



Observations relatives à la communication de la Commission sur l'interopérabilité des bases de données européennes

Bruxelles, le 10 mars 2006

Observations relatives à la communication de la Commission sur l'interopérabilité des bases de données européennes

Le contrôleur européen de la protection des données (CEPD) a pris acte de la publication, le 24 novembre 2005, de la communication de la Commission sur le renforcement de l'efficacité et de l'interopérabilité des bases de données européennes dans le domaine de la justice et des affaires intérieures et sur la création de synergies entre ces bases (ci-après "la communication").¹

Le CEPD salue toute initiative qui, à l'instar de cette communication, tend à améliorer l'efficacité des systèmes d'information européens à grande échelle, à mieux protéger les droits fondamentaux de la personne et à souligner la nécessité de procéder à des analyses d'impact approfondies sur l'évolution de ces systèmes.

Le CEPD a néanmoins quelques inquiétudes, tant générales que particulières, à l'égard de cette communication. Il les souligne dans le présent document.

A. Observations générales sur la notion d'interopérabilité

Cette communication porte principalement sur les aspects techniques et organisationnels de la notion d'interopérabilité. Or, le CEPD ne partage pas entièrement le point de vue de la Commission, pour qui "l'interopérabilité est un concept technique plutôt que juridique ou politique". En effet, il est évident que rendre techniquement possible l'accès à des données ou leur échange constitue, dans de nombreux cas, une puissante incitation à y accéder de facto ou à les échanger. On peut donc, sans trop s'avancer, partir du principe que les moyens techniques seront utilisés dès qu'il seront disponibles; en d'autres termes, ce sont parfois les moyens qui justifient la fin et non le contraire. Il se pourrait que l'on assiste par la suite à des demandes en faveur d'une législation moins stricte pour pouvoir utiliser ces bases de données plus facilement. Les modifications de la législation viennent en effet souvent entériner des pratiques déjà établies.

Le CEPD regrette que cette communication ne donne pas à la notion d'interopérabilité un sens clair et dénué de toute ambiguïté. Le débat sur l'interopérabilité n'a pas débouché sur des conclusions bénéficiant d'un large consensus. Il y a donc lieu de préciser cette notion.

Quand on parle d'interopérabilité, il ne s'agit pas seulement de l'utilisation en commun de systèmes d'information à grande échelle, mais également de possibilités d'accès aux données, d'échange de données ou même de fusion de bases de données. Ceci est regrettable, dans la mesure où des types d'interopérabilité différents requièrent des garanties et des conditions différentes. Tel est notamment le cas lorsque la notion d'interopérabilité sert de point de départ à d'autres mesures proposées visant à faciliter l'échange d'informations. Dans son avis sur le principe de disponibilité², le CEPD a souligné que bien qu'il n'entraîne pas la création

¹ http://europa.eu.int/eur-lex/lex/LexUriServ/site/fr/com/2005/com2005_0597fr01.pdf

² http://www.edps.eu.int/legislation/Opinions_A/06-02-28_Opinion_availability_EN.pdf

de nouvelles bases de données, ce principe suscitera inévitablement une nouvelle manière d'utiliser les bases de données existantes, puisqu'il offre de nouvelles possibilités d'accès à ces bases. C'est l'une des principales raisons pour lesquelles la notion d'interopérabilité doit être l'objet d'un examen très attentif.

En outre, cette communication entend proposer, pour les systèmes d'information à grande échelle, des objectifs nouveaux, allant au-delà de la finalité initiale de ces systèmes, ce qui, par conséquent, rend automatiquement nécessaire une nouvelle analyse complète de leur impact sur la protection des données personnelles. Cela étant, le CEPD insiste sur le fait que la mise en œuvre de l'interopérabilité des systèmes doit se faire en parfait accord avec les principes de protection des données, notamment le principe selon lequel la finalité du traitement des données doit être limitée. Toute limitation du respect des principes relatifs à la protection des données constitue une exception et ne peut être mise en œuvre que sous réserve de l'observation de conditions strictes et avec les garanties qui s'imposent, que celles-ci soient d'ordre technique ou autre.

Ces réflexions mettent une fois de plus en évidence la nécessité d'instaurer dans le troisième pilier un cadre légal pour la protection des données qui soit pleinement conforme aux principes de la protection des données prévus par le Traité CE et qui soit appliqué de manière effective afin de guider les évolutions telles que celles qui sont abordées dans la communication. Dans les pages qui suivent, le CEPD se penchera sur les principales questions que pose la communication. Il a abordé d'autres questions connexes dans ses avis antérieurs sur l'accès au VIS³ et sur la protection des données dans le troisième pilier⁴.

Le CEPD se tient à disposition pour fournir tout élément d'orientation supplémentaire concernant des propositions concrètes et espère être consulté chaque fois que l'action de la Commission fondée sur cette communication tombe sous le coup de l'article 28, paragraphe 2, du règlement (CE) n°45/2001.

B. Utilisation de la biométrie comme clé primaire

1. L'un des éléments essentiels d'une base de données est un numéro unique, que l'on appelle également clé primaire et qui est créé pour chaque article autour duquel sont réunies et conservées des données. A titre d'exemple, le numéro de la vignette-visa, qui fera partie du futur système d'information sur les visas (VIS), pourrait être utilisé comme clé primaire. Toutes les informations réunies pour une demande de visa seront alors reliées à ce numéro unique. Cette clé primaire est généralement considérée comme un élément essentiel de l'interopérabilité des bases de données, étant donné que la manière dont ces clés sont définies varie d'une base de données à l'autre. La limitation de l'accès à ces clés primaires est souvent utilisée comme instrument efficace de protection des données. Dans ce cas, l'interopérabilité est encore possible, mais seulement à travers une procédure moins directe et mieux contrôlée.

Dans sa communication, la Commission préconise l'utilisation de données biométriques, telles que les empreintes digitales ou même l'ADN, en tant que clés primaires. Selon le CEPD, cette utilisation ne serait pas compatible avec le subtil équilibre dont il est question au point 2.1 de la communication. Ce type de clés primaires permettra de fusionner deux bases de données ou plus, pour ainsi dire en temps réel et sans beaucoup d'efforts. Ainsi que cela a été dit dans l'étude d'analyse

³ http://europa.eu.int/eur-lex/lex/LexUriServ/site/fr/com/2005/com2005_0597fr01.pdf

⁴ http://europa.eu.int/eur-lex/lex/LexUriServ/site/fr/oj/2006/c_047/c_04720060225fr00270047.pdf

d'impact approfondie du système d'information sur les visas⁵, dans un rapport commandé par le Parlement européen⁶, de même que dans des avis précédents du CEPD⁷, les données biométriques, qui sont basées sur des probabilités, ne peuvent fournir la clé exempte de toute ambiguïté qui, par définition, est requise pour les clés primaires des bases de données. Ceci risque d'entraîner une violation du principe de la qualité des données.

2. Certains scénarios envisageables décrits par la communication prévoient un pool de bases de données de l'UE ou même, dans le cas des empreintes digitales ou de l'ADN, de bases de données des États membres. Dans cette perspective, l'objet de la communication passe de la notion d'interopérabilité à celle de bases de données interconnectées.

Permise techniquement et favorisée par l'utilisation de données biométriques comme clé primaire, une nouvelle tendance se fait jour. Cette tendance, illustrée par des projets très divers tels que le Traité de Prüm ou la future base de données européenne pour les permis de conduire conduira à des systèmes décentralisés, composés de constellations de bases de données fonctionnant davantage comme des réseaux de poste à poste que comme des systèmes centralisés. Le fait que la clé primaire puisse être créée "*naturellement*" (dans le cas de données biométriques) et ne soit pas produite par chaque système (dans le cas d'un identifiant unique) facilitera aussi le développement de ce pool de bases de données, par l'adjonction de toute une série de bases de données utilisant la même clé primaire librement et aisément accessible.

Cette agrégation de bases de données augmente par ailleurs le risque de "détournement d'usage". En effet, l'interconnexion de deux bases de données ayant deux finalités distinctes débouchera sur une troisième finalité pour laquelle ces deux bases de données n'ont pas été conçues. Or, ce résultat est tout à fait contraire à l'esprit du principe de limitation des finalités.

En fin de compte, cette tendance portera préjudice à l'harmonisation des règles relatives à la protection des données à caractère personnel au sein de l'UE. Elle sera notamment préjudiciable à une mise en œuvre harmonisée des droits de la protection des données en diminuant la possibilité d'un contrôle efficace et systématique tant au niveau de l'UE que des États membres.

C. Observations particulières

1. Il est regrettable que la protection des données à caractère personnel n'ait pas été suffisamment analysée comme un élément faisant partie intégrante du processus d'amélioration de l'interopérabilité des systèmes en question. Le CEPD propose d'ajouter à cette communication une analyse plus cohérente de la protection des données, englobant les technologies de protection de la vie privée afin d'améliorer à la fois l'efficacité et la protection des données.

⁵ *Study for the Extended Impact Assessment of the Visa Information System* (Étude d'analyse d'impact approfondie du système d'information sur les visas), rapport final du EPEC, décembre 2004.

⁶ Étude commandée par la commission LIBE du Parlement européen, "*Biometrics at the frontiers: assessing the impact on Society*" (la Biométrie aux frontières: évaluation des conséquences sur la société, février 2005

Institut de prospection technologique, DG Centre commun de recherche, CE.

⁷ http://europa.eu.int/eur-lex/lex/LexUriServ/site/fr/oj/2005/c_181/c_18120050723fr00130029.pdf
http://europa.eu.int/eur-lex/lex/LexUriServ/site/fr/oj/2006/c_091/c_09120060419fr00380056.pdf

2. Le CEPD partage entièrement le point de vue de la Commission, qui estime regrettable la sous-exploitation des systèmes existants et considère qu'une meilleure utilisation de ces systèmes constitue une priorité. Avant de créer de nouvelles bases de données ou de nouvelles fonctionnalités, il conviendrait d'investir pour permettre la pleine utilisation des bases de données existantes. L'inspection d'Eurodac, que le CEPD a récemment effectuée avec la coopération des services de la Commission, ne visait pas seulement à contrôler la bonne utilisation du système central. Elle avait également pour objet d'énoncer des recommandations pour en améliorer la protection et en rendre l'utilisation plus efficace.
3. La communication en appelle à une meilleure cohérence quant à la saisie des catégories de données dans les systèmes d'information, ce qu'il convient de saluer. Par exemple, l'harmonisation des critères de signalement dans le système SIS II sert également les intérêts des personnes concernées, puisque elle permet d'accroître la sécurité juridique. Ceci a été recommandé dans le cadre des signalements relatifs aux étrangers indésirables dans l'avis du CEPD sur le système SIS II⁸.
4. Le CEPD s'est penché sur la question de l'accès des services répressifs aux données du VIS dans un avis publié le 20 janvier 2006⁹. Il salue l'analyse que fait la Commission au point 6 de sa communication, aux termes de laquelle le seuil que doivent respecter les autorités chargées de la sécurité intérieure pour pouvoir interroger les bases de données recensant des personnes "innocentes" doit être sensiblement plus élevé que le seuil à respecter pour pouvoir interroger des bases de données criminelles. Le CEPD adhère bien évidemment à cette analyse, notamment si de nouveaux instruments permettant d'accéder à ces données étaient proposés. C'est un élément que le CEPD analysera en temps voulu de manière détaillée.
5. En ce qui concerne l'existence d'un système d'entrées-sorties des ressortissants de pays tiers, il convient de noter que l'étude d'analyse d'impact approfondie¹⁰ concernant la mise en place du VIS a rejeté l'idée d'un tel système et s'est prononcée en faveur de celui proposé aujourd'hui. Si la Commission entend changer son approche à ce sujet, cela rendrait nécessaire une nouvelle analyse d'impact comportant de solides arguments pour justifier qu'une option écartée un an auparavant (en raison notamment de "son impact important sur les droits de l'homme") est aujourd'hui considérée comme souhaitable.
6. La gestion des systèmes par une "structure unique", comme il est indiqué dans l'avis du CEPD sur le VIS, représente un important défi, qui ne pourra être relevé que si l'on en décrit les missions de manière exhaustive et claire et que celles-ci bénéficient d'un financement approprié.
7. Il est regrettable que dans un document aussi sensible la notion de système d'identification automatisé d'empreintes digitales (AFIS) soit décrit (point 5.3.1), à tort, comme le regroupement de "toutes les données relatives aux empreintes digitales qui ne sont actuellement disponibles que ...". Il s'agit d'un outil (logiciel) à des fins d'identification, et non pas d'une base de données à proprement parler. En revanche, la notion d'AFIS est correctement utilisée dans l'exemple cité au point 5.4 concernant les changements architecturaux et organisationnels.

8

http://europa.eu.int/eur-lex/lex/LexUriServ/site/fr/oj/2006/c_091/c_09120060419fr00380056.pdf

9

http://europa.eu.int/eur-lex/lex/LexUriServ/site/fr/oj/2006/c_097/c_09720060425fr00060010.pdf

10

Idem point 4

8. La brève démonstration de l'application du principe de proportionnalité à l'ADN est incomplète et ne peut conduire à la conclusion *simpliste* que ce principe sera respecté. La finalité du stockage de données, sa durée, les conditions d'accès etc. doivent également être pris en compte lors de l'analyse de ce principe. Ainsi que cela a déjà été précisé, le CEPD déconseille vivement l'utilisation de données biométriques, notamment de l'ADN, en tant que clés primaires pour ces bases de données, étant donné les risques que présente cette option. Dans son avis sur le principe de disponibilité, le CEPD préconise également quelques exigences générales en ce qui concerne les instruments légaux prévoyant des échanges de données relatives à l'ADN. Ces exigences doivent également être prises en considération dans le présent contexte.

Fait à Bruxelles le 10 mars 2006

Peter HUSTINX
Contrôleur européen de la protection des données