3

Société de l'information et protection des données

Google Street View, Facebook et d'autres médias sociaux se sont intégrés dans la vie quotidienne et dans la société de l'information ces dernières années. En 2010, plusieurs États membres de l'Union européenne (UE) ont fait part de préoccupations relatives à la protection des données, en relation avec ces évolutions. En outre, en 2010, les menaces en matière de sécurité nationale ont continué à influencer les mesures de sécurité prises dans les aéroports ; cela a donné lieu à de vifs débats au sein de l'UE, ainsi que dans certains États membres, particulièrement à propos des scanners corporels. La protection des données à caractère personnel a occupé, en 2010, au sein de l'UE, le premier plan dans de nombreux débats sur les droits fondamentaux liés aux propositions de réforme du cadre de protection des données de l'UE prenant en compte le traité de Lisbonne et le programme de Stockholm.

Ce chapitre traite de l'évolution des politiques de l'Union européenne (UE) et des États membres, ainsi que des pratiques dans le domaine de la société de l'information et de la protection des données en 2010. En premier lieu, il présente les préoccupations des tribunaux nationaux relatives au cadre de l'UE pour la protection des données, notamment la question de la conformité de la directive sur la conservation des données avec les droits fondamentaux, ainsi qu'il examine de manière plus générale la nécessité d'une réforme du cadre. Le chapitre décrit ensuite les préoccupations concernant l'indépendance, les pouvoirs ainsi que les ressources attribués aux autorités chargées de la protection des données dans les États membres. Enfin, réfléchissant au besoin de transparence dans la société de l'information, le chapitre prend en considération l'équilibre délicat qu'il convient de trouver entre la protection des données et le droit à l'information. Le chapitre conclut avec une évaluation de la mesure dans laquelle les objectifs en matière de protection des données ont été atteints en 2010, et la manière dont ils pourront l'être à l'avenir dans les domaines de la coopération en matière de police et de sécurité, des progrès technologiques et de la sécurité dans les aéroports.

Développements clés dans le domaine de la société de l'information et de la protection des données :

- les évolutions technologiques ont soulevé des questions nouvelles concernant les droits fondamentaux et suscité des demandes de modernisation de la législation européenne en matière de protection des données ;
- il a été de plus en plus communément admis que la protection des données constitue une question essentielle dans les accords internationaux, notamment ceux qui traitent des données des dossiers passagers (PNR, Personal name records) et Swift ;
- des inquiétudes ont été exprimées sur les plans politique et juridique face à l'imposition de plus en plus fréquente aux entreprises privées de retenir des données de communication (téléphone et Internet) ;
- le problème de l'indépendance des autorités chargées de la protection des données a été soumis à la Cour de justice de l'Union européenne (CJUE) ;
- les débats politiques se sont poursuivis quant aux conséquences de l'utilisation de scanners corporels comme systèmes de sécurité dans les aéroports ;
- la problématique de l'équilibre entre le souci de protéger les données et le droit à l'information a pris corps, et a été soumise à l'attention de la CJUE.

3.1. Réexamen du cadre actuel de la protection des données au sein de l'UE

La protection des données est explicitement reconnue dans l'article 8 de la Charte des droits fondamentaux de l'Union européenne comme un droit fondamental distinct. La Charte est le premier instrument international de protection des droits de l'homme à comporter pareille disposition. Le traitement des données à caractère personnel et la libre circulation de ces données sont également régis par la directive relative à la protection des données.[1] En outre, après l'adoption du traité de Lisbonne en décembre 2009, la Vice-présidente de la Commission européenne, Viviane Reding, a indiqué que la protection des données à caractère personnel des citoyens de l'Union ferait partie des domaines politiques prioritaires en 2010.

> *« J'aimerais citer ... les domaines prioritaires dans lesquels nous devons à mon avis montrer fermement que la politique de l'Europe change avec le traité de Lisbonne. Nous devons tout d'abord durcir la position de l'UE en matière de protection de la vie privée de nos concitoyens dans le cadre de toutes les politiques européennes. »*
>
> *Viviane Reding, Vice-présidente de la Commission européenne, 11 janvier 2010.*

La rapidité de l'évolution technologique et l'accélération de l'échange de données dans la société de l'information actuelle ont donné lieu à un fructueux débat sur le réexamen de la législation européenne qui date de 1995, et qui régit encore à ce jour la protection des données et de la vie privée. Le cadre régissant la protection des données au sein de l'UE est toujours basé sur le système pré-Lisbonne et reste par conséquent très hétérogène dans ses dispositions et dans sa mise en œuvre. La Commission européenne s'est engagée la première dans ce débat, en 2009, en lançant une consultation publique sur le futur cadre juridique pour la protection des données à caractère personnel dans l'UE.[2] En novembre 2010, la Commission européenne a publié une communication sur la protection des données à caractère personnel au sein de l'UE dans laquelle elle souligne les nouveaux défis à relever et indique qu'il est nécessaire de réviser les règles de protection des données dans les domaines de la coopération policière et judiciaire en matière pénale.[3] La Commission européenne avait précédemment publié une communication présentant une vue d'ensemble de la gestion de l'information dans le domaine de la liberté, de la sécurité et de la justice.[4] En 2010, le Conseil de l'Europe a également ouvert un débat sur la modernisation de son cadre en matière de protection des données : la Convention 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel.[5] Le Conseil de l'Europe cherche à déterminer si le cadre en matière de protection défini par la Convention 108 doit être modifié et complété afin de mieux répondre aux attentes légitimes des individus et professionnels concernées par la protection des données. À cette fin, le Conseil de l'Europe a lancé, à l'occasion du 30e anniversaire de la Convention 108, une consultation publique, afin de permettre à toutes les parties prenantes et les personnes intéressées de mettre en avant leurs points de vue en la matière. La modernisation de la Convention 108 devrait aussi mener à une surveillance meilleure de la mise en application de cette convention.

3.2. Conformité de la directive sur la conservation des données avec les principes des droits fondamentaux

En 2010, la Commission européenne a annoncé que la directive de 2006 sur la conservation des données, qui oblige les opérateurs téléphoniques et fournisseurs d'accès à Internet à collecter des données sur toutes les communications de leurs clients,[6] était en cours de réexamen.[7] Dans les États membres, certains étaient d'avis que la directive n'était pas en conformité avec les droits fondamentaux. Dans une lettre commune en date du 22 juin 2010, plus de cent organisations non gouvernementales (ONG) de 23 États membres ont demandé aux commissaires européens Cecilia Malmström, Viviane Reding et Neelie Kroes de « *proposer la suppression des prescriptions de l'UE en matière de conservation des données en faveur d'un système de conservation rapide et de collecte ciblée des données relatives aux communications* ». Selon cette lettre, une conservation généralisée des données porte atteinte au caractère confidentiel de certaines activités, comme les contacts avec les journalistes, les lignes de crises et les partenaires commerciaux, en les exposant à des risques de divulgation par des fuites et abus.[8] Des campagnes nationales contre l'application de la directive, largement couvertes par les médias, ont eu lieu en **Allemagne**, en **Autriche**, en **Belgique** et en **Bulgarie**. Fin 2009, le Rapporteur spécial des Nations Unies sur la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste a également exprimé son inquiétude à propos de la détérioration progressive de la protection de la vie privée.[9]

1 Directive 95/46/CE, JO 1995 L 281, pp. 31-50.
2 Pour un résumé des réponses à cette consultation, voir Commission européenne (2010a).
3 Commission européenne (2010b).
4 Commission européenne (2010c).
5 Conseil de l'Europe (2010).
6 Directive 2006/24/CE, JO 2006 L 105, p. 54.
7 Commission européenne (2010d).
8 Lettre jointe de plus de cent ONGs datée du 22 juin 2010, disponible sur : www.vorratsdatenspeicherung.de/images/DRletter_Reding.pdf.
9 Scheinin, M. (2009).

Le débat à propos du respect des droits fondamentaux par la directive sur la conservation des données a été alimenté par un certain nombre de décisions de cours constitutionnelles dans les États membres de l'UE. Dans sa décision nº 1258 du 8 Octobre 2009, la Cour constitutionnelle **roumaine** (*Curtea Constituțională*) a déclaré la législation nationale mettant en œuvre l'application de la directive anticonstitutionnelle.[10] En mars 2010, la Cour constitutionnelle fédérale allemande a annulé la législation allemande transposant la directive sur la conservation des données, la cour ayant a estimé que la législation menaçait gravement les droits relatifs à la vie privée.[11] À la suite de cette décision, le Commissaire fédéral allemand chargé de la protection des données et de la liberté de l'information (*Bundesbeauftragter für den Datenschutz und die Informationsfreiheit,* BfDI*)* a demandé aux entreprises allemandes de supprimer toutes les données collectées, vu le caractère anticonstitutionnel constaté. Selon le Commissaire fédéral allemand chargé de la protection des données et de la liberté de l'information, toutes les entreprises se sont conformées à cette demande. Dans une résolution commune, le Commissaire fédéral allemand chargé de la protection des données et de la liberté de l'information et les commissaires chargés de la protection des données au niveau des entités fédérées *(Länder)* ont exhorté le gouvernement fédéral allemand à soutenir la suppression de la directive sur la conservation des données.[12]

> *« Pour éviter tout danger, il découle du principe de proportionnalité que la récupération des données relatives aux télécommunications enregistrées en application du principe de précaution ne saurait être autorisée qu'en cas de risque concret suffisamment avéré pour la vie, l'intégrité physique ou la liberté d'une personne, pour l'existence ou la sécurité du gouvernement fédéral ou d'une entité fédérée (Land) ou afin d'écarter un danger commun ».*
>
> *Cour constitutionnelle allemande,* communiqué de presse, *2 mars 2010.*

En 2006, en **Irlande**, l'organisation non gouvernementale *Digital Rights Ireland* (DRI) a soumis à la Haute Cour (*An Ard-Chúirt*) une plainte concernant la directive proprement dite ainsi qu'à sa transposition dans le droit national. En juillet 2008, la Commission irlandaise pour les droits de l'homme (*An Coimisiún ul Chearta an Duine,* IHRC) a été autorisée par la Haute Cour à être considérée comme *amicus curiae* (amie de la cour – avis d'informateur bénévole et extérieur au procès) dans cette action. D'après le communiqué de presse de l'IHRC, « *cette affaire soulève des questions importantes, à savoir la mesure dans laquelle les lois et dispositions régissant la surveillance de nos vies privées par l'État, dans le cadre de l'élimination de la criminalité protègent suffisamment les droits de l'homme.* »[13] En mai 2010, la Haute Cour a estimé que DRI avait qualité pour agir (*locus standi)* dans cette affaire et a décidé de renvoyer la question de la validité de la directive à la Cour de justice de l'Union européenne (CJUE).[14]

Dans le même temps, la transposition de la directive sur la conservation des données était également retardée dans certains États membres à cause de doutes quant à sa conformité avec les droits fondamentaux. Même si la CJUE avait estimé en juillet 2010 que l'Autriche avait violé le traité de l'UE en ne transposant pas la directive avant le 15 mars 2009,[15] cette transposition a encore été retardée.[16] Au cours de la procédure devant la CJUE, l'Autriche a exprimé son inquiétude quant à la conformité de la directive avec les droits fondamentaux, en particulier avec l'article 8 de la Charte des droits fondamentaux de l'UE.[17] L'application de la directive sur la conservation des données a également été retardée en **Suède** en raison d'inquiétudes par rapport aux droits fondamentaux.

Pratique encourageante :

Consultation publique à propos d'un projet de loi transposant la directive sur la conservation des données

Entre le 15 novembre 2009 et le 15 janvier 2010, le gouvernement autrichien a mené une consultation publique à propos d'un projet de loi transposant la directive sur la conservation des données. Des organismes publics, des entités privées et des particuliers ont soumis, au total, 189 commentaires, le plus grand nombre jamais atteint dans le cadre d'une consultation publique sur un projet de loi en Autriche. La plupart de ces commentaires exprimaient des critiques quant à l'obligation imposée par la directive de conserver les données relatives au trafic, à la localisation et à l'abonné traitées dans des services ou réseaux de communication électronique accessibles au public.

Une liste de tous les commentaires reçus lors de la consultation sur le projet de loi peut etre consultée sur le site du parlement autrichien : http://www.parlinkom.gv.at/PAKT/VHG/XXIV/ME/ME_00117/ index.shtml

3.3. Autorités chargées de la protection des données : indépendance, pouvoirs et ressources

L'article 28 de la directive sur la protection des données stipule qu'une autorité publique chargée de surveiller l'application de la directive doit être mise en place dans chaque État membre de l'UE. En 2010, l'indépendance, les pouvoirs et les ressources des autorités chargées de la protection des

10 Roumanie, *Curtea Constituțională* (2009).
11 Allemagne, *Bundesverfassungsgericht* (2010).
12 Allemagne, BfDI (2010a).
13 European Digital Rights (2008).
14 Irlande, *Digital Rights Ireland Ltd. v. Minister for Communication, Marine and Natural Resources and others*, High Court, McKechnie J., unreported, 5 Mai 2010.
15 CJUE, C-189/09, *Commission c. Autriche*, 29 juillet 2010.
16 Autriche, *Justizministerium* (2010).
17 CJUE, C-189/09, *Commission c. Autriche*, 29 juillet 2010.

données dans les États membres de l'UE sont apparus comme des questions essentielles. La FRA a traité ces problèmes en détail dans un rapport, publié au mois de mai 2010, sur la protection des données dans l'Union européenne et le rôle des autorités nationales chargées de la protection des données.

3.3.1. Indépendance

Dans l'affaire *Commission c. Allemagne*, la CJUE a examiné pour la première fois la question de l'indépendance des autorités de contrôle de la protection des données. En appliquant des critères stricts, la CJUE a estimé que les institutions allemandes de contrôle de la protection des données à l'échelle des entités fédérées *(Länder)*, responsables de la surveillance du traitement des données à caractère personnel par des organismes non publics, n'étaient pas suffisamment indépendantes car elles étaient sous tutelle de l'État.[18] Il s'agissait, pour la CJUE, de se prononcer sur l'interprétation de l'article 28, paragraphe 1, de la directive sur la protection des données stipulant que les autorités chargées de la protection des données « *exercent en toute indépendance les missions dont elles sont investies* ».

> *« Il y a lieu d'interpréter la Directive n° 95/46 en ce sens que les autorités de contrôle compétentes pour la surveillance du traitement des données à caractère personnel dans le secteur non public doivent jouir d'une indépendance qui leur permette d'exercer leurs missions sans influence extérieure. Cette indépendance exclut non seulement toute influence exercée par les organismes contrôlés, mais aussi toute injonction et toute autre influence extérieure, que cette dernière soit directe ou indirecte, qui pourraient remettre en cause l'accomplissement, par lesdites autorités, de leur tâche consistant à établir un juste équilibre entre la protection du droit à la vie privée et la libre circulation des données à caractère personnel. »*
>
> *CJUE, C-518/07,* Commission c. Allemagne*, 9 mars 2010, pt 30.*

Dans ses conclusions, l'avocat général Mazák a qualifié le terme « indépendance » de relatif par nature, dans la mesure où il est nécessaire que le législateur précise le degré de cette indépendance, élément non encore défini. En suivant cette logique, l'avocat général conclut que les autorités allemandes de protection des données en question sont suffisamment indépendantes, bien que soumises à la tutelle de l'État.[19] La CJUE, d'un avis contraire, a rejeté cette argumentation et souligné que la directive devait être interprétée conformément au sens habituel des termes, optant ainsi pour une définition stricte du terme « indépendance ». La CJUE a également fait observer que le terme « indépendance » était complété dans la directive par la locution « en toute » et qu'il convenait donc de l'entendre au sens large.

En décembre 2010, la Commission européenne a assigné l'**Autriche** devant la CJUE pour défaut d'indépendance de son autorité chargée de la protection des données. La loi autrichienne en matière de protection des données stipule que les autorités concernées exercent leurs fonctions de manière indépendante et ne reçoivent aucune instruction dans l'exercice de celles-ci. La Commission considère que l'exercice des missions « en toute indépendance » n'est pas garanti dans la mesure où l'autorité est intégrée à la Chancellerie fédérale, où le Chancelier a le droit d'être informé à tout moment de toutes les questions relatives à la gestion quotidienne de l'autorité.[20]

3.3.2. Pouvoirs

Le 24 juin 2010, la Commission européenne a demandé au **Royaume-Uni** de suivre les prescriptions du droit de l'UE en renforçant les pouvoirs de l'autorité nationale chargée de la protection des données, le Bureau du commissaire à l'information (*Information Commissioner's Office,* ICO).[21] La Commission européenne a demandé à ce que l'ICO ait le pouvoir de conduire des contrôles aléatoires de conformité avec la législation sur la protection des données, d'appliquer des sanctions, et de vérifier le niveau de protection des données du pays destinataire avant tout transfert international de données effectué à partir du Royaume-Uni.[22] La Commission européenne analyse actuellement la réponse du Royaume-Uni aux allégations soulevées.

ACTIVITÉS DE LA FRA :

Comparaison entre les autorités nationales chargées de la protection des données

En mai 2010, la FRA a publié un rapport sur la protection des données dans l'Union européenne et le rôle des autorités nationales chargées de la protection des données, intitulé *Data protection in the European Union : the role of National Data Protection Authorities (Strengthening the fundamental rights architecture in the EU II)*. Ce rapport propose une comparaison des pouvoir et de l'indépendance des autorités chargées de la protection des données au sein de l'UE et met en évidence le manque d'indépendance, de pouvoirs et de ressources des autorités chargées de la protection des données dans certains États membres.

FRA (2010), Data Protection in the European Union : The Role of National Data Protection Authorities – Strengthening the Fundamental Rights Architecture II*, disponible sur : http://fra.europa.eu/fraWebsite/research/publications/publications_en.htm*

3.3.3. Ressources

Les ressources des autorités chargées de la protection des données sont un élément essentiel de leur fonctionnement

18 CJUE, C-518/07, *Commission c. Allemagne*, 9 Mars 2010.
19 *Ibid.*
20 Commission européenne (2010e).
21 Commission européenne (2010f).
22 Royaume-Uni, *Information Commissioner's Office* (2010).

en tant que gardiennes des droits fondamentaux. Néanmoins, en 2010, à la suite de la crise financière, les budgets ont été réduits dans de nombreux États membres de l'UE. Les informations figurant ci-dessous ne sont pas directement comparables mais peuvent tout de même indiquer certaines tendances.

Les pays suivants ont indiqué une réduction significative des ressources humaines et/ou financières pendant la période considérée : **Estonie** (diminution de 12,5 % des ressources financières entre 2008 et 2010), **Irlande** (en 2008, EUR 2,04 millions ; en 2009, EUR 1,81 million ; en 2010, EUR 1,21 million), **Lettonie** (en 2008, 25 personnes ; en 2009, 16 personnes ; en 2010 : 19 personnes ; en 2008 : EUR 730 984 ; en 2009, EUR 476 984 ; en 2010, EUR 381 295), **Lituanie** (les réductions de personnel n'ont pas été précisées mais la masse salariale a été réduite de 69 %, passant de LTL 2 929 000 (EUR 848 690 au 31 décembre 2010) à LTL 1 886 000 (EUR 546 477) ; réduction budgétaire de 64,6 %), **Slovaquie** (pas de modification des ressources humaines ; en 2008 : EUR 960 850 ; en 2010 : EUR 728 696).

En revanche, la **France** et l'**Allemagne** déclarent avoir augmenté de façon significative les ressources humaines et financières entre 2007 et 2010.[23] En **Espagne** l'autorité chargée de la protection des données (*Agencia Española de Protección de Datos*) connaît une tendance similaire, le nombre des employés passant de 99 en 2007 à 155 en 2009. Son budget a également été augmenté de EUR 13,44 millions en 2008, à EUR 15,32 millions en 2009[24].

Enfin, les pays suivants déclarent ne pas avoir modifié ou n'avoir modifié que légèrement les ressources humaines et financières pendant l'année 2010 : **Autriche, Bulgarie, Chypre, Finlande, Grèce, Hongrie, Italie, Malte, Pologne, Roumanie, Royaume-Uni** et **Slovénie.**

3.4. Protection des données et transparence dans la société de l'information

En matière de droits fondamentaux, il est souvent nécessaire et difficile de trouver un équilibre entre des intérêts concurrents. Dans le cas de la protection des données, il s'agit de l'équilibre entre le droit à la protection des données à caractère personnel et le droit à l'information. La CJUE s'est prononcée sur cette question en 2010 dans le cadre de la garantie de la transparence.

En juin 2010, dans l'affaire *Commission c. Bavarian Lager*, la CJUE s'est penchée sur la question du champ d'application de la protection des données à caractère personnel dans le cadre de l'accès aux documents des institutions de l'UE.[25] Dans cette affaire, la Commission avait autorisé l'accès au procès-verbal d'une réunion mais en occultant cinq noms. Le requérant avait demandé l'accès au document complet sans pouvoir justifier que ce type de données à caractère personnel lui soient communiquées. Par conséquent, la CJUE a confirmé la décision de la Commission de refuser l'accès au document complet.

Il est également intéressant de mentionner les affaires jointes C-92/09 et C-93/09 examinées par la Grande Chambre de la CJUE en novembre 2010, puisqu'il s'agissait d'apprécier si la législation de l'Union respectait les droits fondamentaux.[26] Cette affaire concernait la législation de l'UE en matière de politique agricole qui stipule que les États membres doivent assurer annuellement la publication *ex-post* du nom des bénéficiaires et des montants versés par le Fonds européen agricole de garantie (FEAGA) et le Fonds européen agricole pour le développement rural (FEADER).[27] Les requérants avaient demandé au tribunal administratif de Wiesbaden de demander à l'entité fédérée *(Land)* allemande de Hesse de ne pas publier les données les concernant. Le tribunal de Wiesbaden avait donc soumis l'affaire à la CJUE. La CJUE a estimé que, dans une démocratie, les contribuables ont le droit légitime d'être informés de l'utilisation des fonds publics. Parallèlement, la CJUE a également estimé que la publication des données sur un site internet où figurent le nom des bénéficiaires des aides du FEAGA et du FEADER ainsi que le montant précis de ces aides constituent une ingérence dans le droit au respect de la vie privée en général, et de la protection des données à caractère personnel en particulier. La CJUE a conclu que la publication des données à caractère personnel de chacun des bénéficiaires de l'aide du FEAGA et du FEADER n'était pas suffisamment proportionnée parce non strictement nécessaire pour atteindre l'objectif de transparence recherché. La CJUE a donc déclaré certaines dispositions du Règlement n° 1290/2005 et du Règlement n° 259/2008 nulles, invalidant ainsi la législation de l'UE au motif du respect des droits fondamentaux.

3.5. Nouveaux défis

3.5.1. Protection des données et coopération en matière de police et de sécurité

Le traité de Lisbonne a aboli la division préalable de l'UE en trois piliers distincts, et étendu le champ d'application de la procédure législative ordinaire à la coopération policière et judiciaire en matière pénale. En outre, les pouvoirs du Parlement européen ont été considérablement renforcés en ce qui concerne la conclusion d'accords internationaux, qui a eu des répercussions importantes sur la protection des données.

23 Sauf indication contraire ces données ont été fournies par le réseau d'experts juridiques de l'Agence, FRAlex.
24 Espagne, Agencia Española de Protección de Datos (2008), p. 84 et (2009), p. 92.
25 CJUE, C-28/08 P, *Commission c. Bavarian Lager*, 29 juin 2010.
26 CJUE, affaires jointes C-92/09 et C-93/09, *Eifert, Schecke c. Land Hessen,* 9 Novembre 2010.
27 Règlement (CE) n° 1290/2005 du Conseil, JO 2007 L 322, p. 1 et Règlement (CE). No259/2008 de la Commission, JO 2008 L 76, p. 28.

En février 2010, le Parlement européen a utilisé ses nouveaux pouvoirs en refusant de donner son approbation à la conclusion d'un accord intérimaire signé le 30 novembre 2009 entre l'UE et les États-Unis sur le traitement et le transfert de données de messagerie financière de l'UE vers les États-Unis (Accord Swift I). Le Parlement a invoqué le fait que cet accord n'offrait pas une protection suffisante des données à caractère personnel des citoyens de l'UE.[28] Le 8 juillet 2010, après avis du Contrôleur européen de la protection des données (CEPD),[29] le Parlement européen a donné son approbation à l'accord révisé[30] dont la conclusion formelle a eu lieu le 13 juillet 2010.[31]

La question des droits fondamentaux a également soulevé des inquiétudes quant à la signature d'accords internationaux sur l'échange des données des dossiers des passagers (PNR). Le 1er mars 2010, une ONG belge des droits de l'homme (Ligue des droits de l'homme) a porté une affaire devant la Cour constitutionnelle belge en faisant valoir que la législation nationale du 30 novembre 2009 appliquant l'accord de 2007 entre l'UE et les États-Unis sur les PNR violait les normes en matière de protection des données.[32] Le 5 mai 2010, le Parlement européen a adopté une résolution[33] stipulant qu'il convenait de procéder à une évaluation de l'impact sur la vie privée et un test de proportionnalité avant d'adopter toute nouvelle législation européenne sur le transfert des données PNR.

En septembre 2010, la Commission européenne a adopté un ensemble de propositions sur l'échange de données PNR avec des pays tiers,[34] qui comprend une stratégie extérieure de l'UE en matière de dossiers passagers et des recommandations relatives à des directives de négociation en vue de la conclusion de nouveaux accords PNR avec l'Australie, le Canada et les États-Unis.[35] Cette stratégie vise à assurer un niveau de protection élevé des données lors de l'échange de données PNR avec des pays tiers.[36]

3.5.2. Défis technologiques

Les préoccupations en matière de droits fondamentaux posés par les évolutions technologiques figuraient en très bonne place sur l'agenda du Conseil de l'Europe pendant la période concernée. En 2010, le Comité des Ministres du Conseil de l'Europe a adopté un ensemble de déclarations et de recommandations concernant ce sujet : une déclaration sur la stratégie numérique pour l'Europe ;[37] une déclaration sur la neutralité du réseau ;[38] une déclaration sur la gestion dans l'intérêt public des ressources représentées par les adresses du protocole internet ;[39] une déclaration sur une participation accrue des États membres aux questions de gouvernance de l'Internet – le Comité consultatif gouvernemental (GAC) de l'Internet Corporation for Assigned Names and Numbers (ICANN).[40] De plus, l'Assemblé parlementaire du Conseil de l'Europe a adopté la Recommandation 1906(2010)1 : Repenser les droits des créateurs à l'ère d'Internet.[41]

Les nouveaux défis technologiques ont provoqué des débats en matière de droits fondamentaux dans les États membres de l'UE. *Google Street View* est un service proposé par la société des technologies de l'information Google qui offre des vues panoramiques prises sous différents angles dans les rues de nombreuses villes du monde. À cet effet, des voitures spécialement équipées par Google sillonnent les villes de l'UE et au-delà pour rassembler des photos. Cependant, au cours de ces opérations, la société informatique avait, selon la déclaration de Google, collecté par inadvertance des données à caractère personnel transmises sur des réseaux Wi-Fi non sécurisés.

Le 21 mai 2010, la Commission **autrichienne** pour la protection des données (*Österreichische Datenschutzkommission*, DSK) a donc imposé une interdiction temporaire de la collecte de données par les voitures *Google Street View* et a ouvert une enquête. Fin novembre 2010, cette interdiction temporaire a été levée, mais l'enquête sur les procédures de *Google Street View* continue.[42] Des procédures similaires ont été déclenchées dans de nombreux pays, dont l'**Espagne,**[43] l'**Italie,**[44] et la **Slovénie**.[45]

En **Allemagne**, le débat s'est axé sur le droit à contester les photos prises par *Google Street View*. En août 2010, la filiale allemande de *Google* a accepté de prendre en compte les objections des personnes, qu'il est possible de déposer en ligne,[46] contre la publication de photos de maisons privées et de personnes dans ses services *Street View.* Le Commissaire de Hambourg chargé de la protection des données (*Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit*, HmbBfDI) a publié une brochure d'information[47] et un formulaire[48] pour soumettre des réclamations. En outre, le Commissaire fédéral chargé de la protection des données et de la liberté d'information a exigé la création d'un registre central des réclamations concernant la publication de données à caractère personnel sur Internet, notamment par les services comme *Google Street View*.[49] La seconde chambre du parlement fédéral allemand (*Bundesrat*) a adopté un projet de loi amendant la loi fédérale sur la protection des don-

28 Parlement européen (2010a).
29 Contrôleur européen de la protection des données (CEPD) (2010).
30 Parlement européen (2010b).
31 Décision 2010/412/UE du Conseil JO 2010 L 195, p. 3.
32 Belgique, La Ligue des droits de l'Homme (LDH).
33 Parlement européen (2010c).
34 Commission européenne (2010g).
35 Commission européenne (2010h).
36 Agence des droits fondamentaux de l'Union européenne (FRA) (2008).
37 Conseil de l'Europe, Comité des Ministres (2010a).
38 Conseil de l'Europe, Comité des Ministres (2010b).
39 Conseil de l'Europe, Comité des Ministres (2010c).
40 Conseil de l'Europe, Comité des Ministres (2010e).
41 Conseil de l'Europe, Assemblée parlementaire (2010).
42 Autriche, *Österreichischen Datenschutzkommission* (DSK).
43 Espagne, *Agencia Española de Prótección de Datos*.
44 Italie, *Garante Per la Protezione Dei Dati Personali*.
45 Slovénie, *Informacijski Pooblascenec*.
46 Allemagne, *Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit* (HmbBfDI) (2010a).
47 Allemagne, HmbBfDI (2010b).
48 Allemagne, *Das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein* (ULD).
49 Allemagne, BfDI (2010b).

nées (*Bundesdatenschutzgesetz*, BDSG) afin de garantir une meilleure protection des données à caractère personnel par rapport aux services d'information géographique sur Internet comme *Google Street View*.[50] Dans un communiqué de presse du 18 août 2010, le gouvernement fédéral allemand (*Bundesregierung*) semble se prononcer en faveur d'une réforme globale de la loi sur la protection des données en ligne et ferait une proposition dans ce sens.[51]

Le 7 juillet 2010, le Commissaire chargé de la protection des données de Hambourg a ouvert une enquête contre *Facebook* à propos de la collecte de données sur des contacts de messagerie et de téléphonie mobile et de la création de profils de contact à des fins de marketing visant des personnes n'utilisant pas *Facebook* via les carnets d'adresses d'utilisateurs enregistrés.[52] Cette procédure pourrait se solder par une amende. C'est la première fois que ce type de procédure est intenté contre *Facebook* en Europe.

« La plupart des 75 % des jeunes européens qui se connectent sont des utilisateurs enthousiastes des sites des réseaux sociaux ... Cependant, la publication d'informations personnelles ou de photos peut conduire à des situations embarrassantes, voire traumatisantes. Les jeunes ne sont pas toujours conscients du risque que les images en ligne et les vidéogrammes puissent circuler contre leur gré et à leur insu. »

Viviane Reding, Vice-présidente de la Commission européenne, 9 février 2010.

Le rôle de *Facebook* dans les campagnes électorales a même fait l'objet de discussions en **Bulgarie** en 2010. Le 22 juin 2010, plusieurs membres du parti au pouvoir en Bulgarie ont proposé des dispositions introduisant des restrictions concernant les campagnes électorales sur Internet. Leur objectif principal consistait à comparer les informations fournies via des médias électroniques, blogs et réseaux sociaux comme *Facebook* et *Twitter* avec les informations fournies plus traditionnellement par la presse écrite, la radio et la télévision. Normalement, les mêmes règles doivent s'appliquer aux deux formes de médias quant à la couverture des campagnes électorales. En réponse à cette proposition, les partis de l'opposition ont exprimé leur préoccupation et ont déclaré que ces mesures constitueraient une violation de la liberté d'expression et équivaudrait à contrôler l'Internet.[53]

3.5.3. Scanners corporels

Les mesures de sécurité appliquées dans les aéroports, en particulier l'utilisation de scanners corporels, semblent avoir dominé les débats sur la protection des données dans l'UE en 2010. D'ailleurs, après la tentative d'attentat visant à détruire un avion à l'aide d'explosifs dissimulés sur un vol Amsterdam-Détroit le 25 décembre 2009, le débat sur les différents types de scanners corporels utilisés dans les aéroports a pris une dimension plus importante dans le calendrier politique. Le sujet a suscité beaucoup d'attention de la part des médias et il a été allégué que l'affichage sur écran de photos du corps nu de la personne passant dans le scanner constituait une violation de l'exercice du droit au respect de la vie privée. Le 15 juin 2010, la Commission européenne a publié sa communication relative à l'utilisation de scanners de sûreté dans les aéroports de l'UE, faisant valoir que seule une solution au niveau de l'UE pourrait garantir une application uniforme des règles et des normes de sécurité, un facteur essentiel « *pour assurer à la fois le niveau le plus élevé de sûreté aérienne et la meilleure protection possible des droits fondamentaux et de la santé des citoyens de l'UE* ».[54] Dans ce contexte, la Commission européenne a souligné l'importance de certaines dispositions de la Charte des droits fondamentaux de l'Union européenne, y compris la dignité humaine (Article 1), le respect de la vie privée et familiale (Article 7), la protection des données à caractère personnel (Article 8), la liberté de pensée, de conscience et de religion (Article 10), la non-discrimination (Article 21), les droits de l'enfant (Article 24) et enfin un niveau élevé de protection de la santé humaine dans la définition et la mise en œuvre de toutes les politiques et actions de l'UE (Article 35).

Cette question a également été abordée lors de la Conférence des commissaires à la protection des données et de la vie privée qui s'est tenue à Prague en avril 2010. Les commissaires ont adopté une résolution stipulant que les principes et les garanties en matière de protection des données ainsi que le principe de la protection de la vie privée dès la conception doivent être pris en compte afin de statuer sur l'utilisation de scanners corporels.[55]

La Cour européenne des droits de l'homme (CouEDH) s'est référée aux mesures de sécurité dans les aéroports dans l'affaire *Gillan et Quinton c. Royaume-Uni*.[56] Cette affaire concernait les contrôles et les fouilles effectués par la police au Royaume-Uni. Le gouvernement britannique soutenait que les contrôles et fouilles ne constituaient pas une violation du droit à la vie privée dans la mesure où ils équivalaient aux fouilles auxquelles les passagers sont régulièrement soumis dans les aéroports.[57] La CouEDH a rejeté cet argument en faisant observer que les passagers se soumettent habituellement et volontairement à des fouilles parce qu'ils choisissent de prendre l'avion et connaissent l'existence de ces fouilles alors que ce choix n'existe pas dans le cadre des contrôles et fouilles de police, susceptibles de se produire en tout lieu et à tout moment.[58] L'opportunité d'appliquer ce raisonnement aux scanners corporels peut être débattu car que ces derniers vont au-delà des fouilles habituelles.

Des débats sur les scanners corporels et les problèmes par rapport à la protection des données ont également eu lieu

50 Allemagne, Bundestag (2010).
51 *Ibid.*, p. 15.
52 Hamburg.de (2010).
53 Bulgarie, Българският хелзинкски комитет (2010).
54 Commission européenne (2010i).
55 Commissaires à la protection des données et à la vie privée (2010).
56 Cour européenne des droits de l'homme, *Gillan et Quinton c. Royaume Uni*, nº 4158/05, 12 Janvier 2010.
57 *Ibid.*, paragraphe 60.
58 *Ibid.*, paragraphe 64.

en 2010 dans d'autres États membres de l'UE, par exemple en **Allemagne**,[59] en **Espagne**[60] et en **France**.[61]

ACTIVITÉS DE LA FRA :

Les scanners corporels et les droits fondamentaux

En juillet 2010, la FRA a publié un document de travail sur l'utilisation des scanners corporels, reprenant 10 questions et 10 réponses, intitulé *The use of body scanners : 10 questions and answers*. Ce docment identifie les droits fondamentaux auxquels l'utilisation des scanners corporels risque de porter atteinte. Ce document propose également une réflexion sur les nécessités et considérations spécifiques qu'il convient de prendre en compte lors de discussions sur l'introduction de ce type d'appareils dans les aéroports européens. Il examine les conditions qu'il conviendrait d'appliquer afin de répondre aux préoccupations concernant le respect des droits fondamentaux. L'Agence a présenté les conclusions de ce document au cours d'une séance tenue au Comité économique et social européen en janvier 2011.

FRA (2010), The Use of Body Scanners : 10 Questions and Answers*, disponible sur : http://fra.europa.eu/fraWebsite/research/publications/publications_en.htm.*

Perspectives

Les évolutions technologiques continuent de façonner nos vies et génèrent des inquiétudes quant au respect des droits fondamentaux. Facebook, Google Street View et les scanners corporels vont probablement rester à l'ordre du jour et alimenter l'important débat en cours sur la modernisation du cadre de protection des données de l'UE. Deux problématiques, avec en toile de fond le traité de Lisbonne, prendront une place centrale dans un avenir proche : le respect des normes relatives aux droits fondamentaux (par exemple en matière de conservation des données) et l'extension possible du champ d'application du cadre général de protection des données aux domaines de la coopération policière et judiciaire en matière pénale. Cela influera probablement sur la manière dont la protection des données est traitée à l'intérieur comme à l'extérieur de l'UE. D'ailleurs, le débat sur la protection des données continuera probablement à occuper, dans les années à venir, une place de plus en plus centrale dans le discours sur les droits fondamentaux au sein de l'UE.

59 Allemagne, BfDI (2010a) ; Allemagne, BFDI (2010b).
60 Pour un débat d'experts sur l'utilisation des scanners corporels dans les aéroports voir le site de l'Agence de Protection des Données de Madrid : www.dataprotectionreview.eu.
61 France, Commission nationale de l'informatique et des libertés (CNIL) (2010).

Références

Agence de protection des données de Madrid, site web : www.dataprotectionreview.eu

Agence des droits fondamentaux de l'Union européenne (FRA) (2008), *Opinion of the European Union Agency for Fundamental Rights on the Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) data for law enforcement purposes,* Vienne, 28 Octobre 2008.

FRA (2010), *Data Protection in the EU : the role of National Data Protection Authorities - Strengthening the fundamental rights architecture in the EU II*, Luxembourg, Office des publications de l'Union européenne, 7 Mai 2010.

FRA (2010), *The use of body scanners : 10 questions and answers,* Luxembourg, Office des publications de l'Union europeenne, juillet 2010.

Allemagne, *Bundestag* (2010), Entwurf eines Gesetzes zur Änderung des Bundesdatenschutzgesetzes, Publikation/Bt-Drs. 17/2765, 18 août 2010.

Allemagne, *Bundesverfassungsgericht*, Pressemitteilung Nr. 11/2010, Konkrete Ausgestaltung der Vorratsdatenspeicherung nicht verfassungsgemäß, 2 mars 2010.

Allemagne, Bundesbeauftragter für den Datenschutz und die Informationsfreiheit, BfDI (2010a), « Vorratsdatenspeicherung ».

Allemagne, BfDI (2010b), « Google Street View : Schaar fordert Schaffung eines Widerspruchsregisters und Profilbildungsverbot », 18 août 2010.

Allemagne, BfDI (2010c), « Diskretionszone für Körperscanner gewährleisten! », Bonn, 24 novembre 2010.

Allemagne, *Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit* (HmbBfDI) (2010a), « Vorabwiderspruch gegen Veröffentlichungen in Google Street View : So funktioniert's », Hambourg, 13 août 2010.

Allemagne, HmbBfDI (2010b), Aus den Augen, aus dem Sinn ... Information zur Umsetzung des Vorabwiderspruchs gegen Abbildungen im Internetdienst Google Street View, Hambourg.

Allemagne, *Das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein* (ULD).

Autriche (2010), *Österreichischen Datenschutzkommission* (DSK) (2010), « Neue Entwicklungen betreffend Google Street View? ».

Autriche, *Justizministerium* (2010), « Vorratsdaten : Justizministerium prüft Vorschlag », 27 juillet 2010.

Autriche, Telekommunikationsgesetz 2003, Änderung (117/ME).

Belgique, La Ligue des droits de l'Homme (LDH), « PNR, l'oeil de Washington » disponible sur : www.liguedh.be/index.php?option=com_content&view=article&id=854:pnr--lildewashington&catid=110:communiques-de-presse-2010&Itemid=283.

Bulgarie, Българският хелзинкски комитет (2010), ДПС е против опитите да се наложи чрез изборното законодателство контрол върху Интернет, 22 juin 2010.

Commission européenne (2010a), Résumé des réponses à la consultation publique sur le futur cadre juridique pour la protection des données à caractère personnel dans l'Union européenne, Bruxelles, 4 novembre 2010.

Commission européenne (2010b), Une approche globale de la protection des données à caractère personnel dans l'Union européenne, COM(2010) 609 final, Bruxelles, 4 novembre 2010.

Commission européenne (2010c), Présentation générale de la gestion de l'information dans le domaine de la liberté, de la sécurité et de la justice, COM(2010) 385 final, Bruxelles, 20 juillet 2010.

Commission européenne (2010d), « Protection des données : la Commission européenne présente sa stratégie pour renforcer les règles de l'Union en la matière », IP/10/1462, Bruxelles, 4 novembre 2010.

Commission européenne (2010e), « Protection des données : la Commission s'apprête à assigner l'Autriche devant la Cour de justice pour défaut d'indépendance de son autorité chargée de la protection des données », IP/10/1430, Bruxelles, 28 octobre 2010.

Commission européenne (2010f), « Protection des données : la Commission demande au Royaume Uni de renforcer les pouvoirs de l'autorité nationale chargée de la protection des données, comme le prescrit le droit de l'Union européenne », IP/10/811, Bruxelles, 24 juin 2010.

Commission européenne (2010g), Communication de la Commission européenne relative à la démarche globale en matière de transfert des données des dossiers passagers (PNR) aux pays tiers, COM(2010) 492, Bruxelles, 21 septembre 2010.

Commission européenne (2010h), « La Commission européenne adopte une stratégie extérieure de l'UE relative aux dossiers passagers », IP/10/1150, Bruxelles, 21 septembre 2010.

Commission européenne (2010i), Communication de la Commission au Parlement européen et au Conseil relative à l'utilisation de scanners de sûreté dans les aéroports de l'UE, COM(2010) 311 final, Bruxelles, 15 juin 2010.

Conseil de L'Europe (2010) La réponse du Conseil de l'Europe aux défis de la vie privée dans la modernisation de la Convention 108, Jérusalem, 27-29 octobre 2010.

Conseil de l'Europe, Assemblée parlementaire (2010) Recommandation 1906(2010) 1 Repenser les droits des créateurs à l'ère d'internet, Strasbourg, 12 mars 2010.

Conseil de L'Europe, Comité des Ministres (2010a), Déclaration du Comité des Ministres sur la stratégie numérique pour l'Europe, Strasbourg, 29 septembre 2010.

Conseil de L'Europe, Comité des Ministres (2010b), Déclaration du Comité des Ministres sur une participation accrue des Etats membres aux questions de gouvernance de l'Internet – Comité consultatif gouvernemental (GAC) de l'Internet Corporation for Assigned Names and Numbers (ICANN), Strasbourg, 26 mai 2010.

Conseil de L'Europe, Comité des Ministres (2010c), Déclaration du Comité des Ministres sur la neutralité du réseau, Strasbourg, 29 septembre 2010.

Conseil de L'Europe, Comité des Ministres (2010d), Déclaration du Comité des Ministres sur la gestion dans l'intérêt public des ressources représentées par les adresses du protocole internet, Strasbourg, 29 septembre 2010.

Conseil de L'Europe, Comité des Ministres (2010e), Recommandation CM/Rec(2010)13 du Comité des Ministres aux Etats membres sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage, Strasbourg, 23 novembre 2010.

Contrôleur européen de la protection des données (2010), Avis du Contrôleur européen de la protection des données sur la proposition de décision du Conseil relative à la conclusion de l'accord entre l'Union européenne et les États-Unis d'Amérique sur le traitement et le transfert de données de messagerie financière de l'Union européenne aux États-Unis aux fins du programme de surveillance du financement du terrorisme (TFTP II), 22 juin 2010, JO 2010 C 355, p. 10.

Cour européenne des droits de l'homme, *Gillan et Quinton c. Royaume Uni*, nº 4158/05, 12 Janvier 2010.

Cour de justice de l'Union européenne (CJUE), C-189/09, *Commission c. Autriche*, 29 juillet 2010.

CJUE, C-518/07, *Commission c. Allemagne*, 9 mars 2010.

CJUE, C-28/08 P, *Commission c. Bavarian Lager*, 29 juin 2010.

CJUE, affaires jointes C-92/09 et C-93/09, *Schecke et Eifert c. Land Hessen,* 9 novembre 2010.

Commissaires à la protection des données et à la vie privée (2010), Resolution on the use of body scanners for airport security purpose adopted by the European Privacy and Data Protection, Commissioners' Conference, Prague, 29-30 avril 2010.

Décision du Conseil du 13 juillet 2010 relative à la conclusion de l'accord entre l'Union européenne et les États-Unis d'Amérique sur le traitement et le transfert de données de messagerie financière de l'Union européenne aux États-Unis aux fins du programme de surveillance du financement du terrorisme, Bruxelles, JO 2010 L 195, 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, JO 1995 L 281, pp. 31-50.

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

Espagne, *Agencia Española de Protección de Datos* (2008) *Memoria 2008*, Madrid : Agencia Española de Protección de Datos.

Espagne, *Agencia Española de Protección de Datos* (2009), *Memoria 2009*, Madrid : Agencia Española de Protección de Datos.

European Digital Rights (2008), « Irish Human Rights Commission added to data retention challenge », Newsletter EDRI-gram, nº 6.14, 16 juillet 2008.

France, Commission nationale de l'informatique et des libertés (CNIL) (2010), Body scanner : quel encadrement en France et en Europe, 8 juin 2010.

Hamburg.de (2010), « Bußgeldverfahren gegen Facebook wegen Speicherung der Daten Dritter », 7 juillet 2010.

Irlande, *Digital Rights Ireland Ltd. v. The Minister for Communication, Marine and Natural Resources and others*, 5 Mai 2010.

Italie, *Garante Per la Protezione Dei Dati Personali*, « Excerpts From The Italian Dpa's Decision Regarding Google Streetview Information Obligations Applying To Google Inc. », communiqué de presse, 15 Octobre 2010.

Parlement européen (2010a), « SWIFT : les données bancaires des Européens traverseront-elles l'Atlantique ? » 5 février 2010.

Parlement européen (2010b), « Accord UE/États-Unis : traitement et le transfert de données de messagerie financière aux fins du programme de surveillance du financement du terrorisme », Procédure terminée NLE/2010/0178.

Parlement européen (2010c), Résolution du Parlement européen du 5 mai 2010 sur le lancement des négociations sur les accords relatifs aux données des passagers aériens (PNR) avec les États-Unis, l'Australie et le Canada, P7_TA-PROV(2010)0144, Bruxelles, 5 mai 2010.

Reding V., (2010) « Opening remarks at the European Parliament hearing in the Parliament's Committee on Civil Liberties, Justice and home Affairs (LIBE) », 11 janvier 2010.

Reding V. (2010), « Think before you post! How to make social networking sites safer for children and teenagers? » Safer Internet Day, Strasbourg, 9 février 2010.

Règlement (CE) nº 259/2008 de la Commission du 18 mars 2008 portant modalités d'application du règlement (CE) nº 1290/2005 du Conseil en ce qui concerne la publication des informations relatives aux bénéficiaires de fonds en provenance du Fonds européen agricole de garantie (FEAGA) et du Fonds européen agricole pour le développement rural, JO 2008 L 76, p. 28.

Règlement (CE) nº 1437/2007 du Conseil du 26 novembre 2007 portant modification du règlement (CE) nº 1290/2005 relatif au financement de la politique agricole commune, JO 2007 L 322, p. 1.

Roumanie, *Curtea Constituțională*, Decision nº 1258 (1) du 8 octobre 2009.

Scheinin, M. (2009), Report on the protection of the right to privacy in the fight against terrorism, A/HRC/13/37, 28 décembre 2009.

Slovénie, *Informacijski Pooblascenec*, « Google Street View », Lubjljana, 25 mai 2010.

Royaume-Uni, *Information Commissioner's Office* (2010), European data protection Commission's call for the UK to strengthen the powers of its national data protection authority, Londres, 28 juin 2010.

Royaume-Uni, *Ministry of Justice* (2010), Call for Evidence on the data protection legislative framework, Londres, 6 juillet 2010.