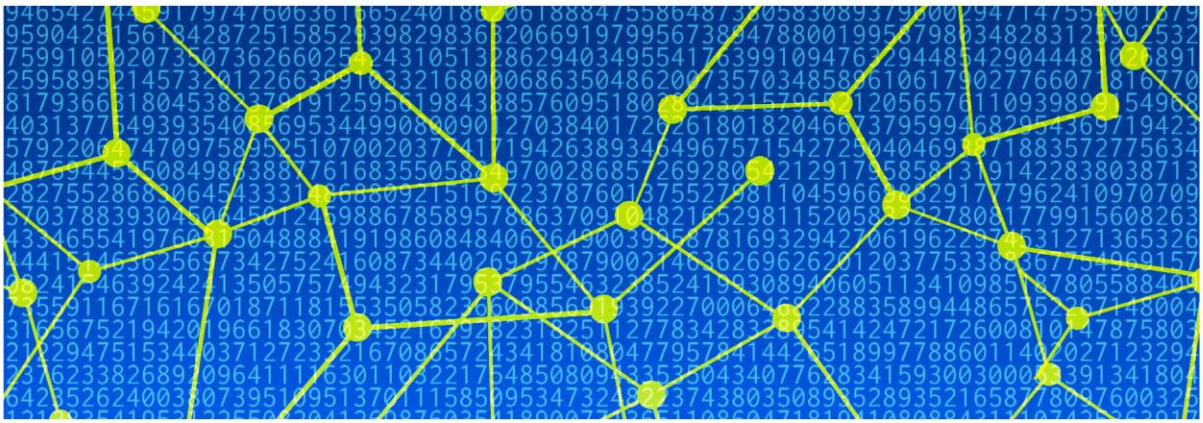

EUROPEAN DATA PROTECTION SUPERVISOR

Document de synthèse sur l'interopérabilité des systèmes d'information au sein de l'espace de liberté, de sécurité et de justice

EDPS

17 novembre 2017

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 document de synthèse a pour objectif de contribuer aux travaux préparatoires sur la future proposition de législation relative à l'interopérabilité des systèmes d'information à grande échelle de l'UE aux fins de la gestion des frontières et de la sécurité. Il s'inscrit dans le cadre de la mission du CEPD, qui consiste à conseiller les institutions de l'UE sur les implications de leurs politiques en matière de protection des données et à encourager l'élaboration responsable de politiques, conformément à l'action nº 9 de la stratégie du CEPD: «Faciliter l'élaboration responsable et éclairée de politiques». Le CEPD estime que le respect des exigences en matière de protection des données est indispensable à une gestion efficace et efficiente de l'information aux fins de la gestion des frontières et de la sécurité.

Synthèse

En principe, l'interopérabilité vise à développer un partage efficace et efficient des informations afin de veiller à ce que les autorités compétentes, tant nationales que de l'UE, disposent des bonnes informations au bon moment. Si elle est mise en œuvre de manière réfléchie, l'interopérabilité peut contribuer, non seulement à répondre à certains besoins des autorités compétentes qui ont recours à des systèmes d'information à grande échelle, mais aussi à réduire les coûts totaux de fonctionnement de ces systèmes. L'interopérabilité peut également servir les intérêts de la protection des données. Par exemple, l'interconnexion de systèmes d'information dont les finalités sont étroitement liées et contenant par ailleurs certaines données identiques pourrait contribuer à éviter que des données identiques ou similaires soient stockées, validées et actualisées à maintes reprises, une fois dans chaque système.

Les attentats terroristes survenus sur le territoire de l'UE ont exacerbé les préoccupations en matière de sécurité. L'UE est par ailleurs confrontée depuis quelques années à un afflux massif de réfugiés et de migrants. Ces circonstances ont conduit la Commission européenne à envisager plusieurs initiatives, y compris l'interopérabilité des systèmes d'information à grande échelle de l'UE créés dans les domaines des migrations, de la gestion des frontières et/ou de la coopération policière.

Bien que nous soyons conscients du fait que la Commission pourrait avoir envisagé l'interopérabilité comme un outil dans l'unique but de faciliter l'utilisation des systèmes, nous comprenons qu'elle pourrait envisager de l'étendre à de nouvelles possibilités d'échange ou de recoupement de données.

Dans la mesure où l'introduction de l'interopérabilité risque de susciter des traitements de données à caractère personnel nouveaux (ou modifiés), de tels changements nécessiteraient une base juridique claire dans le strict respect de la Charte des droits fondamentaux de l'Union européenne. En particulier, tout nouveau traitement de données ou toute modification d'un traitement de données devra être clairement défini(e) dans l'instrument juridique pertinent, et devrait être tout aussi nécessaire et proportionné au regard de ses objectifs clairement énoncés.

Allant bien au-delà des principes de protection des données dès la conception/par défaut, ainsi que de l'obligation de mettre en œuvre des mesures de sécurité, le respect des règles européennes régissant la protection des données nécessite, en premier lieu, d'établir la nécessité et la proportionnalité du traitement.

Nous attendons dès lors avec grand intérêt la prochaine proposition de législation de la Commission européenne, laquelle devrait définir clairement les problèmes que l'interopérabilité vise à résoudre. Elle devra également établir clairement quelles catégories de données à caractère personnel seraient traitées, et à quelles fins spécifiques, dans le contexte de ses futures initiatives en matière d'interopérabilité. Cela permettra d'engager un vrai débat sur l'interopérabilité sous l'angle des droits fondamentaux. La réalisation d'une analyse complète de l'impact de l'interopérabilité sur les droits fondamentaux à la vie privée et à la protection des données sera essentielle dès que de plus amples détails sur l'initiative prévue seront disponibles. La prochaine proposition de législation pourrait, en ce sens, être l'occasion de concevoir un cadre plus cohérent et plus homogène.

TABLE DES MATIÈRES

1 Initiatives en cours dans le contexte de «l'interopérabilité» des systèmes d'information à grande échelle

1 Les attentats terroristes survenus sur le territoire de l'UE ont exacerbé les préoccupations en matière de sécurité. L'UE est, par ailleurs, confrontée depuis quelques années à un afflux massif de réfugiés et de migrants. Ces circonstances ont conduit la Commission européenne à envisager plusieurs initiatives, y compris la création de nouveaux systèmes d'information à grande échelle de l'UE[1], la modification de systèmes actuels[2] ainsi que l'interopérabilité de tous ces systèmes.

2 Dans sa communication du 6 avril 2016 intitulée «*Des systèmes d'information plus robustes et plus intelligents au service des frontières et de la sécurité*» (la «communication de 2016»)[3], la Commission a souligné la nécessité d'améliorer l'interopérabilité des systèmes d'information; elle a également présenté des pistes pour le développement futur des systèmes d'information. La Commission a institué un groupe d'experts de haut niveau sur les systèmes d'information et l'interopérabilité (le «GEHN»). Le GEHN avait pour mission de se pencher sur «les aspects juridiques, techniques et opérationnels des différentes options permettant de parvenir à l'interopérabilité des systèmes d'information, en examinant notamment l'utilité, la faisabilité technique et la proportionnalité des options disponibles et leurs conséquences sur le plan de la protection des données»[4].

3 Le GEHN a présenté ses recommandations sur le renforcement et le développement des systèmes d'information de l'UE et de l'interopérabilité, dans un premier temps, dans son rapport intérimaire de décembre 2016[5], puis, plus tard, dans son rapport final de mai 2017[6]. Le CEPD a été invité à participer aux travaux du GEHN. Il a publié une déclaration sur le concept de l'interopérabilité en matière de migrations, d'asile et de sécurité, laquelle est reprise dans le rapport final du GEHN.

4 Don son septième rapport sur les progrès accomplis dans la mise en place d'une union de la sécurité réelle et effective[7], la Commission a exposé une nouvelle approche de la gestion des données pour les frontières et la sécurité, conforme à la communication de 2016 et aux recommandations du GEHN. Selon cette approche, tous les systèmes d'information centralisés de l'UE assurant la gestion de la sécurité, des frontières et des migrations devraient être interopérables de telle sorte que:

- les systèmes puissent être interrogés simultanément en utilisant un portail de recherche européen, éventuellement à l'aide de règles simplifiées pour l'accès des services répressifs;
- les systèmes utilisent un service partagé de mise en correspondance permettant d'effectuer des recherches dans différents systèmes d'information contenant des données biométriques, éventuellement avec des indicateurs de concordance/non-concordance signalant le rapport avec des données biométriques connexes trouvées dans un autre système;
- les systèmes partagent un répertoire commun de données d'identité contenant des données d'identité alphanumériques, afin de détecter les enregistrements de personnes sous des identités multiples dans différentes bases de données.

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. Il a invité la Commission à poursuivre les travaux sur trois dimensions de l'interopérabilité (à savoir, le portail de recherche européen, le service de mise en correspondance de données biométriques et un répertoire commun de données d'identité)[8].

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[9]. La consultation était accompagnée d'une analyse d'impact initiale. Dans son document indicatif de planification du 2 octobre[10], la Commission mentionne la date du 12 décembre aux fins de l'adoption de la proposition de législation sur l'interopérabilité.

6 En attendant avec intérêt la future proposition législative, le présent document de synthèse constitue notre contribution supplémentaire. Il sera suivi d'un avis formel du CEPD en vertu de l'article 28, paragraphe 2, du règlement nº 45/2001.

2 Le concept d'interopérabilité

7 L'interopérabilité est communément définie comme la capacité de différents systèmes d'information à communiquer, à échanger des données et à utiliser les informations qui ont été échangées. Bien qu'elle soit souvent perçue comme un concept purement technique, nous considérons que, dans le contexte actuel, l'interopérabilité ne saurait être dissociée des questions visant à déterminer si l'échange de données est nécessaire, politiquement souhaitable ou juridiquement possible. En d'autres termes, même si l'interopérabilité des systèmes d'information sera, finalement, mise en œuvre grâce à des moyens techniques, il est nécessaire qu'elle fasse l'objet d'un débat politique quant à ses finalités et à sa future portée.

8 Nous observons que rendre techniquement possible l'échange des données constitue, dans de nombreux cas, une puissante incitation à les échanger. Ce faisant, on peut raisonnablement supposer que les moyens techniques seront utilisés dès lors qu'ils seront disponibles; en d'autres termes, le risque est dans ce cas que les moyens justifient la fin. Afin de permettre un vrai débat sur les risques et avantages de l'interopérabilité, il est essentiel d'attribuer à cette notion un sens clair et dénué de toute ambiguïté.

9 Nous remarquons que l'interopérabilité pourrait intervenir à plusieurs niveaux, que ce soit au niveau d'une simple infrastructure de communication entre deux systèmes ou à celui de la capacité de ces systèmes à, à la fois, échanger et utiliser les informations qui ont été échangées. Nous reconnaissons que, si elle est mise en œuvre de manière judicieuse, l'interopérabilité peut contribuer, non seulement à répondre à certains besoins des autorités compétentes qui ont recours à des systèmes d'information à grande échelle, mais aussi à réduire les coûts totaux de fonctionnement de tels systèmes. L'interopérabilité pourrait également être bénéfique en termes de protection des données. Par exemple, l'interconnexion de systèmes d'information dont les finalités sont étroitement liées, et contenant par ailleurs certaines données identiques, pourrait contribuer à éviter que des données identiques soient stockées à deux reprises, une fois dans chaque système[11].

10 L'interopérabilité viserait en principe à rendre les règles qui sont actuellement applicables à la fois plus efficaces et plus efficientes. Par exemple, le portail de recherche européen

envisagé par la Commission permettrait aux autorités compétentes d'interroger simultanément plusieurs systèmes plutôt que de devoir interroger chaque système séparément. Si ces interrogations étaient effectuées par des autorités compétentes autorisées agissant dans le plein respect de leurs droits d'accès et conformément aux finalités respectives de chaque système telles que définies dans les bases juridiques de ce dernier, il n'y aurait pas de problème fondamental en matière de protection des données. Un utilisateur accéderait uniquement aux informations auxquelles il est autorisé à accéder et exclusivement à la ou aux fins spécifiques au système en question.

11 Toutefois, bien que nous soyons conscients du fait que la Commission pourrait avoir envisagé l'interopérabilité uniquement comme moyen de faciliter l'utilisation des systèmes, nous comprenons qu'elle pourrait désormais chercher à l'étendre à de nouvelles possibilités d'échange ou de recoupement de données. Par exemple, l'analyse d'impact initiale mentionne l'utilisation d'un service partagé de mise en correspondance des données biométriques («le BMS») afin de permettre une mise en correspondance des données biométriques stockées dans les divers systèmes. De même, un «répertoire commun de données d'identité» regrouperait des données alphanumériques (telles que des noms et dates de naissance) qui ont été stockées dans les divers systèmes aux fins de la gestion des frontières et de la sécurité. L'utilisation combinée du BMS partagé et du répertoire commun de données d'identité permettrait de détecter les identités multiples au moyen d'une seule et unique identification reposant sur des données alphanumériques et/ou biométriques. L'interopérabilité met dès lors en jeu de nouveaux traitements des données qui ne sont pas couverts par les bases juridiques actuelles et dont l'impact sur les droits fondamentaux à la vie privée et à la protection des données doit être soigneusement évalué.

3 L'interopérabilité sous l'angle de la protection des données

3.1 Les données à caractère personnel «doivent être traitées loyalement, à des fins déterminées»

12 Nous considérons que l'interopérabilité ne devrait pas être une fin en soi, mais devrait toujours servir un véritable objectif d'intérêt public. L'analyse d'impact initiale mentionne, en premier lieu, l'objectif général consistant à «développer des systèmes d'information plus robustes et plus intelligents au service des frontières et de la sécurité». Elle répertorie ensuite les objectifs spécifiques suivants:

- veiller à ce que les utilisateurs finaux, en particulier les garde-frontières, les agents des services répressifs, les agents des services de l'immigration et les autorités judiciaires, aient accès rapidement et sans interruption à toutes les informations dont ils ont besoin pour s'acquitter de leurs missions;
- faciliter et simplifier l'accès des autorités répressives aux systèmes d'information qui ne relèvent pas des services répressifs lorsque cela est nécessaire aux fins de la prévention et de la détection des infractions pénales, et d'enquêtes et de poursuites en la matière;
- fournir une solution afin de détecter, et de lutter contre, l'usurpation d'identité[12].

13 Dans ce contexte, il est important de souligner que les objectifs généraux tels que ceux répertoriés dans l'analyse d'impact initiale ne représentent pas nécessairement des objectifs d'intérêt public aux termes de la loi, comme par exemple aux termes de l'article 52,

paragraphe 1, de la Charte, ainsi qu'au regard des finalités du traitement de données aux termes de la législation en matière de protection des données. Les objectifs mentionnés semblent se focaliser sur ce que l'interopérabilité permettrait de réaliser sur le plan technique. Toutefois, les traitements envisagés, l'intérêt général et leur(s) finalité(s) spécifique(s) ne sont pas expliqués. Au lieu de cela, l'analyse d'impact initiale semble assimiler le *traitement* que l'interopérabilité faciliterait ou permettrait (par exemple, la consultation des données, l'accès à celles-ci, leur utilisation, leur extraction, etc.) aux *finalités* du traitement.

14 Nous invitons la Commission à décrire clairement les finalités spécifiques des traitements des données envisagés. Si les objectifs du type «assurer un accès rapide et ininterrompu aux bases de données» pourraient être utiles comme moyen de parvenir à une fin du point de vue de la politique générale, ils ne sont toutefois pas assez spécifiques aux fins de la législation en matière de protection des données dans la mesure où ils ne sont pas liés à un traitement spécifique de catégories définies de données à caractère personnel. Ce faisant, ils pourraient ne pas permettre aux personnes de comprendre quelles sont les données à caractère personnel les concernant qui sont traitées, les finalités de ces traitements, ainsi que leurs conséquences.

15 Il est important de comprendre que la spécification des finalités est une condition indispensable à l'application de nombreux autres principes de la protection des données. Seule une définition claire et spécifique des finalités permettra de déterminer les données pertinentes à collecter, les périodes de conservation applicables, et de multiples autres aspects clés de la façon dont les données à caractère personnel seront traitées pour atteindre la ou les finalités choisie(s). La description de l'objectif d'intérêt général pourrait ne pas satisfaire à l'exigence de spécification de la finalité, en particulier lorsque l'intérêt général est susceptible d'englober différents aspects[13]. Aussi, recommandons-nous que la future proposition de législation définisse clairement les finalités précises des divers traitements de données envisagés.

3.2 Clarification des raisons pour lesquelles l'interopérabilité est une nécessité

16 Une description claire des finalités des traitements de données envisagés sera également indispensable à l'évaluation de leur nécessité et de leur proportionnalité. Ces finalités doivent être suffisamment détaillées non seulement pour permettre une évaluation objective visant à déterminer si la collecte et l'utilisation proposées sont conformes au droit, mais aussi pour établir les garanties qu'il convient de mettre en place. Nous vous invitons à vous référer au «guide pour l'évaluation de la nécessité», lequel fournit au législateur européen des conseils faciles à utiliser sur la façon de déterminer la conformité au regard des articles 7, 8 et 52, paragraphe 1, de la Charte. En particulier, l'évaluation de la nécessité et de la proportionnalité nécessite que le législateur détermine exactement ce que la mesure proposée prévoit en ce qui concerne le traitement des données à caractère personnel et quel(le)(s) est (sont) le(s) objectif(s) et la (les) finalité(s) concrète(s) de la mesure. Les problèmes que la mesure entend résoudre devraient également être suffisamment et clairement décrits, et être accompagnés d'éléments de preuve objectifs de leur existence. Enfin, il devrait être prouvé qu'aucun autre moyen moins intrusif ne permet de réaliser la ou les finalités envisagées[14].

17 Nous observons que l'analyse d'impact initiale recense quatre lacunes principales mises en évidence dans la communication de 2016, à savoir:
- les fonctionnalités sous-optimales des systèmes d'information actuels;
- des lacunes au niveau de l'architecture de gestion des données de l'UE;
- un ensemble complexe de systèmes d'information régis différemment; et
- une architecture fragmentée de gestion des données en matière de gestion des frontières et de sécurité.

18 Il est alors indiqué que l'interopérabilité des systèmes est indispensable à la résolution des carences susmentionnées, notamment en ce qui concerne:
- l'absence de données complètes et exactes;
- l'absence d'accès rapide et ininterrompu à toutes les informations;
- les conditions que les autorités répressives doivent remplir afin d'avoir accès aux bases de données qui ne relèvent pas des services répressifs; et
- l'usurpation d'identité.

19 Toutefois, si l'analyse d'impact initiale identifie un certain nombre de problèmes, elle ne décrit pas pour autant en détail les obstacles précis. Il n'est souvent pas clair si le problème fondamental est de nature juridique, technique ou les deux. Par exemple, que signifie exactement «l'absence d'accès rapide et ininterrompu à toutes les informations»? Est-ce une question juridique (à savoir le cadre juridique actuel ne permet pas à un utilisateur d'accéder à certaines données) ou technique (par exemple, le temps de réponse du système est trop long), ou peut-être les deux à la fois? Selon la façon dont le problème est défini, il se peut que la solution appropriée afin de le résoudre soit différente, en particulier en ce qui concerne le traitement des données. Sans une description claire et suffisamment détaillée des problèmes et besoins, il est difficile de s'assurer que les options stratégiques proposées (à savoir l'établissement d'un portail de recherche européen, un BMS partagé ou un répertoire commun) sont appropriées, proportionnées et répondent pleinement aux besoins identifiés.

20 En d'autres termes, seule une description claire des problèmes identifiés au regard des objectifs poursuivis permettra au législateur européen de déterminer les solutions juridiques et techniques les plus appropriées, dans le plein respect de la législation en matière de protection des données. La technologie doit toujours soutenir les politiques et besoins des utilisateurs, et non pas l'inverse. Ce qui est techniquement faisable n'est pas nécessairement justifié d'un point de vue juridique ou souhaitable d'un point de vue éthique. Ainsi que cela est souligné dans le préambule du règlement général sur la protection des données, «le traitement des données à caractère personnel devrait être conçu pour servir l'humanité»[15].

3.3 Limitation de la finalité en matière de migration, d'asile et de coopération policière et judiciaire

21 Nous souhaitons souligner l'importance d'envisager l'interopérabilité des systèmes d'information en tenant également compte du contexte politique dans lequel les systèmes d'information actuels ont été conçus. Telle qu'elle est envisagée par la Commission, l'interopérabilité aurait des répercussions sur des instruments mis en place afin de soutenir les politiques dans le domaine i) des vérifications aux frontières, de l'asile et de l'immigration, ainsi que ii) de la coopération policière et iii) de la coopération judiciaire. La politique européenne a de plus en plus tendance à associer gestion des flux migratoires et finalités sécuritaires. Cette tendance est observée dans le cadre de l'octroi de l'accès aux

systèmes actuels à des fins répressives[16], du développement d'un nouveau système d'information[17] ou de l'élargissement des compétences d'un organe existant[18]. Nous craignons que les références répétées aux migrations, 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 le terrorisme. Cela pourrait même contribuer à susciter une assimilation entre terroristes et étrangers.

22 Bien que les systèmes existants aient été développés dans l'optique d'une application distincte des politiques européennes en matière migratoire et répressive, nous reconnaissons qu'il pourrait exister des synergies entre les politiques et objectifs relevant du domaine migratoire et ceux relevant du domaine de la coopération policière. Il convient toutefois de ne pas perdre de vue le fait que les migrations, d'une part, et la coopération policière, de l'autre, restent deux domaines d'intervention publique et objectifs d'intérêt général différents, qui reposent sur des bases juridiques distinctes dans le TFUE et visent à atteindre des objectifs spécifiques qui doivent être clairement distingués. Cela pourrait avoir un impact sur l'évaluation de la compatibilité des finalités du traitement des données dont la Commission doit tenir compte dans le contexte de la future proposition de législation.

3.4 Les options proposées en matière d'interopérabilité

23 Nous souhaitons d'ores et déjà attirer l'attention du législateur européen sur certaines questions relatives à la protection des données qui pourraient se poser en lien avec certaines des solutions spécifiques actuellement à l'étude, à supposer que:

- la future proposition de législation décrive clairement les finalités, les objectifs et les besoins identifiés au vu des problèmes rencontrés et,
- des informations suffisantes soient fournies afin d'évaluer la nécessité et la proportionnalité des solutions retenues[19].

Ces questions concernent en particulier les conditions d'accès aux bases de données, l'utilisation des bases de données existantes à des fins nouvelles/supplémentaires, et la sécurité des données.

Nouveaux accès (Nouvelles modalités d'accès)

24 L'analyse d'impact initiale mentionne que, lorsque les utilisateurs finaux n'ont pas accès à certaines données au sein des systèmes centraux, le portail de recherche européen (grâce à des données alphanumériques) et le service partagé de données biométriques (grâce à des données biométriques) permettraient l'accès sur la base d'indicateurs de concordance/non-concordance, à savoir en indiquant la simple présence de données pertinentes dans les systèmes sous-jacents, sans pour autant révéler lesdites données.

25 Selon le ou les objectifs d'une telle nouvelle fonctionnalité, elle pourrait être considérée comme constituant:

- un nouveau cas de traitement de données à caractère personnel, à savoir *un nouvel accès*: l'autorité n'est pas autorisée à accéder aux données enregistrées dans un système donné mais saurait si ledit système contient ou non des informations concernant une personne donnée;

- un changement des *conditions applicables au traitement des données* (en l'occurrence, les conditions d'accès aux données à caractère personnel): l'autorité est déjà autorisée à accéder aux données mais sous réserve de certaines conditions (qui, du point de vue des droits fondamentaux, pourraient faire office de *garanties*). Selon l'approche proposée de concordance/non-concordance, une autorité aurait directement accès à une base de données qui lui permettrait de vérifier si la base de données contient ou non des informations au sujet d'une personne donnée. Toutefois, elle obtiendrait uniquement une indication de concordance ou de non-concordance. En cas de concordance, l'autorité devrait remplir une ou plusieurs conditions spécifiques afin d'accéder à davantage d'informations (par exemple, obtenir l'autorisation d'une autorité indépendante).

26 Dans le cas d'un *nouvel accès* tel que décrit ci-dessus, il est important de clarifier que l'existence (ou l'absence) de concordance constitue une donnée à caractère personnel même lorsque le minimum absolu d'information est en jeu (par exemple, connu ou inconnu dans un système donné) dans la mesure où cela représente une information concernant une personne (par exemple, la personne en question fait ou non l'objet d'un signalement dans le système d'information Schengen). Dès lors, un utilisateur qui n'est pas autorisé à accéder à des données conservées dans un système donné n'est pas non plus autorisé à avoir accès à des informations sur la concordance/non-concordance dans la mesure où cette seule information limitée constitue une donnée à caractère personnel. Par ailleurs, nous nous interrogeons sur l'utilité d'une telle fonction. En effet, être au courant de l'existence d'informations (concordance) sans pour autant être autorisé à accéder à tout l'éventail de données ne serait normalement pas utile dans le cadre du processus décisionnel et pourrait être contraire au principe de qualité des données (à savoir, seules les données à caractère personnel qui sont nécessaires aux fins indiquées peuvent être traitées) relatif à la protection des données.

27 S'agissant du recours à l'approche de concordance/non-concordance comme *condition d'accès*, le CEPD est conscient que l'objectif d'une telle approche pourrait être de fournir des garanties (à savoir, un accès limité) venant remplacer une ou plusieurs des conditions que les autorités répressives doivent actuellement remplir dans le cadre de l'accès aux bases de données qui ne relèvent pas des services répressifs.

28 À l'heure actuelle, une autorité répressive souhaitant accéder à des bases de données qui ne relèvent pas des services répressifs doit remplir plusieurs conditions (par exemple, accès nécessaire dans le cadre d'une affaire particulière, soupçons justifiés, contrôle préalable des bases de données nationales, etc.). Elle doit également avoir l'autorisation préalable d'une autre autorité agissant en toute indépendance et responsable de la prévention et de la détection des infractions terroristes et des autres infractions pénales graves, ainsi que des enquêtes en la matière. Avant d'octroyer une autorisation, ladite autorité vérifie si toutes les conditions d'accès prévues dans la base juridique du système d'information pertinent sont remplies.

29 Le rapport du GEHN suggère que, afin d'établir si un système à grande échelle contient (ou non) des informations au sujet d'une personne donnée, les autorités répressives devraient être autorisées à accéder à des systèmes d'information qui ne relèvent pas des services répressifs sans autorisation préalable. Pour les autres finalités (telles que par exemple celle de retracer les déplacements d'un suspect connu dans le cadre d'une enquête donnée), l'obtention d'une autorisation préalable demeurerait obligatoire.

30 Il est utile de souligner dans ce contexte que les systèmes d'information à grande échelle de l'UE - tels que le système d'information sur les visas ou Eurodac - ont été mis en place à des fins de migration et d'asile. La possibilité pour les autorités répressives d'accéder à ces bases de données a été ajoutée à un stade ultérieur, et uniquement sous réserve du respect de conditions (garanties) spécifiques visant à limiter les incidences anormales sur les personnes. Dès lors, tout assouplissement éventuel de ces conditions existantes devrait être spécifiquement justifié et nécessiterait une analyse rigoureuse et exhaustive de toutes les garanties restantes et/ou nouvelles afin d'évaluer la nécessité et la proportionnalité dudit éventuel assouplissement. En particulier, afin de préserver un niveau suffisamment élevé de protection contre d'éventuels abus, le relâchement des garanties des contrôles ex ante devrait, à tout le moins, s'accompagner d'un renforcement des contrôles ex post.

Nouvelles utilisations de données

31 L'analyse d'impact initiale indique que le service partagé de mise en correspondance des données biométriques («le BMS») permettrait une mise en correspondance des données biométriques stockées dans les divers systèmes, alors que le répertoire commun de données d'identité regrouperait des données alphanumériques (telles que des noms et dates de naissance) qui ont été stockées dans les divers systèmes d'information aux fins de la gestion des frontières et de la sécurité. L'utilisation combinée du BMS partagé et du répertoire commun de données d'identité permettrait de détecter les identités multiples liées aux mêmes données biométriques présentes dans les divers systèmes à grande échelle et contribuerait donc à la lutte contre l'usurpation d'identité.

32 Il convient de ne pas perdre de vue le fait que, combinée aux possibilités techniques de collecte de toutes les informations disponibles au sujet des personnes dans d'autres systèmes d'information, l'utilisation d'identificateurs uniques constituerait un nouveau traitement de données à caractère personnel devant être justifié de manière adéquate et suffisante (voir sections 3.1 et 3.2).

33 Par ailleurs, les systèmes d'information qui alimenteraient le répertoire commun de données d'identité ont été conçus à des fins autres que la lutte contre l'usurpation d'identité, laquelle constituerait une nouvelle finalité du traitement des données. Dans ce contexte, nous percevons un risque de «détournement d'usage» [à savoir, un élargissement de l'usage d'un système ou d'une base de données au-delà de la ou des fins pour laquelle/lesquelles il(elle) était à l'origine prévu(e)]. Comme avec toute initiative susceptible de permettre des utilisations des données ou systèmes autres que celles qui étaient initialement prévues par la loi, nous recommandons la prudence. L'argument selon lequel, les données ayant déjà été collectées, elles peuvent tout aussi bien être utilisées à d'autres fins, ne saurait être accepté sans sourciller, étant donné que tout tel nouveau traitement pourrait avoir un plus grand impact sur les personnes.

34 Enfin, nous souhaiterions saisir cette occasion pour clarifier le principe de minimisation des données, lequel est souvent méconnu. Par exemple, la communication de 2016 indique que le stockage des mêmes données dans plusieurs systèmes d'information est contraire au principe de minimisation des données. L'analyse d'impact initiale précise en outre qu'un répertoire commun de données d'identité contribuerait à une amélioration de l'efficacité en évitant la duplication des données. Toutefois, éviter la duplication des données n'assurera pas, en soi, la minimisation des données. Aux termes de la législation en matière de

protection des données, le principe de minimisation des données exige avant tout que la collecte et le traitement des données soient limités aux données qui sont adéquates, pertinentes et nécessaires au regard des finalités envisagées[20]. Dans la pratique, cela signifie que le partage des données entre des bases de données traitant les mêmes données ne sera pas forcément suffisant pour assurer la mise en œuvre du principe de minimisation des données.

Nouveaux défis en matière de sécurité

35 Nous souhaitons souligner que l'interopérabilité - telle que la conçoit la Commission à ce jour - introduirait un changement fondamental au niveau de l'architecture actuelle des systèmes d'information à grande échelle: le passage d'un environnement fermé à un environnement commun mettant en jeu la connectivité entre les divers systèmes. De nouveaux risques de sécurité s'ensuivraient. Prenons pour exemple le portail de recherche européen. De tels risques découleraient entre autres du fait qu'un pirate n'aurait alors besoin de compromettre qu'un seul point d'accès (au lieu de plusieurs, c'est-à-dire un point d'accès pour chaque système d'information) afin d'avoir accès à plusieurs systèmes d'information à grande échelle.

36 Il est dès lors primordial d'analyser de façon adéquate les conséquences sur la sécurité de l'information des diverses options proposées dans l'optique de l'interopérabilité. Une gestion exhaustive des risques liés à la sécurité de l'information conforme à l'article 22 du règlement (CE) nº 45/2001 et aux orientations émises par le CEPD semble s'imposer avant que tout changement susceptible d'affecter la sécurité de tous les systèmes ne soit entrepris[21].

4 Conclusions

37 Nous soutenons l'interopérabilité, dès lors qu'elle est mise en œuvre de manière judicieuse et en respectant les conditions fondamentales de nécessité et de proportionnalité. L'interopérabilité peut alors être un outil utile permettant de répondre aux besoins légitimes des autorités compétentes qui ont recours à des systèmes d'information à grande échelle de l'UE, et notamment d'améliorer le partage des informations.

38 Bien qu'elle soit souvent perçue comme un concept purement technique, l'interopérabilité ne saurait être dissociée, dans le contexte actuel, des questions visant à déterminer si l'échange de données est véritablement nécessaire, politiquement souhaitable ou justifié sur le plan juridique.

39 Du point de vue des droits fondamentaux, nous pensons que la Commission pourrait avoir envisagé l'interopérabilité uniquement comme moyen de faciliter l'utilisation des systèmes et de rendre les règles qui sont actuellement applicables à la fois plus efficaces et plus efficientes. Nous croyons toutefois comprendre que la Commission pourrait envisager de l'étendre à de nouvelles possibilités d'échange ou de recoupement de données. Cela mettrait en jeu de nouveaux traitements des données qui ne sont pas couverts par les instruments juridiques actuels. Leur impact sur les droits fondamentaux à la vie privée et à la protection des données devrait être soigneusement évalué.

40 Il convient de ne pas perdre de vue le fait que, allant bien au-delà des principes de protection des données dès la conception/par défaut, ainsi que, notamment, de l'obligation de mettre en œuvre des mesures de sécurité, le respect des règles européennes régissant la protection des données exige, en premier lieu, d'établir la nécessité et la proportionnalité du traitement.

41 En particulier, les problèmes que l'interopérabilité vise à résoudre devraient être clairement identifiés dans la future proposition de législation afin de permettre d'engager un vrai débat sous l'angle des droits fondamentaux. Nous observons que la Commission identifie un certain nombre de problèmes, sans pour autant décrire en détail les obstacles précis. Il n'est souvent pas clair si le problème fondamental est de nature juridique, technique ou les deux. Selon le problème, il se peut que la solution appropriée afin de le résoudre soit différente, en particulier en ce qui concerne le traitement des données. La proposition devrait également établir clairement les finalités spécifiques des éventuels traitements des différentes catégories de données à caractère personnel.

42 Ce faisant, nous estimons que la réalisation d'une analyse complète de l'impact de l'interopérabilité sur les droits fondamentaux à la vie privée et à la protection des données sera essentielle dès que de plus amples détails sur l'initiative prévue seront disponibles. La prochaine proposition de législation pourrait, en ce sens, être l'occasion de concevoir un cadre plus cohérent et plus homogène.

Bruxelles, le 17 novembre 2017

Giovanni BUTTARELLI

Notes

[1] Voir par exemple la proposition de règlement du Parlement européen et du Conseil portant création d'un système d'entrée/sortie pour enregistrer les données relatives aux entrées et aux sorties des ressortissants de pays tiers qui franchissent les frontières extérieures des États membres de l'Union européenne ainsi que les données relatives aux refus d'entrée les concernant, portant détermination des conditions d'accès à l'EES à des fins répressives et portant modification du règlement (CE) nº 767/2008 et du règlement (UE) nº 1077/2011, COM(2016) 194 final; 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) n° 515/2014, (UE) 2016/399, (UE) 2016/794 et (UE) 2016/1624, COM (2016) 731 final.

[2] Voir par exemple le paquet législatif relatif au SIS comprenant i) la proposition de règlement du Parlement européen et du Conseil sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen (SIS) dans le domaine des vérifications aux frontières, modifiant le règlement (UE) nº 515/2014 et abrogeant le règlement (CE) nº 1987/2006, COM(2016) 882 final; ii) la proposition de règlement du Parlement européen et du Conseil sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen (SIS) dans le domaine de la coopération policière et de la coopération judiciaire en matière pénale, modifiant le règlement (UE) nº 515/2014 et abrogeant le règlement (CE) nº 1986/2006, la décision 2007/533/JAI du Conseil et la décision 2010/261/UE de la Commission, COM(2016) 883 final, et iii) la proposition de règlement du Parlement européen et du Conseil relatif à l'utilisation du système d'information Schengen aux fins du retour des ressortissants de pays tiers en séjour irrégulier, COM(2016) 881 final. Voir également la proposition de règlement du Parlement européen et du Conseil relatif à la modification du règlement (UE) nº 603/2013 concernant la création d'«Eurodac» pour la comparaison des empreintes digitales aux fins de l'application efficace du [règlement nº 604/2013] établissant les critères et mécanismes de détermination de l'État membre responsable de l'examen d'une demande de protection internationale présentée dans l'un des États membres par un ressortissant de pays tiers ou un apatride, et de l'identification des ressortissants de pays tiers ou apatrides en séjour irrégulier, et relatif aux demandes de comparaison avec les données d'Eurodac présentées par les autorités répressives des États membres et par Europol à des fins répressives COM(2016)272 final.

[3] 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, 6.4.2017, COM(2016) 205 final.

[4] Ibidem, p. 15.

[5] 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

[6] 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

[7] 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.

[8] 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.

[9]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.

[10] Liste des points prévus pour figurer à l'ordre du jour des prochaines réunions de la Commission, http://ec.europa.eu/transparency/regdoc/rep/2/2017/EN/SEC-2017-415-F1-EN-MAIN-PART-1.PDF.

[11] Voir avis 6/2016 du CEPD sur le deuxième train de mesures «Frontières intelligentes» de l'Union européenne, point III.3.d), p. 15. https://edps.europa.eu/sites/edp/files/publication/16-09-21_smart_borders_fr.pdf.

[12] Analyse d'impact initiale , p.2.

[13] Voir «Étape 3» du «guide pour l'évaluation de la nécessité» publié par le CEPD le 11 avril 2017, et consultable à l'adresse suivante: https://edps.europa.eu/sites/edp/files/publication/17-06-01_necessity_toolkit_final_fr.pdf.

[14] Voir le «guide pour l'évaluation de la nécessité» publié par le CEPD le 11 avril 2017, lequel a pour but de mieux équiper les législateurs de l'UE chargés de préparer et d'examiner les mesures impliquant le traitement de données à caractère personnel et susceptibles d'interférer avec le droit à la vie privée, la protection des données et d'autres droits et libertés énoncés dans la Charte des droits fondamentaux de l'Union européenne; consultable à l'adresse suivante: https://edps.europa.eu/sites/edp/files/publication/17-06-01_necessity_toolkit_final_fr.pdf.

[15] 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 (règlement général sur la protection des données), JOCE du 4.5.2016, L 119/1.

[16] 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 du 29.6.2013, p. 1.

[17] Voir par exemple la proposition de règlement du Parlement européen et du Conseil portant création d'un système d'entrée/sortie pour enregistrer les données relatives aux entrées et aux sorties des ressortissants de pays tiers qui franchissent les frontières extérieures des États membres de l'Union européenne ainsi que les données relatives aux refus d'entrée les concernant, portant détermination des conditions d'accès à l'EES à des fins répressives et portant modification du règlement (CE) nº 767/2008 et du règlement (UE) nº 1077/2011, COM(2016) 194 final. Voir également la 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) 2016/974 et (UE) 2016/1624, COM(2016) 731 final.

[18]Proposition de règlement relatif au corps européen de garde-frontières et de garde-côtes et abrogeant le règlement (CE) n° 2007/2004, le règlement (CE) n° 863/2007 et la décision 2005/267/CE du Conseil (COM(2015) 671 final).

[19]Voir le «guide pour l'évaluation de la nécessité» publié par le CEPD le 11 avril 2017, lequel a pour but de mieux équiper les législateurs de l'UE chargés de préparer et d'examiner les mesures impliquant le traitement de données à caractère personnel et susceptibles d'interférer avec le droit à la vie privée, la protection des données et d'autres droits et libertés énoncés dans la Charte des droits fondamentaux de l'Union européenne; consultable à l'adresse suivante: https://edps.europa.eu/sites/edp/files/publication/17-06-01_necessity_toolkit_final_fr.pdf.

[20] Aux termes de l'article 5, paragraphe 1, point c), du règlement général sur la protection des données, les données à caractère personnel doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données).

[21]Guidance on Security measures for Personal Data Processing, Article 22 of Regulation 45/2001 (Orientations sur les mesures de sécurité relatives au traitement des données à caractère personnel, article 22 du règlement 45/2001), https://edps.europa.eu/sites/edp/files/publication/16-03-21_guidance_isrm_en.pdf.