ce qui concerne l'article 47, paragraphe 4, des propositions, le CEPD recommande d'inclure l'obligation pour l'État membre d'informer immédiatement la personne concernée après la rectification ou la suppression des données la concernant.**

126 Enfin, le CEPD tient à souligner que, dans leur phase initiale, les éléments d'interopérabilité traiteront principalement des données qui sont déjà stockées dans les systèmes concernés à ce moment-là. Par conséquent, la question se pose de savoir comment les responsables du traitement peuvent fournir aux personnes concernées les informations pertinentes avant le traitement. **Le CEPD recommande qu'une campagne de sensibilisation adéquate soit lancée par les États membres et au niveau de l'UE, avant que les éléments d'interopérabilité ne soient mis en œuvre et deviennent pleinement opérationnels.**

4.11 Accès du personnel de l'agence eu-LISA

127 L'article 68, paragraphe 3, des propositions dispose que l'agence eu-LISA pourrait avoir accès à toutes les données nécessaires aux fins de la maintenance technique. Étant donné que l'eu-LISA est le fournisseur et l'administrateur de tous les systèmes et de tous les éléments d'interopérabilité, le CEPD est conscient que cette agence doit avoir accès aux données à caractère personnel stockées dans les systèmes.

128 Toutefois, **le CEPD recommande de souligner à l'article 68, paragraphe 3, des propositions que l'agence eu-LISA ne devrait avoir accès aux données à caractère personnel que sous des garanties strictes et pour des finalités légitimes et spécifiques. À cet égard, les propositions devraient définir clairement les situations pertinentes dans lesquelles l'eu-LISA peut légalement accéder à des données à caractère personnel, comme par exemple lorsqu'un État membre lui demande d'intervenir pour la déconfliction des données (en particulier avec la biométrie) ou pour obtenir de l'aide, etc. Le CEPD recommande donc d'étudier ces circonstances et - si nécessaire - de modifier les propositions en conséquence.**

129 **Le CEPD souligne en outre que tout accès par l'agence eu-LISA devrait être consigné et recommande vivement d'insérer une disposition pertinente dans les propositions.**

4.12 Période de transition

130 Le CEPD croit comprendre que, conformément aux considérants 21 et 22 et à l'article 17, paragraphe 2, des propositions, le CIR conserverait les données à caractère personnel (données biographiques et biométriques) de ressortissants de pays tiers issues de l'EES, du VIS, d'Eurodac, de l'ETIAS et de l'ECRIS-TCN. Il est également clair que ces données ne resteraient pas dans les systèmes susmentionnés, dans la mesure où le CIR sera «*une architecture centrale qui remplacera les systèmes centraux*».

131 Toutefois, à la suite du plan de la Commission et de l'étude de faisabilité concernant le CIR, une solution hybride s'appliquerait pendant un certain temps. Partant, les données stockées dans le CIR resteraient dans les systèmes sous-jacents afin d'assurer le bon fonctionnement du nouveau système. Cela signifie que, pour une période indéfinie, il y aurait duplication des données.

132 **Le CEPD reconnaît la nécessité d'une telle période, mais cette solution hybride devrait être reflétée dans l'article transitoire des propositions, et il convient de souligner que cette solution hybride ne devrait être en place que pendant une durée limitée.**

4.13 Registres

133 Le CEPD se réjouit du fait que les éléments d'interopérabilité stockeront des registres aux fins de la protection et du suivi des données. Toutefois, **il recommande que les propositions comprennent également des dispositions précisant qui aura accès aux registres et comment cet accès sera accordé**, l'article 42 pertinent des propositions ne fournissant aucune information supplémentaire concernant la gestion et l'accès à ces registres.

134 Le CEPD prend note du fait que, conformément à l'article 10, paragraphe 1, et à l'article 16, paragraphe 1, des propositions, les registres de toutes les opérations de traitement des données au sein de l'ESP et du BMS partagé sont conservés de manière centralisée par l'eu-LISA. Néanmoins, l'article 45 des propositions oblige les responsables du traitement des données à prendre les mesures nécessaires afin de contrôler la conformité des opérations de traitement, notamment en vérifiant fréquemment les registres, et à coopérer, au besoin, avec les autorités de contrôle visées aux articles 49 et 50 des propositions.

135 Étant donné que ni les États membres, en tant que responsables du traitement des données (cf. article 40), ni les autorités de contrôle nationales n'ont accès aux registres de l'ESP et du BMS partagé, le CEPD conclut qu'une vérification ou un contrôle adéquat de l'ESP et du BMS partagé n'est pas possible.

136 **Le CEPD recommande donc de conserver les registres de l'ESP et du BMS partagé au niveau national également, de même que les registres du CIR (article 24, paragraphe 5) et du MID (article 36, paragraphe 2).**

4.14 Autorités de contrôle nationales

137 Conformément à l'article 49 des propositions, les autorités de contrôle nationales veillent à ce que les autorités nationales responsables réalisent, tous les quatre ans au minimum, un audit des opérations de traitement des données, conformément aux normes internationales d'audit applicables. Toutefois, les propositions ne prévoient pas le contrôle de la licéité du traitement des données à caractère personnel dans le cadre de ces propositions par l'autorité de contrôle nationale, mais évoquent plutôt, à l'article 45, un autocontrôle effectué par les responsables du traitement eux-mêmes.

138 **Le CEPD recommande vivement d'introduire une disposition prévoyant que chaque État membre veille à ce que l'autorité ou les autorités de contrôle désignées en vertu de l'article 51 du règlement (UE) 2016/679 et de l'article 41 de la directive (UE) 2016/680 contrôlent la licéité du traitement de données à caractère personnel en vertu des propositions de règlement.**

139 **Le CEPD recommande d'ajouter l'autorité de contrôle nationale à l'article 44, paragraphe 3, des propositions.**

4.15 Rôle du CEPD

140 Le CEPD est l'autorité compétente en matière de protection des données pour le contrôle de l'eu-LISA. Afin de lui permettre de contrôler efficacement l'eu-LISA dans le cadre de ses compétences, le CEPD estime qu'il devrait être inscrit sur la liste des destinataires des rapports que l'eu-LISA doit publier conformément à l'article 68, paragraphes 2 et 4, des propositions.

141 En outre, le CEPD rappelle que le contrôle ne peut être efficace que s'il dispose de ressources suffisantes. Alors que l'article 49, paragraphe 2, des propositions prévoit que les autorités de contrôle nationales devraient disposer de ressources suffisantes pour accomplir les tâches qui leur sont confiées en vertu du présent règlement, **le CEPD**

recommande d'inclure une disposition similaire à l'article 50 afin de lui garantir des ressources suffisantes.

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'UE 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'UE, 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'UE 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,

Giovanni BUTTARELLI

Notes

[1] JO L 281 du 23.11.1995, p. 31.
[2] JO L 119 du 4.5.2016, p. 1.
[3] JO L 8 du 12.1.2001, p. 1.
[4] JO L 350 du 30.12.2008, p. 60.
[5] JO L 119 du 4.5.2016, p. 89.
[6] 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.
[7] Ibidem, p. 15.
[8] 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.
[9] 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.
[10] Communication du 16.05.2017 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.
[11] Conclusions du Conseil sur la voie à suivre pour améliorer l'échange d'informations et assurer l'interopérabilité des systèmes d'information de l'UE, 8 juin 2017: http://data.consilium.europa.eu/doc/document/ST-10151-2017-INIT/fr/pdf.
[12]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.
[13] https://edps.europa.eu/sites/edp/files/publication/17-11-16_opinion_interoperability_en.pdf.
[14] 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, JOCE. L 327/20, 9.12.2017.
[15] 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.
[16] 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.
[17] 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, J.O.C.E., L 135/53.
[18] Déclaration du Contrôleur européen de la protection des données sur le concept d'interopérabilité dans le domaine de la migration, de l'asile et de la sécurité, annexé au rapport final du groupe d'experts de haut niveau sur les systèmes d'information et l'interopérabilité créé 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.
[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 13.8.2008, p. 129; règlement (UE) nº 603/2013 du Parlement européen et du Conseil du 26 juin 2013 relatif à la création d'Eurodac pour la comparaison des empreintes digitales aux fins de l'application efficace du règlement (UE) nº 604/2013 établissant les critères et mécanismes de détermination de l'État membre responsable de l'examen d'une demande de protection internationale introduite dans l'un des États membres par un ressortissant de pays tiers ou un apatride et relatif aux demandes de comparaison avec les données d'Eurodac présentées par les autorités répressives des États membres et Europol à des fins répressives, et modifiant le règlement (UE) nº 1077/2011 portant création d'une agence européenne pour la gestion opérationnelle des systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice (refonte), JO L 180/1 du 29.06.2013.

[20] 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 et Eurodac; règlement (UE) nº 603/2013 du Parlement européen et du Conseil du 26 juin 2013 relatif à la création d'Eurodac pour la comparaison des empreintes digitales aux fins de l'application efficace du règlement (UE) nº 604/2013 établissant les critères et mécanismes de détermination de l'État membre responsable de l'examen d'une demande de protection internationale introduite dans l'un des États membres par un ressortissant de pays tiers ou un apatride et relatif aux demandes de comparaison avec les données d'Eurodac présentées par les autorités répressives des États membres et Europol à des fins répressives, et modifiant le règlement (UE) nº 1077/2011 portant création d'une agence européenne pour la gestion opérationnelle des systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice.

[21]Règlement (UE) nº 2016/1624 du Parlement européen et du Conseil du 14 septembre 2016 relatif au corps européen de garde-frontières et de garde-côtes, modifiant le règlement (UE) nº 2016/399 du Parlement européen et du Conseil et abrogeant le règlement (CE) nº 863/2007 du Parlement européen et du Conseil, le règlement (CE) nº 2007/2004 du Conseil et la décision 2005/267/CE du Conseil.

[22] Excepté l'ECRIS-TCN, qui a été développé à des fins de coopération judiciaire.

[23] Analyse d'impact, p. 9 et 10.

[24] Analyse d'impact, p. 39.

[25] CJUE, Digital Rights Ireland Ltd, C-293/12, 8 avril 2014, point 60.

[26] CJUE, Digital Rights Ireland Ltd, C-293/12, 8 avril 2014, point 61.

[27] CJUE, Digital Rights Ireland Ltd, C-293/12, 8 avril 2014, point 61.

[28] Proposition de règlement 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] Analyse d'impact, p. 39.

[30] Proposition de règlement 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.

[31] Avis du Contrôleur européen de la protection des données sur la proposition de décision du Conseil 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 [COM (2005) 600 final], consultable à l'adresse suivante: https://edps.europa.eu/sites/edp/files/publication/06-01-20_access_vis_fr.pdf, Avis du Contrôleur européen de la protection des données sur la proposition modifiée de règlement du Parlement européen et du Conseil relatif à la création d'Eurodac pour la comparaison des empreintes digitales aux fins de l'application efficace du règlement (CE) nº (…/…) (établissant les critères et mécanismes de détermination de l'État membre responsable de l'examen d'une demande de protection internationale introduite dans l'un des États membres par un ressortissant de pays tiers ou un apatride), et sur la proposition de décision du Conseil relative aux demandes de comparaison avec les données d'Eurodac présentées par les autorités répressives des États membres et Europol à des fins répressives, consultable à l'adresse suivante: https://edps.europa.eu/sites/edp/files/publication/09-10-07_access_eurodac_fr.pdf; Avis 06/2016 sur le deuxième train de mesures «Frontières intelligentes» de l'Union européenne, recommandations sur la proposition révisée visant à créer un système d'entrée/sortie, p. 19 et 20, consultable à l'adresse suivante: https://edps.europa.eu/sites/edp/files/publication/16-09-21_smart_borders_fr.pdf, Avis 3/2017 sur la proposition de règlement portant création d'un système européen d'information et d'autorisation concernant les voyages, p.13, consultable à l'adresse suivante: https://edps.europa.eu/sites/edp/files/publication/17-03-070_etias_opinion_fr.pdf.

[32] Analyse d'impact, p. 25 et 43.

[33] Décision du Conseil 2008/615/JAI du 23 juin 2008 relative à l'approfondissement de la coopération transfrontalière, notamment en vue de lutter contre le terrorisme et la criminalité transfrontalière.

[34] Décision du Conseil 2008/615/JAI du 23 juin 2008 relative à l'approfondissement de la coopération transfrontalière, notamment en vue de lutter contre le terrorisme et la criminalité transfrontalière.

[35] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE, JO L 119, 4.5.2016, p. 1.

[36] Proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la

libre circulation de ces données, et abrogeant le règlement (CE) nº 45/2001 et la décision nº 1247/2002/CE, COM(2017) 8 final.
[37] Voir page 12 de l'exposé des motifs, COM (2016) 793 final.
[38] Voir le considérant 71 du RGPD.
[39] Voir par exemple l'article 34, paragraphe 3, du règlement SIS II.
[40] https://edps.europa.eu/sites/edp/files/publication/16-09-21_smart_borders_fr.pdf.
[41] https://edps.europa.eu/sites/edp/files/publication/17-03-070_etias_opinion_fr.pdf.
[42] https://edps.europa.eu/sites/edp/files/publication/17-05-02_sis_ii_opinion_fr.pdf.
[43] https://edps.europa.eu/sites/edp/files/publication/17-10-10_eu-lisa_opinion_fr_0.pdf.
[44] Avis 6/2016 du CEPD sur le deuxième train de mesures «Frontières intelligentes» de l'Union européenne, point 70 ou Avis 11/2017 du CEPD sur la proposition de règlement sur l'ECRIS-TCN, point 42.
[45] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_fr.pdf.