3 Société de l'information et protection des données à caractère personnel

Deux thèmes (la sécurité et la technologie) ont dominé le débat dans le domaine de la société de l'information et de la protection des données à caractère personnel en 2011, une année qui marquait les 10 ans des attaques terroristes du 11 septembre aux États-Unis. L'anniversaire a suscité le débat sur la manière de trouver le bon équilibre entre la sécurité et les droits à la vie privée et à la protection des données à caractère personnel et l'attention s'est portée sur des sujets thématiques tels que la conservation des données de télécommunication, la collecte et l'analyse des données des passagers, la création d'un système de surveillance du financement du terrorisme et l'utilisation des scanners corporels. La mise à jour du cadre de protection des données à caractère personnel pour faire face aux avancées technologiques a également été abordée. L'attention s'est notamment portée sur les sites de réseaux sociaux.

Le présent chapitre analyse les principaux changements intervenus en 2011 au sein de l'Union européenne (UE) et de ses États membres concernant la législation, les politiques et les pratiques dans le domaine de la protection des données à caractère personnel. Il traitera des évolutions majeures enregistrées au niveau européen puis, dans un second temps, des thèmes qui ont marqué l'actualité de 2011 dans le domaine, à savoir : la conservation des données à caractère personnel, les données des dossiers passagers (PNR), les systèmes de surveillance du financement du terrorisme, l'utilisation des scanners corporels et les sites de réseaux sociaux.

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

- les tribunaux et les parlements de certains États membres de l'UE font part d'inquiétudes relatives aux législations nationales mettant en œuvre la directive sur la conservation des données à caractère personnel ; la Commission européenne adopte, à la fin de l'année 2010, un rapport d'évaluation sur la directive ;
- dans le cadre du dossier des données passagers (PNR), le Parlement européen adopte l'accord PNR entre l'UE et l'Australie, alors que l'approbation parlementaire est attendue pour l'accord PNR entre l'UE et les États-Unis ; la Commission européenne propose une directive pour échanger des données PNR entre les États membres de l'UE aux fins de l'application de la loi ;
- l'UE rédige de nouvelles règles pour l'utilisation des scanners corporels dans les aéroports européens. Dans un même temps, un certain nombre d'États membres de l'UE testent et évaluent l'utilisation de ces scanners dans la pratique ;
- la Commission européenne présente des options pour un système européen de surveillance du financement du terrorisme, alors que la mise en œuvre de la coopération existante entre l'UE et les États-Unis, connue sous le nom de programme de surveillance du financement du terrorisme, subit deux révisions, qui demandent toutes deux plus de transparence.

3.1. Aperçu général

En novembre 2010, la Commission européenne a présenté ses plans dans le domaine de la protection des données à caractère personnel.[1] Cette communication souligne l'approche de la Commission concernant la révision du système de l'UE en matière de protection des données à caractère personnel dans tous les domaines d'activité de l'UE, en tenant compte des enjeux résultant de la mondialisation et des nouvelles technologies. Plusieurs objectifs ont ainsi été fixés, notamment : renforcer les droits des personnes, accroître la transparence et le niveau de sensibilisation aux droits en matière de

1 Commission européenne (2010c).

protection des données à caractère personnel, permettre aux intéressés d'exercer un meilleur contrôle sur les données les concernant, garantir un consentement éclairé et libre, actualiser le système de protection des données sensibles et renforcer l'efficacité des voies de recours et des sanctions. Dans son avis sur la communication de la Commission, le Contrôleur européen de la protection des données a préconisé la mise en place de solutions plus ambitieuses renforçant le contrôle des citoyens européens sur leurs données personnelles pour rendre le système plus efficace. Il a en outre souligné que l'intégration de la coopération policière et judiciaire au cadre juridique s'avère essentielle pour la mise en place d'un système de protection des données à caractère personnel efficace.[2]

Le sondage Eurobaromètre intitulé *Attitudes à l'égard de la protection des données et de l'identité électronique* a été publié en 2011.[3] L'une des principales conclusions de ce sondage auquel ont participé 26 574 Européens de 15 ans et plus, dans les 27 États membres de l'UE, est que trois Européens sur quatre reconnaissent que la divulgation de données personnelles fait partie de leur quotidien, mais qu'ils sont inquiets quant à la façon dont les entreprises, notamment les moteurs de recherche et les réseaux sociaux, utilisent leurs informations. Ce rapport révèle en outre que 62 % des personnes interrogées dans l'UE fournissent un minimum d'informations de façon à protéger leur identité et que 75 % souhaitent pouvoir supprimer leurs données personnelles en ligne lorsqu'elles le désirent, faisant ainsi référence au « droit à l'oubli ». Ils sont également nombreux à être favorables à une intervention de l'UE dans ce domaine puisque 90 % d'entre eux souhaitent que les droits en matière de protection des données à caractère personnel soient identiques dans tous les pays de l'UE. Le sondage a été réalisé entre fin novembre et mi-décembre 2010. Tous les entretiens ont été effectués en face-à-face au domicile des personnes interrogées, dans leur langue nationale.

« Plus de la moitié des Européens interrogés déclarent qu'une amende devrait être infligée aux [...] entreprises (qui utilisent les données des individus sans les informer) (51 %). 4 personnes sur 10 considèrent qu'il faudrait interdire à ces entreprises d'utiliser les données à caractère personnel à l'avenir (40 %) ou les contraindre à dédommager les victimes (39 %) ».

Eurobaromètre n° 359, Attitudes à l'égard de la protection des données et de l'identité électronique dans l'Union européenne*, numéro spécial sur Bruxelles, juin 2011, p. 190*

Dans son rapport sur l'évolution de la protection de la vie privée, trente ans après les lignes directrices de l'Organisation de Coopération et de Développement Économiques (OCDE) sur la protection de la vie privée,[4] l'OCDE décrit les tendances actuelles en matière de traitement des données personnelles et les risques qui en découlent pour la vie privée. Le rapport présente des initiatives et des approches innovantes en matière de protection de la vie privée en mettant particulièrement l'accent sur les activités économiques. L'OCDE a également publié un rapport économique sur la réglementation des flux de données transnationales, qui traite des risques croissants qui pèsent sur la vie privée du fait du nombre de plus en plus important de transferts de données personnelles sur l'internet dans une économie mondialisée. Ce rapport dresse un inventaire systématique de la réglementation au niveau international et analyse les politiques sous-jacentes[5] dans le but de contribuer au débat sur la réglementation future des flux de données transnationales.

Au Conseil de l'Europe, le débat sur la révision de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE n° 108) s'est poursuivi.[6] Dans le rapport du Conseil de l'Europe sur la consultation correspondante[7], les personnes interrogées soulignent l'importance de garantir la cohérence avec les règles de protection de l'UE. Par ailleurs, le Comité des ministres du Conseil de l'Europe a adopté à la fin novembre 2010, une Recommandation sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage.[8] Celle-ci vise à définir des règles de profilage loyal et licite respectant pleinement les droits fondamentaux, notamment le droit à la vie privée, la protection des données à caractère personnel et le principe de non-discrimination. En septembre 2011, le Conseil de l'Europe a aussi publié un projet de stratégie pour la gouvernance de l'internet (2012-2015). Ce projet, qui a été adopté le 15 mars 2012, fait référence au fait que la promotion de la protection des données à caractère personnel et de la vie privée font partie de ces objectifs principaux. Pour finir, en 2011, une procédure de révision des recommandations du Comité des Ministres 87(15) visant à réglementer l'utilisation des données à caractère personnel dans le secteur de la police et 89(2) sur la protection des données à caractère personnel utilisées à des fins d'emploi a été lancée.

Au niveau de l'Union européenne, le rôle de la protection des données à caractère personnel dans le domaine de la liberté, de la sécurité et de la justice a suscité un intérêt particulier. Une étude préparée pour le Parlement européen a analysé les nouveaux défis découlant des politiques et systèmes de protection des données à caractère personnel relevant de la coopération policière et judiciaire en matière pénale.[9] Elle a identifié une série de principes fondamentaux communs et de normes visant à garantir véritablement la protection

2 Contrôleur européen de la protection des données (CEPD) (2011a).
3 Commission européenne (2011a).
4 Organisation de coopération et de développement économiques (OCDE) (2011b).
5 OCDE (2011a).
6 Conseil de l'Europe (2011a).
7 Conseil de l'Europe (2011b).
8 Conseil de l'Europe (2010).
9 Bigo D. *et al.* (2011).

des données à caractère personnel à chaque phase de l'élaboration de la politique de l'UE et à mettre en œuvre ce droit fondamental de façon effective.

La conférence des Commissaires européens à la protection des données a adopté une résolution insistant sur la nécessité de mettre en place un cadre global de protection des données à caractère personnel couvrant le secteur des forces de l'ordre.[10]

Le règlement 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 a été adopté le 25 octobre 2011.[11] Cette nouvelle agence agira en tant qu'autorité de gestion des systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice : la nouvelle génération d'une base de données européenne regroupant et diffusant des informations sur les personnes et l'existence d'intérêts de sûreté nationale, les contrôles aux frontières et les services répressifs (SIS II) ; un système d'échange de données relatives aux visas (VIS) ; et une base de données européenne pour la comparaison des empreintes digitales aux fins d'identifier les demandeurs d'asile et les personnes franchissant les frontières de manière irrégulière (Eurodac).

Sur un plan plus général, l'indépendance des autorités de protection des données à caractère personnel (dont la liste est présentée dans le Tableau 3.1) est restée problématique. Comme le souligne le Rapport annuel publié l'année dernière, la Cour de justice de l'Union européenne (CJUE) a rendu un arrêt[12] sur le défaut d'indépendance suffisante des autorités allemandes chargées de la protection des données au niveau des États fédérés (*Länder*). La Commission européenne a assigné l'Autriche devant la CJUE pour défaut d'indépendance de son autorité de protection des données.[13] Les débats sur la nouvelle Constitution hongroise, entrée en vigueur début 2012, ont porté notamment sur l'indépendance de l'autorité hongroise chargée de la protection des données. Le 17 janvier 2012, la Commission européenne a engagé des procédures d'infraction accélérées contre la Hongrie pour statuer à ce sujet.[14]

> *« L'indépendance des autorités de contrôle de la protection des données est garantie par l'article 16 du traité sur le fonctionnement de l'UE et l'article 8 de la Charte des droits fondamentaux de l'Union européenne. En outre, les règles de l'UE relatives à la protection des données (directive 95/46/CE) exigent des États membres qu'ils créent un organisme de surveillance totalement indépendant pour contrôler l'application de la directive. [...] le seul risque que les autorités de tutelle puissent exercer une influence politique sur les décisions des autorités de contrôle suffit pour entraver l'exercice indépendant des missions de celles-ci. »*
>
> *Commission européenne, communiqué de presse IP/12/24, Bruxelles, 17 janvier 2012*

Tableau 3.1 : Instances requises dans le cadre de la législation européenne – autorités de protection des données à caractère personnel, par pays

Pays	Nom de l'instance en français	Nom de l'instance dans la langue nationale ou alternative
AT	Commission autrichienne de protection des données	*Österreichische Datenschutzkommission*
BE	Commission de la protection de la vie privée	*Commission de la protection de la vie privée/Commissie voor de bescherming van de persoonlijke levenssfeer/Ausschuss für den Schutz des Privatlebens*
BG	Commission pour la protection des données à caractère personnel	*Комисията за защита на личните данни*
CY	Commissaire à la protection des données à caractère personnel	*Γραφείο Επιτρόπου Προστασίας Δεδομένων Προσωπικού Χαρακτήρα*
CZ	Office de protection des données à caractère personnel	*Úřad pro ochranu osobních údajů*
DE	Commissaire fédéral à la protection des données et à la liberté de l'information	*Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit*
DK	Agence danoise de protection des données	*Datatilsynet*

10 Conférence des Commissaires européens à la protection des données (2011).
11 Règlement (EU) n° 1077/2011, JO 2011 L 286.
12 Cour de Justice de l'Union européenne (CJUE), C-518/07, *Commission c. Allemagne,* 9 mars 2010.
13 Commission européenne (2010b).
14 Commission européenne (2012).

Tableau 3.1 (suite)

Pays	Nom de l'instance en français	Nom de l'instance dans la langue nationale ou alternative
EE	Inspection estonienne de la protection des données	*Andmekaitse Inspektsioon*
EL	Autorité grecque de protection des données	*Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα*
ES	Autorité espagnole de protection des données	*Agencia Española de Protección de Datos, AEPD*
FI	Bureau du médiateur chargé de la protection des données	*Tietosuojavaltuutetun toimisto, Dataombudsmannens byrå*
FR	Commission Nationale de l'Informatique et des Libertés	*Commission Nationale de l'Informatique et des Libertés*
HU	Autorité chargée de la protection des données et de la liberté de l'information	*Nemzeti Adatvédelmi és Információszabadság Hatóság*
IE	Commissaire à la protection des données	*An Coimisinéir Cosanta Sonraí*
IT	Autorité de protection des données	*Garante per la protezione dei dati personali*
LT	Autorité nationale de protection des données	*Valstybinė duomenų apsaugos inspekcija*
LU	Commission nationale pour la protection des données	*Commission nationale pour la protection des données*
LV	Inspection nationale de protection des données	*Datu valsts inspekcija*
MT	Bureau du commissaire à la protection des données	*Office of the Data Protection Commissioner*
NL	Autorité néerlandaise de protection des données	*College bescherming persoonsgegevens*
PL	Bureau de l'inspecteur général de protection des données à caractère personnel	*Generalny Inspektor Ochrony Danych Osobowych*
PT	Autorité portugaise de protection des données	*Comissão Nacional de Protecção de Dados*
RO	Autorité nationale de contrôle pour le traitement des données à caractère personnel	*Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal*
SE	Conseil suédois d'inspection des données	*Datainspektionen*
SI	Commissaire à l'information	*Informacijski pooblaščenec*
SK	Office de protection des données à caractère personnel de la République slovaque	*Úrad na ochranu osobných údajov*
UK	Bureau du commissaire à l'information	*The Office of the Information Commissioner/ Swyddfa'r Comisiynydd Gwybodaeth*

Source : http://ec.europa.eu/justice/data-protection/bodies/authorities/eu/index_en.htm

3.2. Conservation des données à caractère personnel

L'Union européenne a adopté une directive qui oblige les opérateurs téléphoniques et fournisseurs d'accès à l'internet à conserver des données de trafic complètes concernant l'usage non lié au contenu de l'internet et du téléphone. Depuis son adoption en 2006, cette directive sur la conservation des données[15] suscite des préoccupations quant au respect des droits fondamentaux.

En avril 2011, la Commission européenne a publié un rapport évaluant sa mise en œuvre et son application.[16] Selon ce rapport, la directive elle-même ne garantit pas que les données personnelles conservées soient stockées, extraites et utilisées dans le respect le plus total du droit à la vie privé et à la protection des données à caractère personnel. La Commission a indiqué que cette directive n'a visé qu'à harmoniser partiellement les approches en matière de conservation des données à caractère personnel. Par conséquent, il n'est guère surprenant que les États membres de

15 Directive 2006/24/CE, JO 2006 L 105.

16 Commission européenne (2011e).

l'UE n'aient pas d'approche commune, même en ce qui concerne les domaines couverts par la directive, tels que le délai de conservation des données personnelles, et encore moins pour ceux qui ne sont pas couverts, tels que le fait de savoir à qui incombe la responsabilité de couvrir les frais liés à cette obligation de conservation des données.[17] La Commission a conclu que l'historique des données de communication s'avère important dans les enquêtes pénales et que l'Union européenne doit, par conséquent, continuer à promouvoir et à réglementer la conservation des données à caractère personnel comme mesure de sécurité.

La Commission européenne a consulté les différentes parties prenantes concernant les possibilités envisagées pour la modification du cadre de conservation des données personnelles. Dans son avis sur le *rapport d'évaluation* de la directive, le Contrôleur européen de la protection des données a conclu que cette dernière ne répond pas aux exigences de respect des droits fondamentaux en matière de vie privée et de protection des données à caractère personnel.[18]

« La directive [sur la conservation des données] est sans aucun doute l'instrument le plus préjudiciable au respect de la vie privée jamais adopté par l'Union européenne eu égard à son ampleur et au nombre de personnes qu'elle touche. »

Contrôleur européen de la protection des données, « Le moment de vérité pour la directive sur la conservation des données », discours prononcé à Bruxelles le 3 décembre 2010

Au niveau national, l'Allemagne, Chypre, les Pays-Bas, la République tchèque, la Roumanie et la Suède ont eux aussi critiqué la directive sur la conservation des données. Le 22 mars 2011, la Cour constitutionnelle de la **République tchèque** a déclaré inconstitutionnelles certaines dispositions nationales[19] concernant la mise en œuvre de la directive,[20] dans le cadre de poursuites engagées par un groupe de 51 députés du Parlement tchèque. La Cour a notamment évoqué le manque de proportionnalité concernant l'ingérence des dispositions nationales dans l'exercice du droit à la vie privée ; l'absence d'une définition claire concernant l'objectif de la conservation des données personnelles ; l'absence de liste explicite des institutions autorisées à accéder aux données ; l'absence d'obligation d'information des personnes concernées ; et l'absence de contrôle judiciaire approprié. À **Chypre**, la Cour suprême a elle aussi déclaré inconstitutionnelles certaines dispositions nationales relatives à la mise en œuvre de la directive sur la conservation des données.[21] L'affaire concernait l'accès des agents de police aux données de télécommunications sur injonction des tribunaux. La cour a fait valoir le fait que la directive n'impose pas aux États membres de promulguer une loi permettant à la police d'accéder à ce type de données puisque cela n'entre pas dans son champ d'application. Elle a en outre souligné que les injonctions de tribunaux concernées avaient été prononcées avant qu'une modification constitutionnelle prévoyant des exceptions au droit de la confidentialité des communications ne soit votée.

Aux **Pays-Bas**, deux commissions du Sénat ont fait part de leur déception vis-à-vis de l'évaluation de la directive sur la conservation des données faite par la Commission européenne, dans une lettre adressée au Ministre de la Sécurité et de la Justice, en date du 31 mai 2011.[22] Ces commissions ont contesté plusieurs points, soulignant notamment que cette évaluation n'était pas satisfaisante du fait qu'elle s'était abstenue de démontrer la nécessité de cette directive et n'avait pas accordé suffisamment d'attention à la proportionnalité de la conservation des données personnelles. Les deux commissions ont, par ailleurs, soulevé des questions au sujet de la méthodologie utilisée et préconisé le retrait de la directive.[23]

L'**Allemagne** envisage de transposer intégralement la directive sur la conservation des données à caractère personnel dans sa législation nationale et d'y intégrer également les conditions définies dans un arrêt de la Cour constitutionnelle allemande de 2010.[24] Toutefois, à ce jour, aucun consensus sur une nouvelle proposition législative n'a été trouvé. Le service de recherche de la Chambre des représentants (*Bundestag*) a en effet souligné que la directive sur la conservation des données ne peut pas être mise en œuvre en garantissant, sans la moindre réserve, que cette dernière est compatible avec la Charte des droits fondamentaux de l'Union européenne.[25] Ces réserves portent notamment sur la liberté d'entreprise, la directive imposant aux entreprises privées de créer et de maintenir des structures très coûteuses pour la conservation des données de communication. Une autre étude de la Chambre basse des représentants (*Bundestag*) conclut que la conservation des données n'a augmenté de manière significative, dans aucun des pays de l'UE, le nombre de délits résolus.[26] L'étude souligne cependant qu'aucune donnée statistique permettant d'évaluer l'impact de la directive sur le taux d'élucidation des délits n'est dis-

17 *Ibid.*, p. 31.
18 CEPD (2010).
19 République tchèque, Loi sur la communication électronique, n° 127/2005 Coll., section 97, sous-section 3 et 4 ; décret mettant en œuvre la directive sur la conservation des données.
20 République tchèque, Cour constitutionnelle, fichier relatif à la décision n° Pl ÚS 24/10, 22 mars 2011.
21 Chypre, Cour suprême, *Christos Matsias et autres*, 65/2009, 78/2009, 82/2009, 15-22/2010, décision du 1 février 2011.
22 Pays-Bas, Sénat (2011a).
23 Pays-Bas, Sénat (2011b).
24 Allemagne, Bundesverfassungsgericht, *1 BvR 256/08 vom 2.3.2010*, 2 mars 2010.
25 Derksen, R. (2011).
26 Becher, J. (2011).

ponible. De même, le Commissaire fédéral à la protection des données et à la liberté de l'information estime que rien n'indique que la conservation des données personnelles a augmenté de manière significative les taux de détection des infractions pénales.[27] La police fédérale allemande a cependant rendus publics des éléments prouvant que l'absence de mesures de conservation des données a un impact négatif sur les enquêtes judiciaires.[28] Une étude commandée par le Ministère de la Justice, réalisée par l'Institut Max Planck de droit pénal étranger et international, a mis en doute la valeur ajoutée de la conservation des données. Les résultats de cette étude empirique à grande échelle ont été présentés à la Commission des affaires juridiques du Bundestag le 27 janvier 2012.[29]

Dans le cadre de la mise en œuvre de la directive sur la conservation des données, la **Suède** a présenté à la fin de l'année 2010 un projet de loi sur la conservation des données relatives au trafic.[30] Le parti écologiste, le parti des Démocrates suédois et le parti de gauche ont cependant voté minoritairement en faveur de ce projet de loi, retardant ainsi la transposition de la directive. Le Parlement ne le réexaminera pas avant le 17 mars 2012. De même, en **Roumanie,** le Sénat réuni en séance plénière le 21 décembre 2011 a rejeté à l'unanimité la nouvelle proposition législative, faisant suite à une décision de la Cour constitutionnelle de 2009 qui avait estimé que la législation nationale de transposition de la directive était contraire à la Constitution.[31]

3.3. Données des dossiers passagers

Les données des dossiers passagers (PNR) sont des informations fournies par les passagers, qui sont recueillies et conservées dans les systèmes de réservation et de contrôle des départs des transporteurs aériens. Peu après les attaques terroristes du 11 septembre 2001, certains pays en dehors de l'UE ont immédiatement adopté une législation imposant aux compagnies aériennes assurant le transport de passagers au départ, à destination, ou via leur territoire de fournir aux autorités nationales les données PNR stockées dans leur système informatique de réservation. Ces données, envoyées bien avant le départ d'un vol, doivent aider les forces de l'ordre à vérifier l'identité des passagers pour détecter des liens éventuels à des organisations terroristes et toute autre forme de crime grave.[32]

En 2011, les institutions de l'UE ont discuté des accords sur l'échange des données PNR avec différents pays. Le Parlement européen a ainsi adopté l'accord UE-Australie sur les données des dossiers passagers[33] et doit encore approuver l'accord entre l'UE et les Etats-Unis.[34] Ces accords remplaceront les deux précédents accords signés respectivement en 2008 et 2007. Le Parlement européen a demandé une modification du projet d'accord avec les États-Unis afin de réduire la durée du stockage des données personnelles et de garantir aux citoyens de l'UE le droit de faire appel des décisions d'interdiction de voyage prononcées à leur encontre en relation avec les données PNR.[35] Le Contrôleur européen de la protection des données a émis des avis concernant ces deux accords.[36] S'il a salué les garanties relatives à la sécurité des données personnelles et les mécanismes de contrôle prévus par les deux accords, il a fait part de ses préoccupations concernant les principes généraux des droits fondamentaux, tels que la nécessité et la proportionnalité.

La Commission européenne a présenté en février une nouvelle proposition de directive concernant l'échange des données PNR au sein des États membres à des fins répressives.[37] La directive proposée reprend une proposition législative de 2007, à savoir la décision-cadre sur les données passagers,[38] introduite avant l'entrée en vigueur du Traité de Lisbonne. Plusieurs instances de l'UE ont contesté la proportionnalité de la proposition quant à son impact sur les droits au respect de la vie privée et à la protection des données à caractère personnel (articles 7, 8 et 52 de la Charte des droits fondamentaux de l'UE). Le Contrôleur européen de la protection des données a souligné que la nécessité et la proportionnalité de ce système – qui implique la collecte à grande échelle des données PNR dans le but de procéder à une évaluation systématique de tous les passagers – doivent être clairement établies.[39] Il a également formulé des recommandations couvrant divers aspects de la proposition et concernant notamment : la limitation du champ d'application ; la durée de conservation des données à caractère personnel ; la liste des données PNR stockées ; l'amélioration des principes de protection des données à caractère personnel ; et la réalisation d'une évaluation exhaustive du système. Le Groupe de travail «Article 29» sur la protection des données a lui aussi questionné la nécessité et la proportionnalité des systèmes PNR et demandé des éclaircissements complémentaires concernant le champ d'application de la proposition.[40] Le Comité économique et social européen (CESE) a jugé cette proposition disproportionnée du fait qu'elle « n'apporte pas

27 Allemagne, Commissaire fédéral à la protection des données et au droit à l'information (2011).
28 Allemagne, Ministère de l'Intérieur (2011b).
29 Max Planck Institut für Ausländisches und Internationales Strafrecht (2012).
30 Suède, Regeringskansliet (2010).
31 Roumanie, Curtea Constituțională a României, décision n° 1258, 8 octobre 2009.
32 Commission européenne (2011d), p. 3.
33 Parlement européen (2011b).
34 Conseil de l'Union européenne (2011).
35 Commission européenne (2011b).
36 Contrôleur européen de la protection des données (CEPD) (2011a) et (2011b).
37 Commission européenne (2011d).
38 Commission européenne (2007).
39 CEPD (2011a).
40 Groupe Article 29 sur la Protection des Données (2011).

d'arguments suffisants pour justifier qu'il soit nécessaire d'utiliser de manière généralisée et indistincte les données des dossiers passagers (PNR) de tous les citoyens qui empruntent des vols internationaux ».[41]

« Avant de soumettre de nouvelles propositions de mesures, les mesures applicables sur la collecte des données personnelles, à des fins répressives et de contrôle des mouvements migratoires, doivent être évaluées et les «failles de sécurité» identifiées. Tout projet de proposition concernant le transfert de données PNR doit inclure une analyse d'impact approfondie et assortie d'informations fiables et actualisées sur l'efficacité, les coûts et les répercussions sur les droits fondamentaux. »

Lettre du Comité permanent d'experts en matière de droit international relatif à l'immigration, aux réfugiés et aux affaires pénales (Comité Meijers) adressée à la Commissaire Cecilia Malström, référence CM1108, 21 juin 2011, disponible sur : www.commissie-meijers.nl

ACTIVITÉ DE LA FRA

Second avis sur la conformité d'une proposition de directive sur les données PNR aux droits fondamentaux

À la demande du Parlement européen, la FRA a présenté un avis quant à la nouvelle proposition de directive sur les données PNR de la Commission européenne[42] et sur sa conformité à la Charte des droits fondamentaux. L'agence avait déjà émis, en octobre 2008, un premier avis au sujet des données PNR à la demande du Conseil de l'Union européenne.

Ce second avis soulève des préoccupations au sujet des droits fondamentaux, en mettant notamment l'accent sur les risques de discrimination indirecte liés au profilage et sur l'importance de la collecte de statistiques appropriées pour détecter ce type de discrimination. L'accent est aussi mis sur les conditions de nécessité et de proportionnalité pour le respect des droits fondamentaux et sur une supervision efficace et proactive pour garantir les droits des passagers. Cet avis contribuera aux débats qui auront lieu au Conseil de l'Union européenne et au Parlement européen.

Le **Royaume-Uni** est favorable à la mise en place d'une directive de l'UE sur les données PNR prévoyant des dispositions pour les vols intracommunautaires. Le gouvernement considère en effet que « des accords PNR clairs entre l'Union européenne et les pays tiers s'avèrent essentiels pour lever toute incertitude juridique à l'égard des compagnies aériennes assurant des vols à destination de ces pays et permettent de garantir que les données PNR peuvent être partagées rapidement et de manière sécurisée, toutes les mesures nécessaires en matière de protection des données étant mises en place ».[43] Selon la Commission pour l'Union européenne de la Chambre des Lords (Sous-commission des affaires intérieures), il est impératif d'adopter une législation à l'échelle de l'UE dans ce domaine. Elle estime ainsi qu'une mesure législative unique doit couvrir la collecte des données PNR sur les vols dans l'ensemble des États membres, ainsi que le partage de ces données avec les autorités d'autres États membres.[44] D'autres préoccupations ont été abordées dans une déclaration faite, le 10 mai, à la Chambre des communes par le Ministre de l'Immigration, interpellant notamment l'Assemblée au sujet de la nécessité et de la proportionnalité des données PNR.[45]

En **France**, le Ministère de l'Intérieur a indiqué qu'il « [soutenait] activement la création d'un système européen de PNR » et annoncé « [qu']une mission interministérielle a été mise en place pour réfléchir à la mise en place d'un tel système » qui soit « capable de traiter les données PNR et de prendre en compte l'ensemble des pays extérieurs à l'espace Schengen. »[46] Mais des critiques ont également été formulées. Le 17 février, la Commission Nationale de l'Informatique et des Libertés a émis un avis dans lequel elle observe que l'expérimentation d'un dispositif national précurseur d'un système PNR sur une période de quatre ans n'a pas permis de démontrer clairement l'efficacité de ce dispositif. Elle souligne également que « le taux d'alertes [...] erronées demeure anormalement élevé. » Néanmoins, elle s'est déclarée favorable à la poursuite de l'expérimentation en cours afin de « préparer une future plate-forme française de traitement de données relatives aux passagers dans le cadre de la mise en œuvre d'un futur système [...] PNR basé sur une réglementation européenne ».[47]

Dans d'autres États membres, comme l'**Autriche**, la **République tchèque** et la **Roumanie**, les parlements respectifs ont fait part de leurs doutes quant à la mise en place d'un système européen de collecte et d'analyse de données PNR.

L'**Autriche** demeure sceptique à l'égard de l'utilisation des données PNR au sein de l'UE en tant qu'outil complémentaire de la lutte contre le terrorisme, opinion qui était d'ailleurs partagée par les parlementaires, tous partis politiques confondus, au mois d'avril. Selon le Ministre fédéral de l'Intérieur alors en fonction, trois conditions devaient être remplies avant que l'Autriche

41 Comité économique et social européen (CESE) (2011a).
42 Commission européenne (2011d).
43 Royaume-Uni, Home Office (2011b).
44 Royaume-Uni, House of Lords (2011), p. 7.
45 Royaume-Uni, Home Office (2011a).
46 France, Le Fur, M. (2010).
47 France, Commission nationale de l'informatique et des libertés (CNIL) (2011).

ne soutienne un tel système : les solutions envisagées doivent respecter les droits de l'homme ; l'usage des données PNR doit apporter une valeur ajoutée significative à la lutte contre le terrorisme ; les ressources financières et personnelles engagées doivent être proportionnelles à la valeur du système.[48] Le Conseil autrichien de la protection des données (*Datenschutzrat*) a publié, en février 2011, un communiqué sur la proposition de directive de l'UE sur les données PNR, soulignant que le fait de stocker les données personnelles de tous les passagers, alors même qu'aucun soupçon ne pèse sur ces derniers, interfère avec le droit à la vie privée. Dans ce cas précis, le législateur doit s'assurer de l'adéquation et de la nécessité d'une telle violation. Or, la proposition de l'UE n'apporte pas la preuve de cette adéquation et de cette nécessité, ajoute le conseil.[49]

Au cours du premier semestre de 2011, le Sénat[50] et la Chambre des députés de la **République tchèque**[51] ont appelé le gouvernement à respecter scrupuleusement les garanties offertes par la Constitution concernant le droit à la vie privée dans le cadre de l'élaboration d'une proposition relative aux données PNR. Selon l'avis émis par les deux chambres législatives, les délits liés à l'utilisation des données de dossiers passagers doivent être définis de manière plus détaillée pour garantir la proportionnalité. Elles ont en outre souligné l'absence de réglementation complémentaire concernant la forme sous laquelle les données sont conservées et mentionné que la durée de conservation était inappropriée. Enfin, les deux chambres ont refusé d'étendre l'obligation de stockage et de transmission des données à caractère personnel sur les vols entre les États membres de l'UE.

En **Roumanie**, le Sénat (*Senatul*) a émis un avis sur la proposition de directive relative aux données PNR,[52] la jugeant conforme au principe de subsidiarité, mais pas à celui de proportionnalité. Concernant ce dernier point, le Sénat a en effet estimé que les définitions concernant certains types de données personnelles requis pour la collecte sont floues et que toute décision susceptible d'avoir des répercussions importantes ne devrait pas être prise en se basant sur le traitement automatique des données PNR.[53] Des préoccupations similaires ont été formulées en Lituanie[54], au Portugal[55] et en Allemagne[56].

48 Autriche, Parlament (2011).
49 Autriche, Datenschutzrat (2011).
50 République tchèque, Sénat, Résolution n° 207, 28 avril 2011.
51 République tchèque, Chambre des députés, Résolution n° 446, 28 avril 2011.
52 Commission européenne (2011d).
53 Roumanie, Sénat du Parlement roumain (2011).
54 Lituanie, Lietuvos Respublikos Seimo Europos reikalų komitetas (2011).
55 Portugal, Comissão Nacional de Protecção de Dados (2011).
56 Allemagne, Commissaire fédéral à la protection des données et au droit à l'information (2011), p. 145.

Le débat autour du système PNR de l'UE proposé et de son respect des droits fondamentaux devrait se poursuivre en 2012.

3.4. Programme de surveillance du financement du terrorisme

Le programme de surveillance du financement du terrorisme (*Terrorist Finance Tracking Programme*, TFTP) a suscité un important débat au sein de l'UE, qui nécessite de trouver un équilibre entre les préoccupations liées à la protection des données à caractère personnel et celles liées à la sécurité. Il s'agit notamment de fournir aux services de sécurité des données relatives aux opérations financières à partir de certains services de messagerie financière constituant des plates-formes sécurisées, développées pour les applications intra- et interbancaires. L'idée de base est de lutter contre le terrorisme en suivant les circuits empruntés par l'argent via des standards communs de données de messagerie développés pour les transactions financières internationales. Le programme de surveillance du financement du terrorisme était, à l'origine, un programme du gouvernement américain mis en place dans le cadre de sa « Guerre globale contre le terrorisme » (*Global War On Terrorism*).

L'accord TFTP UE-États-Unis,[57] entré en vigueur en 2010, confère à Europol la responsabilité de vérifier si les demandes émanant des États-Unis sont proportionnées et nécessaires, conformément aux conditions qui y sont énoncées. Il définit un mécanisme d'examen périodique commun destiné à contrôler la mise en œuvre et l'efficacité de l'accord, ainsi que le rôle d'Europol concernant ce dernier point.[58] En novembre 2010, l'Autorité commune de contrôle d'Europol (ACC) a réalisé une inspection et constaté que les demandes écrites reçues n'étaient pas suffisamment spécifiques pour lui permettre de les approuver ou de les rejeter. Europol a néanmoins approuvé chacune des requêtes reçues.

> *« Europol a indiqué que l'information fournie oralement joue un rôle dans la vérification de chaque requête. [...] La place significative d'informations orales rend tout audit correct, interne ou externe, mené respectivement par le service de protection des données d'Europol ou par l'autorité commune de contrôle, impossible. »*
>
> *Le Président de l'Autorité commune de contrôle (ACC) d'Europol, 2 mars 2011*

57 Union européenne, États-Unis d'Amérique (2010).
58 Autorité de contrôle commune Europol (2011).

Dans le cadre de l'analyse du rapport de l'ACC par la Commission des libertés civiles, de la justice et des affaires intérieures du Parlement européen le 16 mars 2011, les membres du Parlement européen ont fait part de leurs vives préoccupations quant à la protection des données à caractère personnel. Le président a ainsi évoqué le sentiment « d'insatisfaction, d'inquiétude et de malaise » éprouvé par les membres de la Commission avant d'ajouter que « le Parlement européen doit exercer un contrôle sur la mise en œuvre de cet accord ».[59] Selon l'autorité fédérale de protection des données en **Allemagne**, la plupart des données de messagerie financière transmises aux autorités américaines, qui les conservent pendant de nombreuses années, ne sont en aucun cas liées au terrorisme international, le risque étant ainsi qu'elles soient utilisées à d'autres fins. Elle fait valoir qu'Europol, l'autorité chargée de surveiller l'échange des données avec les États-Unis conformément à l'accord en vigueur, n'est pas un garant approprié puisqu'elle profite, elle aussi, de l'échange de données à caractère personnel.[60]

La Commission européenne a publié en mars la première évaluation de l'accord TFTP effectuée conjointement par l'UE et les États-Unis, conformément aux dispositions de l'accord.[61] Le rapport d'évaluation conjoint est parvenu à la conclusion qu'Europol avait pris ses missions très au sérieux et mis en place les procédures nécessaires pour les exécuter avec professionnalisme et conformément à l'accord. Il partage cependant l'opinion de l'ACC en mentionnant : « il semble qu'il y ait lieu de fournir des justifications plus détaillées et plus ciblées concernant les demandes » pour permettre à Europol « de s'acquitter de sa mission encore plus efficacement ».[62] Ce rapport émet également plusieurs recommandations destinées à améliorer l'application de l'accord. Il souligne notamment qu'une plus grande transparence par rapport à la valeur ajoutée du programme de lutte contre le terrorisme, au volume global de données concernées et à d'autres aspects pertinents, contribuerait à convaincre davantage de personnes des bénéfices réels fondé de l'accord TFTP et à rehausser le niveau de confiance envers le programme. Le rapport note qu'il convient d'aspirer, autant que possible, à ce niveau de transparence sans compromettre l'efficacité du programme en tant que tel.

En réponse à une invitation du Parlement européen et du Conseil de l'Union européenne, la Commission européenne a présenté, au mois de juillet, différentes options pour la création d'un système européen de surveillance du financement du terrorisme.[63] La communication de la Commission a été examinée brièvement et ce, à une seule occasion, par la Commission des Libertés civiles, de la Justice et des Affaires intérieures du Parlement européen, mais n'a pas été abordée plus en détail. Le Conseil de l'Union européenne a organisé plusieurs débats à ce sujet, au niveau ministériel notamment, les principales considérations abordées ayant été le coût d'un futur système européen de surveillance du financement du terrorisme et sa compatibilité avec l'accord en vigueur avec les États-Unis. La communication insiste sur la nécessité de respecter pleinement les droits fondamentaux, et notamment le droit à la protection des données à caractère personnel. Au niveau des États membres de l'UE, aucun consensus n'a été trouvé pour le moment concernant cette question. Le gouvernement du **Royaume-Uni** a fait savoir qu'il était totalement favorable au programme TFTP existant, estimant également qu'il convient d'expliquer les raisons justifiant la création d'un système européen de surveillance du financement du terrorisme. Selon l'autorité fédérale de protection des données en **Allemagne**, la proposition de la Commission européenne suivrait des principes similaires à ceux de l'accord UE-États-Unis et aboutirait à un stockage massif de données à caractère personnel concernant des personnes non suspectes pour la plupart.[64]

3.5. Scanners corporels

L'utilisation de scanners corporels (ou « scanners de sûreté » selon le terme employé par la Commission européenne dans sa Communication de 2010 relative à *l'utilisation de scanners de sûreté dans les aéroports de l'UE*)[65] a été controversée en 2011, en raison de ses implications pour la dignité humaine et la vie privée. Le Parlement européen[66] et le Comité économique et social européen[67] ont organisé des auditions sur ce sujet. Fin 2011, la Commission européenne a adopté une législation sur l'utilisation des scanners de sûreté dans les aéroports de l'UE.[68] Le Contrôleur européen de la protection des données a contesté l'adoption de cette nouvelle législation à travers une procédure réglementaire, les propositions n'étant pas purement techniques, mais ayant également un impact sur les droits fondamentaux.[69]

59 Parlement européen (2011a).
60 Allemagne, Commissaire fédéral à la protection des données et au droit à l'information (2011).
61 Commission européenne (2011f).
62 *Ibid.*, p. 12.
63 Commission européenne (2011c).
64 Allemagne, Commissaire fédéral à la protection des données et au droit à l'information (2011).
65 Commission européenne (2010a).
66 Commission des libertés civiles, de la justice et des affaires intérieures du Parlement européen (LIBE) (2010).
67 CESE (2011b).
68 Règlement (UE) n° 1141/2011 de la Commission ; Règlement d'exécution (UE) n° 1147/2011 de la Commission.
69 CEPD (2011c).

ACTIVITÉ DE LA FRA

Les scanners corporels et les droits fondamentaux

La FRA a présenté son document de travail sur l'utilisation des scanners corporels en 10 questions et réponses (*The use of body scanners: 10 questions and answers*), lors d'une audition du Comité économique et social européen organisée en janvier 2011. Ce document préconise les mesures pratiques suivantes afin de garantir les droits fondamentaux des passagers : consultation des images par un opérateur distant de la personne faisant l'objet du contrôle, sans stockage ni archivage des images ; floutage du visage de la personne contrôlée pour garantir l'anonymat ; utilisation de tableaux synoptiques pour afficher les résultats au lieu d'images. Le document suggère en outre que les passagers devraient avoir le choix entre le passage au scanner corporel et des contrôles de sécurité plus conventionnels, tels que la fouille par palpation. Les passagers devraient également recevoir au préalable des informations complètes pour leur permettre de faire leur choix en connaissance de cause.

La législation autorise les États membres et les aéroports de l'UE à installer et à utiliser les scanners corporels comme l'une des méthodes possibles pour contrôler les passagers aux points de contrôle de sécurité, dans des conditions spécifiques respectueuses des droits fondamentaux. Par exemple, les scanners de sûreté ne doivent pas stocker, conserver, copier, imprimer ni récupérer des images ; tout accès non autorisé à une image et utilisation de celle-ci sont prohibés et doivent être empêchés ; l'opérateur qui analyse l'image doit se trouver dans un espace séparé et l'image ne doit pas être associée à la personne faisant l'objet de l'inspection, ni à d'autres personnes. Les passagers doivent être informés des conditions dans lesquelles se déroule le contrôle au moyen du scanner de sûreté. En outre, ils ont le droit de ne pas se soumettre au contrôle à l'aide de scanners et de choisir une autre méthode d'inspection.[70]

> *« Les scanners de sûreté ne sont pas la panacée, mais ils offrent une véritable possibilité de renforcer la sûreté des passagers. Ils constituent une alternative appréciable aux méthodes d'inspection/filtrage existantes et s'avèrent très efficaces pour détecter des objets métalliques et non métalliques. Il appartient toujours à chaque État membre ou aéroport de décider de déployer ou non les scanners de sûreté, mais ces nouvelles règles garantissent que lorsque cette nouvelle technologie est utilisée, elle sera soumise à des normes relatives à la capacité de détection applicables à l'échelle européenne ainsi qu'à des garanties strictes visant à protéger la santé et les droits fondamentaux. »*
>
> *Vice-président de la Commission européenne Sliim Kallas chargé des transports, communiqué de presse IP/11/1343, 14 novembre 2011*

70 Commission européenne (2011g).

Les approches des États membres de l'UE devraient continuer de diverger. En **Italie**, par exemple, une seconde phase d'expérimentation a été lancée début 2011 dans 3 aéroports (Rome Fiumicino, Milan Malpensa et Venise) avec l'application d'une nouvelle technologie,[71] mais cette dernière n'a été mise en œuvre que dans deux des trois aéroports (Rome et Milan) dès le mois de mai.[72] La première phase d'expérimentation avait eu lieu en 2010 (Rome Fiumicino, Milan Malpensa, Venise et Palerme). Selon l'autorité nationale de l'aviation civile,[73] les « scanners de sûreté expérimentés n'ont pas d'impact sur la santé et garantissent le respect de la vie privée des passagers ». Mais elle souligne également que les résultats de l'expérimentation ont été inférieurs à ceux escomptés du fait des alertes erronées et des délais d'enregistrement extrêmement longs. De son côté, le Ministre de l'Intérieur **allemand** a décidé, à la suite d'essais sur le terrain, que les scanners corporels ne seraient pas utilisés pour le moment dans les aéroports en Allemagne. Il s'est en effet avéré, à travers l'expérimentation de deux scanners corporels à l'aéroport de Hambourg, que la technologie n'a pas encore atteint un niveau qui permette aux dispositifs disponibles d'être adaptés à un usage quotidien.[74] Selon le Commissaire à la protection des données, les scanners corporels ne peuvent être utilisés légalement que si les données à caractère personnel ne sont pas stockées et si l'image des contours de la silhouette n'est pas visible à l'écran.[75]

Des préoccupations concernant les droits à la vie privée, à la protection des données à caractère personnel et à la dignité et les risques éventuels pour la santé ont été avancées en Suède[76] et en Slovénie[77].

3.6. Services de réseaux sociaux

La question de l'utilisation, de la conservation et du transfert des données personnelles par les services de réseaux sociaux s'est, elle aussi, trouvée au centre du débat public, étant donné le caractère personnel des informations concernées et les implications pour le droit à la vie privée.

Les autorités de protection des données des pays scandinaves ont adressé à Facebook 40 questions concernant la manière dont l'entreprise gère les données à caractère personnel. Facebook a répondu au

71 Italie, Autorità per l'Aviazione Civile (2010).
72 Italie, Autorità per l'Aviazione Civile (2011).
73 *Ibid.*
74 Allemagne, Ministère de l'Intérieur (2011a).
75 Allemagne, Commissaire fédéral à la protection des données et au droit à l'information (2011).
76 Suède, Commission de la justice, Parlement suédois (2010).
77 Slovénie, Ministère de l'Intérieur (2010) ; Slovénie, *Informacijski pooblaščenec* (2011).

mois de septembre[78] et confirmé que la société pouvait utiliser les informations liées aux mises à jour du statut des utilisateurs et à leur utilisation du bouton « J'aime » pour afficher des publicités ciblées. En revanche, elle a affirmé ne pas divulguer d'informations personnelles à d'autres entreprises, en dehors de celles que l'utilisateur consent à fournir lors du processus d'installation d'applications. Ayant son siège social européen en Irlande, la société considère qu'elle est soumise aux lois européennes de protection des données à caractère personnel.[79]

Un groupe autrichien baptisé L'Europe contre Facebook (*Europe versus Facebook*), dont les membres estiment avoir été victimes d'une violation de leur droit à la vie privé, a dressé une liste de 22 plaintes contre Facebook Irlande, l'entité chargée de toutes les activités du réseau social en dehors des États-Unis et du Canada, qu'il a transmise au mois d'août au Commissaire irlandais à la protection des données. Les plaintes contiennent les allégations suivantes : le bouton « J'aime » crée des données pouvant être utilisées pour suivre la trace des utilisateurs ; des identifications peuvent être faites sans le consentement de l'utilisateur ; et les « pokes », les publications, les images et les messages peuvent encore être visualisés après avoir été effacés par l'utilisateur.[80] En septembre, le Commissaire irlandais à la protection des données a annoncé son intention d'ouvrir d'une enquête au sujet de ces plaintes.[81] Le siège social international de Facebook étant situé en Irlande, le commissaire irlandais examinera l'ensemble des activités régies par les lois de protection des données à caractère personnel irlandaises et européennes. Toute décision prise concernant cette affaire pourrait avoir des implications pour des millions d'utilisateurs dans le monde.

Concernant l'utilisation des services de réseaux sociaux, les points suivants ont soulevé des inquiétudes dans les États membres : l'incertitude quant au caractère privé ou public des déclarations faites sur les sites de réseaux sociaux ; la création de profils et le traçage des utilisateurs par les sites de réseaux sociaux ; le manque de protection des enfants de la part des sites de réseaux sociaux.

En **France**, le Conseil de prud'hommes de Boulogne-Billancourt a rendu un arrêt le 19 novembre 2010 dans une affaire concernant la nature publique des déclarations faites sur les sites de réseaux sociaux. L'affaire concernait trois employés qui avaient été licenciés pour avoir critiqué leurs supérieurs hiérarchiques sur Facebook.[82] Le tribunal a estimé que les commentaires postés sur le site étaient mis à la disposition du public étant donné qu'ils étaient accessibles aux « amis des amis ». Les publications n'étaient plus privées dès lors qu'elles étaient accessibles à des personnes non impliquées dans la discussion. Par conséquent, le tribunal a jugé que le licenciement était fondé. Cependant, il subsiste des incertitudes quant à la jurisprudence à appliquer dans ce domaine. Le procureur de la République de Périgueux, par exemple, a traité différemment une affaire similaire. Il a ainsi estimé que les déclarations faites par deux employés sur leurs supérieurs étaient suffisamment protégées pour être considérées comme des discussions privées, visibles uniquement par les contacts directs des employés, et non pas par le « second cercle de contacts ».[83] Face à ce flou juridique, les opérateurs du secteur ont rapidement réagi. Le 30 juin, Google lançait le réseau Google+, nouveau service de réseau social où les messages ont différents niveaux de confidentialité en fonction des différents « cercles » définis par l'utilisateur. Le 13 septembre, Facebook lançait de nouveaux outils permettant aux utilisateurs d'organiser leurs listes d'amis pour mieux gérer les informations partagées.[84] Néanmoins, le caractère public ou privé des messages postés sur les sites de réseaux sociaux reste relativement incertain.

En **Allemagne**, à la suite d'une intervention du Centre indépendant pour la protection des données du Schleswig Holstein, les sites web hébergés dans le Land du Schleswig-Holstein ont eu jusqu'à fin septembre pour retirer le bouton « J'aime » de Facebook, sous peine de devoir payer une amende pouvant aller jusqu'à 50 000 EUR. À la base de cette injonction figurait la préoccupation selon laquelle le service était utilisé pour suivre la trace des utilisateurs et créer des profils.[85]

> *« Le libellé des conditions d'utilisation et des déclarations de confidentialité de Facebook ne répond pas aux exigences légales concernant les mentions légales, le consentement en matière de vie privée et les conditions générales d'utilisation. »*[87]
>
> *Allemagne, Centre indépendant pour la protection des données du Schleswig-Holstein*

En **Espagne**, l'autorité de protection des données a exprimé ses inquiétudes au sujet du nombre croissant de cas de violations de la vie privée signalés à propos des réseaux sociaux, concernant les enfants notamment

78 Norvège, Data Inspection Board (2011).
79 Suède, Datainspektion (2011).
80 Pour plus d'informations, voir : www.europe-v-facebook.org.
81 Voir aussi : http://m.zdnet.com/blog/facebook/irish-data-protection-commissioner-to-begin-facebook-audit/4262, consulté le 14 octobre 2011.
82 France, Tribunal de Boulogne-Billancourt, 19 novembre 2010, *Mme. B. c. SAS Alten Sir* ; *Mme S. c. SAS Alten Sir.*
83 Le Monde (2011b).
84 Le Monde (2011a).
85 Allemagne, Landesdatenschutzbeauftragte Schleswig-Holstein (2010).

(40 en 2010 contre 32 en 2009). Afin de régler ce problème, l'autorité a rencontré les responsables d'importants réseaux sociaux, tels que Tuenti et Facebook, dans le but d'améliorer leurs politiques de protection de la vie privée et d'empêcher l'inscription des enfants de moins de 14 ans. Le site Tuenti a réagi en déclarant qu'il passerait en revue jusqu'à 300 000 profils par an et qu'il supprimerait les profils d'enfants de moins de 14 ans. À la demande de l'autorité de protection des données, Facebook a annoncé qu'il ferait passer l'âge minimum à 14 ans pour pouvoir s'inscrire de l'Espagne sur son réseau. En outre, Facebook s'est engagé à mettre en place de meilleurs contrôles et à envisager plusieurs options pour mettre en œuvre un système de vérification de l'âge, ainsi qu'un système de consentement parental.[87]

Perspectives

Trouver un équilibre entre les obligations en matière de droits fondamentaux et les inquiétudes en matière de sécurité restera un défi pour les institutions de l'UE et ses États membres. La discussion actuelle relative à la directive sur la conservation de données à caractère personnel sera une des facettes de ce débat plus vaste.

Les institutions de l'UE poursuivront également le débat sur le cadre européen dans le domaine de la protection des données à caractère personnel. La Commission européenne a déposé des propositions en janvier 2012 pour réformer le cadre existant. Elles consistent en une proposition pour un règlement remplaçant la directive de 1995 sur la protection des données à caractère personnel et en une proposition de nouvelle directive définissant des règles pour la protection des données personnelles traitées à des fins de prévention, de détection, d'investigation ou de poursuite d'infractions pénales et d'activités judiciaires associées.

L'attitude envers la protection des données des utilisateurs et des fournisseurs de plates-formes sociales et d'autres outils en ligne continuera à alimenter le débat public et devrait de plus en plus devenir le sujet des délibérations devant les tribunaux. La disponibilité et l'utilisation des mécanismes de recours devront être examinées de près pour s'assurer que les droits fondamentaux sont entièrement respectés lors de l'utilisation des nouvelles technologies de l'information et de la communication.

La CJUE devrait une fois de plus aborder un autre domaine de préoccupation, l'indépendance des autorités de protection des données à caractère personnel.

86 *Ibid.*
87 Espagne, Agencia Española de Protección de Datos (2011a), p. 28.

Références

Allemagne, Bundesverfassungsgericht (BVerfG), 1 BvR 256/08, 2 mars 2010.

Allemagne, Commissaire fédéral à la protection des données et au droit à l'information (*Bundesbeauftragter für den Datenschutz und die Informationsfreiheit*) (2011), Rapport Annuel 2009/10.

Allemagne, Landesdatenschutzbeauftragte Schleswig-Holstein (2010), « Sicherheits- und Datenschutzziele miteinander in Einklang bringen », entretien, 17 septembre 2010.

Allemagne, Ministère de l'Intérieur (*Bundesministerium des Innern*) (2011a), « Körperscanner im Test: Leistungsfähig, aber noch nicht flächendeckend einsetzbar », communiqué de presse, 31 août 2011.

Allemagne, Ministère de l'Intérieur (2011b), *Studie des BKA bekräftigt Notwendigkeit von Mindestspeicherfristen*.

Autorité de contrôle commune Europol (2011), « US and EU agreement on exchanging personal data for the purposes of the Terrorist Finance Tracking Program (the TFTP Agreement) – first inspection performed by the Europol Joint Supervisory Body (JSB) raises serious concerns about compliance with data protection principles », communiqué de presse, Bruxelles, 2 mars 2011.

Autriche, Datenschutzrat (2011), *Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über die Verwendung von Fluggastdaten für die Verhinderung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität (Richtlinie EU-PNR)*, Avis du Conseil sur la protection des donnees.

Autriche, Parlament (2011), *V-19 der Beilagen zu den Stenographischen Protokollen des Nationalrates XXIV. GP – Beratungen des Ständigen Unterausschusses des Hauptausschusses in Angelegenheiten der Europäische Union*, 5 avril 2011.

Becher, J. (2011), *Die praktischen Auswirkungen der Vorratsdatenspeicherung auf die Entwicklung der Aufklärungsquoten in den EU-Mitgliedsstaaten*, WD 7 – 3000 – 036/11, mars 2011.

Bigo, D., Carrera, S., González Fuster, G., Guild, E., De Hert, P., Jeandesboz, J. et Papakonstantinou, V. (2011), *Towards a new EU legal framework for data protection and privacy: challenges, principles and the role of the European Parliament*, EP studies, Bruxelles, 15 septembre 2011.

Contrôleur européen de la protection des données (CEPD) (2010), « Le «Moment de vérité» pour la directive sur la conservation des données », Discours, Bruxelles, 3 décembre 2010.

CEPD (2011a), *Avis du contrôleur européen de la protection des données sur la communication de la Commission au Parlement européen, au Conseil, au Comité économique et social et au Comité des régions intitulée – « Une approche globale de la protection des données à caractère personnel dans l'Union européenne »*, 14 janvier 2011.

CEPD (2011b), *Avis du Contrôleur européen de la protection des données sur la proposition de décision du Conseil relative à la conclusion de l'accord entre les États-Unis d'Amérique et l'Union européenne sur l'utilisation et le transfert des données des dossiers passagers (données PNR) au ministère américain de la sécurité intérieure*, 9 décembre 2011.

CEPD (2011c), *Letter of Mr Giovanni Buttarelli, Assistant Supervisor, to Mr Sim Kallas, Vice-President of the European Commission*, 17 octobre 2011.

Chypre, Cour suprême, *Christos Matsias et autres*, requêtes 65/2009, 78/2009, 82/2009, 15-22/2010, décision du 1 février 2011.

Cour de justice de l'Union européenne (CJUE), Affaires jointes C-468/10 et C-469/10, *ASNEF et FECEMD c. Administracion del Estado*, 24 novembre 2011.

CJUE, C-70/10, *Scarlet Extended SA c. Société belge des auteurs, compositeurs et éditeurs*, 24 novembre 2011.

Comité économique et social européen (CESE) (2011a), Avis du Comité économique et social européen sur la Proposition de directive du parlement européen et du conseil relative à l'utilisation des données des dossiers passagers pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière, SOC 414, 5 mai 2011.

CESE (2011b), *Report of the Public Hearing on the use of security scanners at EU airports,* Bruxelles, 11 janvier 2011.

Commission des libertés civiles, de la justice et des affaires intérieures du Parlement européen (LIBE) (2010), *Meeting of the Committee on Civil Liberties, Justice and Home Affairs on recent developments in Counter-terrorism policies*, Parlement européen, Bruxelles, 27 janvier 2010.

Commission européenne (2007), *Proposition de décision-cadre du Conseil relative à l'utilisation des données des dossiers passagers (Passenger Name Record, PNR) à des fins répressives*, COM(2007) 654 final, Brussels, 6 novembre 2007.

Commission européenne (2010a), *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.

Commission européenne (2010b), « 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 », Communiqué de presse, IP/10/1430, 28 octobre 2010.

Commission européenne (2010c), *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 (2011a), *Attitudes à l'égard de la protection des données et de l'identité électronique dans l'Union européenne*, Rapports Eurobaromètre spéciaux, Bruxelles, 16 juin 2011.

Commission européenne (2011b), *Draft Agreement on the use of PNR between the EU and the United States*, SJ (2011) 603245, Service juridique de la Commission européenne, 18 mai 2011.

Commission européenne (2011c), *Options envisageables pour la création d'un système européen de surveillance du financement du terrorisme,* COM(2011) 429 final, Bruxelles, 13 juillet 2011.

Commission européenne (2011d), *Proposition de directive du Parlement européen et du Conseil relative à l'utilisation des données des dossiers passagers pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière*, COM(2011) 32 final, Bruxelles, 2 février 2011.

Commission européenne (2011e), *Rapport d'évaluation concernant la directive sur la conservation des données (directive 2006/24/CE)*, COM(2011) 225, Bruxelles, 18 avril 2011.

Commission européenne (2011f), *Report on the joint review of the implementation of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program,* Document de travail du personnel de la Commission, SEC(2011) 438 final, Bruxelles, 30 mars 2011.

Commission européenne (2011g), « Sûreté aérienne : la Commission adopte de nouvelles règles concernant l'utilisation des scanners de sûreté dans les aéroports européens », Communiqué de presse, IP/11/1343, 14 novembre 2011.

Commission européenne (2012), « La Commission européenne ouvre une procédure d'infraction accélérée contre la Hongrie concernant l'indépendance de sa banque centrale et de ses instances de protection des données et concernant certaines mesures relatives à son système judiciaire », Communiqué de presse, IP/12/24, Bruxelles, 17 janvier 2012.

Conférence annuelle des Commissaires à la protection des données et de la vie privée (2010), Résolution appelant à la convocation d'une conférence intergouvernementale aux fins d'adopter un instrument international contraignant sur le respect de la vie privée et la protection des données personnelles, 32e Conférence annuelle des Commissaires à la protection des données et de la vie privée, Jérusalem, Israël, 27-29 octobre 2010.

Conférence des Commissaires européens à la protection des données (2011), Résolution sur la nécessité d'un cadre global de protection des données, Bruxelles, 5 avril 2011.

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

Conseil de l'Europe (2011a), Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatise des données à caractère personnel, STE n° 108 T-PD (2011), Feuille de route, 19 avril 2011.

Conseil de l'Europe (2011b), *Rapport sur la consultation relative à la modernisation de la Convention 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel*, T-PD-BUR(2011) 10 en, Strasbourg, 21 juin 2011.

Conseil de l'Union européenne (2011), *Accord entre les États-Unis d'Amérique et l'Union européenne sur l'utilisation des données des dossiers passagers (données PNR) et leur transfert au Ministère américain de la sécurité intérieure*, 17434/11, 8 décembre 2011.

Derksen, R. (2011), « Zur Vereinbarkeit der Richtlinie über die Vorratsspeicherung von Daten mit der Europäischen Grundrechtecharta », WD 11 – 3000 – 18/11, février 2011.

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, JO 2006 L 105.

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.

Espagne, Agencia Española de Protección de Datos (2011), *Memoria 2010*, AEPD, 2011.

France, Commission nationale de l'informatique et des libertés (CNIL), (2011) Délibération n° 2011-048 du 17 février 2011 portant avis sur un projet d'arrêté modifiant l'arrêté du 28 janvier 2009 pris pour l'application de l'article 7 de la loi n° 2006-64 du 23 janvier 2006 et visant à proroger l'expérimentation du « fichier des passagers aériens » (FPA) jusqu'au 31 décembre 2011 (demande d'avis n° 1183168V2) CNIX1108803X, 31 mars 2011.

France, Le Fur, M. (2010), Question écrite n° 91193 de M. Marc Le Fur au Ministre de l'Intérieur, de l'outre-mer et des collectivités territoriales, 19 octobre 2010 ; réponse du Ministre de l'Intérieur, de l'outre-mer et des collectivités territoriales, disponible sur : http://questions.assemblee-nationale.fr/q13/13-91193QE.htm.

France, Tribunal de Boulogne-Billancourt , *Mme S. c. SAS Alten Sir*, 19 novembre 2010.

Groupe Article 29 sur la Protection des Données (2011), Avis 10/2011 sur la proposition de directive du Parlement européen et du Conseil relative à l'utilisation des données des dossiers passagers pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière, 00664/11/FR WP 181, 5 avril 2011.

Italie, Autorità per l'Aviazione Civile (2010), « In ENAC riunione cisa sui security scanner (body scanner): terminate prima fase sperimentazione senza risultati attesi », communiqué de presse, 19 décembre 2010.

Italie, Autorità per l'Aviazione Civile (2011), « Messa a punto dei security scanner L3 provision sugli aeroporti di Roma Fiumicino e Milano Malpensa », communiqué de presse, 9 mai 2011.

Le Monde (2011a), « Facebook propose de classer ses «amis» », 14 septembre 2011.

Le Monde (2011b), « Peut-on traiter son chef de minable sur Facebook ? », 10 mars 2011.

Lituanie, Lietuvos Respublikos Seimo Europos reikalų komitetas (2011), *Komiteto Išvados*, 2011.

Max Planck Institut für Ausländisches und Internationales Strafrecht (2012), *Rechtswirklichkeit der Auskunftserteilung über Telekommunikationsverbindungsdaten nach §§ 100g, 100h StPO, Forschungsbericht im Auftrag des Bundesministeriums der Justiz*, 27 janvier 2012.

Norvège, Data Inspection Board (2011), « Facebook's Response to Questions from the Data Inspectorate of Norway », septembre 2011.

Organisation de coopération et de développement économiques (OCDE) (2011a), Christopher Kuner, « Regulation of transborder data flows under data protection and privacy laws », *OECD Digital Economy Paper*, n° 187, 8 décembre 2011.

OCDE (2011b), « The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines », *OECD Digital Economy Papers*, n° 176, 6 avril 2011.

Parlement européen (2011a), « Rapport d'exécution SWIFT : importantes préoccupations en matière de protection des données », communiqué de presse, 16 mars 2011.

Parlement européen (2011b), Résolution législative du 27 octobre 2011 sur le projet de décision du Conseil relative à la conclusion de l'accord entre l'Union européenne et l'Australie sur le traitement et le transfert de données des dossiers passagers (données PNR) par les transporteurs aériens au service australien des douanes et de la protection des frontières, P7_TA-PROV(2011)0470, 27 octobre 2011.

Pays-Bas, Sénat (*Eerste Kamer der Staten-Generaal*) (2011a), *E110022 – Evaluatierapport over de dataretentierichtlijn*.

Pays-Bas, Sénat (*Eerste Kamer der Staten-Generaal*) (2011b), *Korte aantekeningen*, 5 juillet 2011.

Portugal, Comissão Nacional de Protecção de Dados (2011), Parecer n° 39, 9 mai 2011.

Règlement (CE) n° 460/2004 du Parlement européen et du Conseil du 10 mars 2004 instituant l'Agence européenne chargée de la sécurité des réseaux et de l'information, JO 2004 L 77.

Règlement (CE) n° 767/2008 du Parlement européen et du Conseil du 9 juillet 2008 concernant le système d'information sur les visas (VIS) et l'échange de données entre les États membres sur les visas de court séjour (règlement VIS), JO 2008 L 218.

Règlement (UE) n° 1077/2011 du Parlement européen et du Conseil du 25 octobre 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, JO 2011 L 286.

Règlement (UE) n° 1141/2011 de la Commission du 10 novembre 2011 modifiant le règlement (CE) n° 272/2009 complétant les normes de base communes en matière de sûreté de l'aviation civile en ce qui concerne l'utilisation de scanners de sûreté dans les aéroports de l'Union européenne, JO 2011 L 293/22.

Règlement d'exécution (UE) n° 1147/2011 de la Commission du 11 novembre 2011 modifiant le règlement

(UE) n° 185/2010 fixant des mesures détaillées pour la mise en œuvre des normes de base communes dans le domaine de la sûreté de l'aviation civile en ce qui concerne l'utilisation de scanners de sûreté dans les aéroports de l'Union européenne, JO 2011 L 294/7.

République tchèque, Chambre des députés, Résolution n° 446, 28 avril 2011.

République tchèque, Cour constitutionnelle (*Ústavní soud*), décision Pl ÚS 24/10, 22 mars 2011.

République tchèque, Loi sur la communication électronique, n° 127/2005 Coll., (*Zákon o elektronických komunikacích, 127/2005 Coll.*)

République tchèque, Sénat, Résolution n° 207, 28 avril 2011.

Roumanie, Curtea Constituțională a României, Décision n° 1258, 8 octobre 2009.

Roumanie, Sénat du Parlement roumain (2011), Avis motivé sur la proposition de directive du parlement européen et du conseil relative à l'utilisation des données des dossiers passagers pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière (COM(2011) 32 final), 6 avril 2011.

Royaume-Uni, European Scrutiny Committee (2011c), « Terrorist Finance Tracking Systems », Londres, 20 septembre 2011.

Royaume-Uni, Home Office (2011a), « EU Directive on Passenger Name Records », Communiqué de presse, Londres, 10 mai 2011.

Royaume-Uni, Home Office (2011b), « The UK's Opt-in to Council Decision to Sign and Conclude the EU-Australia PNR Agreement », Déclaration ministérielle écrite, 5 septembre 2011.

Royaume-Uni, House of Lords (2011), *The United Kingdom Opt-in to the Passenger Name Record Directive,* European Union Committee, Eleventh Report, HL Paper 113, The Stationery Office, Londres, 11 mars 2011.

Slovénie, Informacijski pooblaščenec (2011), Entretien avec un représentant, 7 octobre 2011.

Slovénie, Ministère de l'Intérieur (*Ministrstvo za notranje zadeve*) (2010), « Le Secrétaire d'État Goran Klemenčič participe à la réunion informelle du Conseil sur la Justice et les Affaires intérieures à Tolède », Communiqué de presse, 21 janvier 2010.

Suède, Commission de la justice, Parlement suédois (2010), *Propositions d'une résolution parlementaire sur l'utilisation des scanners corporels aux aéroports de l'UE (2010/11:JuU4)*, 23 novembre 2010.

Suède, Datainspektion (2011), « Facebook svarar de nordiska länderna », 20 septembre 2011.

Suède, Regeringskansliet (2010), *Lagring av trafikuppgifter för brottsbekämpande ändamål – genomförande av direktiv*, Proposition 2010/11:46 2006/24/EG.

Union européenne, États-Unis d'Amérique (2010), *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*, JO 2010 L 195/5.

ONU et CdE

Janvier

Février

Mars

Avril

Mai

21 juin – Le Bureau du Comité Consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du Conseil de l'Europe présente un rapport sur la consultation relative à la modernisation de la Convention 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel

Juin

Juillet

Août

Septembre

Octobre

Novembre

Décembre

UE

Janvier

2 février – La Commission européenne adopte une proposition de directive relative à l'utilisation des données des dossiers passagers (PNR) pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière

Février

16 mars – La Commission européenne publie son premier rapport sur l'examen conjoint de la mise en œuvre de l'accord Union européenne-États-Unis relatif au traitement des données de l'Union européenne (UE) et à leur transfert aux États-Unis pour le programme de surveillance du financement du terrorisme

Mars

18 avril – La Commission européenne adopte le rapport d'évaluation concernant la directive sur la conservation des données

Avril

Mai

16 juin – Publication du sondage Eurobaromètre spécial n° 359 sur les attitudes à l'égard de la protection des données et de l'identité électronique dans l'Union européenne

Juin

13 juillet – La Commission européenne adopte une communication au Parlement européen et au Conseil qui présente les options envisagées pour la mise en place d'un système européen de surveillance du financement du terrorisme

Juillet

Août

26 septembre – Le Conseil des ministres approuve les propositions de la Commission européenne concernant l'utilisation de scanners corporels dans les aéroports de l'UE

29 septembre – Signature de l'accord UE-Australie sur les données des dossiers passagers (PNR)

Septembre

25 octobre – L'UE adopte un règlement du Parlement européen et du Conseil portant création de l'Agence pour la gestion opérationnelle des systèmes d'information à grande échelle dans le domaine de la liberté, de la sécurité et de la justice

27 octobre – Le Parlement européen adopte une résolution législative sur le projet de décision du Conseil relative à la conclusion de l'accord entre l'Union européenne et l'Australie sur le traitement et le transfert de données des dossiers passagers (données PNR) par les transporteurs aériens au service australien des douanes et de la protection des frontières

Octobre

10 novembre – La Commission européenne adopte un règlement complétant les normes de base communes en matière de sûreté de l'aviation civile en ce qui concerne l'utilisation de scanners de sûreté dans les aéroports de l'UE

11 novembre – La Commission européenne adopte un règlement d'exécution fixant des mesures détaillées pour la mise en œuvre des normes de base communes dans le domaine de la sûreté de l'aviation civile en ce qui concerne l'utilisation de scanners de sûreté dans les aéroports de l'UE

24 novembre – La Cour de justice de l'Union européenne rend un arrêt dans deux affaires relatives à la protection des données à caractère personnel et à la société de l'information : *ASNEF et FECEMD c. Administración del Estado* et *Scarlet Extended SA c. Société belge des auteurs, compositeurs et éditeurs*

Novembre

13 décembre – Le Conseil des ministres donne son feu vert pour le nouvel accord UE-États Unis sur les données des dossiers passagers (données PNR)

Décembre