Passenger Name Record 2012

Par Claudine GUERRIER

Professeur de droit à Institut des Mines Télécom, Télécom Ecole de Management

Claudine.Guerrier@telecom-em.eu

Introduction

Le 25 avril 2012, le Parlement européen, sur la base du traité d'Amsterdam, adopte la nouvelle mouture de l'accord entre les USA et l'Union européenne relatif à l'utilisation et au transfert des données des dossiers passagers[1] au ministère américain de la sécurité intérieure.

L'Organisation de l'aviation civile internationale (OACI) s'est préoccupée depuis longtemps du « *Passenger Name Record* ». Les compagnies aériennes collectent des informations auprès des passagers dans le cadre des services de réservation. Ces informations sont stockées dans les bases de données des systèmes de réservation, puis échangées entre les sociétés intervenantes du moment de la réservation jusqu'à la réalisation des prestations demandées par les passagers. Les données qui sont présentes dans ces bases sont des enregistrements d'informations standardisées au plan international et dénommées « *PNR* ». Le PNR contient, en fonction des prestations offertes par les compagnies et demandées par le client, des indications précises : les nom et prénom du client, les renseignements sur l'agence de voyage auprès de laquelle la réservation est effectuée, l'itinéraire du déplacement, les éléments afférents aux vols : numéro des vols successifs, date, heures, classe, le groupe de personnes pour lesquelles une même réservation est faite, le contact à terre du passager ; coordonnées téléphoniques et électroniques, les tarifs acceptés, l'état du paiement effectué et ses modalités par carte bancaire, les réservations d'hôtels ou de voitures à l'arrivée, les services demandés à bord : numéro de place affecté à l'avance, les repas, les services induits par l'état de santé. Il est rare que tous les champs soient remplis.

Les données PNR ne sont pas confondues avec les données APIS[2], qui sont collectées par les compagnies lors de la phase d'enregistrement des passagers sur un vol. Elles englobent le numéro et le type du document de voyage utilisé, la nationalité, le nom complet, la date de naissance, le point de passage frontalier utilisé pour entrer sur le territoire des Etats membres, le code de transport, les heures de départ et d'arrivée du transport, le nombre total des personnes transportées et le point d'embarquement initial. Il existe moins de données APIS que de données PNR. Néanmoins, les données APIS sont intéressantes dans la mesure où elles sont vérifiées par le personnel des transporteurs au moment de l'enregistrement du vol. Les données PNR sont fournies par les voyageurs au stade de la réservation commerciale, qui peut changer jusqu'à l'embarquement.

Avant 2001, les données PNR stockées à des fins commerciales par les opérateurs pouvaient être requises par les autorités judiciaires afin de satisfaire aux besoins d'une enquête ou d'une instruction. Après les attentats de septembre 2001, et la large exploitation médiatique et politique qui est réalisée autour de ces évènements, des lois sécuritaires sont adoptées aux USA puis dans d'autres pays alliés des USA, notamment l'Australie et le Canada. Les USA, l'Australie, le Canada se dotent alors de « *systèmes PNR* » qui donnent ensuite lieu à des accords avec l'Union européenne. Le système américain est le plus ancien et le plus abouti. Le 19 novembre 2001, les USA adoptent une loi sur la sécurité de l'aviation et du transport[3] ; le 5 mai 2002 une loi assez stricte relative aux conditions d'entrée sur le territoire américain[4] entre en vigueur. La loi de 2002 stipulait qu'à partir du 5 mars 2003, les compagnies aériennes devaient communiquer aux services des douanes et de sécurité

[1] PNR
[2] Advance Passenger Information System
[3] The Aviation and Transportation Security Act
[4] Enhanced Border Security and Visa Entry Reform Act

américains des informations personnelles afférentes à leurs passagers, sous peine de contrôles renforcés, d'amendes, voire de suspension du droit d'atterrir. Ces dispositions concernent donc les personnes physiques voyageurs et les personnes morales que sont les compagnies aériennes, les services de sécurité américains[5].L'IAO avait pour finalité d'assurer une surveillance technologique, automatique et permanente de toutes les formes possibles d'information qui permettraient de signaler les prémices d'une éventuelle activité terroriste. Ce projet baptisé *Terrorism Information Awareness*[6] avait pour but d'établir des connexions entre des données policières et judiciaires et des comportements tels que la demande d'un visa, l'utilisation d'une carte de crédit… Le TIA comportait plusieurs autres volets tels la surveillance de banque de données médicales ou la transcription automatique de communications en langues étrangères. Ce projet, âprement discuté par les défenseurs des libertés individuelles a été supprimé en septembre 2003 et fut remplacé par le CAPPS[7] et CAAPS 2, qui s'applique, pour ce dernier, uniquement aux utilisateurs des transports aériens.

Au sein de l'Union européenne, le Royaume-Uni est le seul Etat-membre à posséder un système PNR complet dans le cadre du programme e-borders. Entré en vigueur en mars 2008, il regroupe à la fois la collecte des données APIS et les données PNR. Le système britannique n'établit pas a priori de distinction entre les vols en provenance d'un état membre de l'Union européenne ou d'un état tiers. En Belgique, les services de police sont en mesure dans le cadre d'une autorisation judiciaire de demander aux compagnies aériennes un accès à leurs données PNR. En France, l'article sept de la loi du 23 janvier 2006[8] autorise la collecte et l'exploitation des données PNR et APIS. Sont en fait concernées les données APIS, les données PNR, les données collectées à partir de la bande de lecture optique[9] des documents de voyage, de la carte nationale d'identité et des visas des passagers de transporteurs aériens, maritimes, ferroviaires ; grâce à cette technique, il est possible d'enregistrer les données contenues dans la bande optique, y compris quand les agents aux frontières sont confrontés à l'arrivée simultanée de plusieurs vols. La loi de 2006 écarte par contre l'utilisation des données dites sensibles au sens de la directive 95/46 et au sens de l'article 8 de la loi du 6 janvier 1978 modifiée par la loi du 6 août 2004. Ainsi les données concernant les types de repas à bord[10] ou l'état de santé du voyageur ne sont pas susceptibles de faire l'objet de transmissions. La mise en œuvre de la loi du 23 janvier 2006 a abouti à la création du Fichier des passagers aériens[11] par un arrêté du 19 décembre 2006. Cette expérimentation ne concernait que les données APIS des passagers des vols directs en provenance et à destination de l'Afghanistan, du Pakistan, de l'Iran, de la Syrie, du Yémen. Cette expérimentation n'a pas été concluante en raison du manque de rigueur constaté dans la transmission des données par certaines compagnies et en raison de la multiplicité d'erreurs imputables à des homonymies ou à des transcriptions inexactes des noms. Toutefois, La France n'est pas inexpérimentée puisqu'elle applique l'article 65 du code des douanes qui permet aux douanes de requérir ponctuellement et expressément les données PNR de certains vols.

L'Australie et le Canada ont mis en place des systèmes PNR. En dépit des divergences qui existent en matière de protection des données à caractère personnel entre le droit de l'Union européenne, les droits de l'Australie et du Canada, et surtout le droit des USA, les problèmes techniques ont été résolus dans la gestion des données de voyage par les opérateurs, qui souhaitent néanmoins une harmonisation pour diminuer le coût des transmissions.

Cette harmonisation n'a cessé de poser des problèmes juridiques à l'occasion des accords passés entre l'Union européenne et l'Australie, l'Union européenne et le Canada, l'Union européenne et les USA. Le focus est ici celui de la relation Union européenne/USA.

---

[5] En janvier 2002, est créé *l'Information Awareness Office*, (IAO)
[6] TIA
[7] Computer Assisted Passenger Prescreening System
[8] Loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme
[9] Dénommée « *MRZ* »
[10] Qui peuvent être révélatrices de convictions religieuses
[11] FPA

Après avoir tiré les leçons des accords passés depuis 2004, la problématique se centrera sur le difficile équilibre de 2012 entre paramètres de sécurité et paramètres de liberté.

I) L'Union européenne et les USA ont été contraints de tirer les leçons des étapes : 2004, 2007.

A) La première confrontation : 2004

1) La directive 2004/82/CE du Conseil du 29 avril 2004

Elle oblige les transporteurs à communiquer les données relatives aux passagers, en se fondant sur l'accord de Schengen et règle les échanges de données PNR, dans un but officiel de lutte contre le terrorisme et contre l'immigration illégale. Selon l'article douze, elle autorise « *l'utilisation de ces données comme élément de preuve dans des procédures visant à l'application des lois et des règlements sur l'entrée et l'immigration, notamment des dispositions relatives à la protection de l'ordre public et de la sécurité nationale* ».

2) L'accord de mai 2004 USA/Union européenne

Les USA sollicitent l'Union européenne en 2004 afin d'obtenir un accès complet aux PNR des compagnies européennes. En mai 2004, USA et UE signent le *« 2004 Passenger Name Record Data Transfer agreement* » qui permet au CBP d'accéder à 34 informations contenues dans le PNR. A cette date, l'Union européenne se considère satisfaite par le niveau de protection des données garanti par les autorités américaines, dans la mesure où elles les utilisent dans le cadre prévu, à savoir « *prévenir et combattre les attaques terroristes et du crime organisé international* ». Mais ces exigences américaines heurtaient les règles européennes en matière de protection des données à caractère personnel[12]. Cet accord est invalidé par la Cour européenne de justice[13].

B) L'accord de 2006-2007

1) Un accord nécessaire

L'accord était nécessaire pour que les compagnies aériennes sachent comment réguler le flux des informations. L'accord est conclu le 19 octobre 2006 et entre en vigueur le 1er août 2007.

2) Le contenu de l'accord de 2007

L'accord, matérialisé par la décision du conseil du 23 juillet 2007[14], se situe dans le cadre du troisième pilier européen, consacré aux questions de police et de justice. Il a une durée de sept ans et est applicable à partir du 23 juillet 2007. Au bout de sept ans, les données devraient être stockées dans une base inactive pour une durée de huit ans, pendant laquelle l'accès au Department of Homeland Security n'est possible que dans des situations exceptionnelles ou lorsque des vies sont en jeu. Le nombre d'informations transmises est réduit à 19. Néanmoins, le DHS peut transférer les données PNR à d'autres autorités gouvernementales et il lui est loisible, certes dans des cas circonscrits, d'accéder à des données sensibles, c'est-à-dire aux données pouvant révéler l'origine ethnique, les convictions religieuses, politiques ou un problème de santé ; les finalités du système sont larges et évolutives. Aucune garantie n'est apportée sur la destruction au bout de quinze ans-les sept années initiales et les huit années supplémentaires- des données concernées. C'est pourquoi cet accord est

[12] C'est la directive-cadre 95/46/CE votée par le Parlement européen et le Conseil qui est le texte de référence au niveau de la protection de la vie privée et des données à caractère personnel ; elle est complétée par la directive du 12 juillet 2002 sur la protection de la vie privée et des données à caractère personnel dans le secteur des communications électroniques complétée par la directive du 25 novembre 2009 sur le service universel et la protection de la vie privée et des données à caractère personnel dans le secteur des communications électroniques

[13] C.J.CE., Grande chambre, 30 mai 2006, Parlement européen c. Conseil de l'Union européenne, Affaires jointes C-317/04 et C-318/04 (la décision 2004/235 est exclue du champ d'application de la directive 95/46)

[14] 2007/551/PESC/JAI

souvent critiqué au sein de l'Union européenne, chez certains eurodéputés, au niveau institutionnel, au niveau des organismes de régulation des données à caractère personnel, y compris le G29, au niveau des associations de défense des droits de l'homme et des libertés individuelles. Dès le mois de décembre 2007, le G29 initie un rapport qui remet en cause les principes de base de l'accord : « *Dans sa rédaction actuelle, la proposition de décision-cadre prévoit la collecte d'un grand nombre de données à caractère personnel relatives aux passagers aériens ou sortant de l'Union européenne, indépendamment du fait qu'ils soient soupçonnés ou innocents. Ces données seront ensuite conservées ….en vue d'un éventuel usage ultérieur, permettant ainsi le profilage des voyageurs. Cette proposition s'ajoute au relevé des empreintes digitales de tous les voyageurs demandant un passeport, et à la conservation de toutes les données liées au trafic des télécommunications au sein de l'UE. (…) Un régime PNR européen ne saurait aboutir à la surveillance généralisée de tous les passagers* »[15]. Les USA, eux, considèrent qu'il s'agit d'un bon accord pour le droit de l'Union européenne. Le dit accord protègerait à la fois les données recueillies et la vie privée des personnes physiques. Aucun cas de détournement de données PNR par le gouvernement américain n'a été décelé depuis le début des transferts. Soulignons que l'accord de 2007 est un accord provisoire.

A la suite des nombreuses critiques émises par certains eurodéputés, ces derniers font savoir en mai 2010 qu'ils souhaitent renforcer la protection des données à caractère personnel des passagers aériens dans le dossier PNR. Le 5 mai 2010, le Parlement européen adopte une résolution qui demande une renégociation de l'accord. Le 2 décembre 2010, le Conseil autorise la Commission à négocier un nouvel accord sur le transfert des données PNR. Les objectifs sont clairement déterminés : encouragement de la coopération entre les USA et l'Union européenne dans un esprit de partenariat transatlantique, lutte contre le terrorisme tout en respectant les droits fondamentaux et en reconnaissant l'importance de la vie privée, prise en compte de la sécurité des voyageurs et protection des frontières. Les USA entament la négociation car ils redoutent que l'accord de 2007, provisoire, ne soit pas reconduit en 2014. Le précédent de l'affaire SWIFT amène les USA à prendre le Parlement européen au sérieux.

C) Les contrôles exercés au sein de l'Union européenne

1) La Cour européenne de justice

L'accord du 28 mai 2004 a été dénoncé par l'Union européenne à la suite de l'arrêt rendu le 30 mai 2006 par la Cour européenne de justice parce qu'il ne présentait pas une base juridique appropriée. En effet, l'accord du 28 mai 2004 se fondait sur la base du premier pilier. Les champs de compétence de l'Union européenne sont répartis en trois piliers : le premier pilier englobe les matières relatives au marché intérieur et à la libre circulation ; le deuxième pilier s'intéresse aux questions de défense et de politique étrangère ; le troisième pilier est concerné par les questions de police et de justice. En 2004, les règles d'adoption des textes européens différaient selon les piliers : le premier pilier correspondait à la majorité qualifiée, la codécision avec le Parlement européen et le contrôle de la Cour de justice ; le troisième pilier correspondait à l'unanimité, à l'avis simple du Parlement européen et à l'absence de contrôle de la Cour de justice. Cette dernière a considéré que l'accord de 2004 n'était pas approprié puisqu'il était arrêté dans le cadre du premier pilier. En effet, le traitement lié au transfert des données PNR aux autorités américaines avait pour finalité la sécurité publique ; un accord devait être conclu dans le cadre du troisième pilier.

2) Le G29

Il ne prend pas de décision mais fait connaître son opinion sur les accords et notamment sur l'accord de 2007.

2.1) L'utilité en matière de lutte contre le terrorisme et la criminalité

[15] G29, avis 2/2007 concernant l'information des passagers au sujet du transfert des données des dossiers passagers (Passenger Name Record, PNR) aux autorités américaines, adopté le 15 février 2007

Le G29 souligne que les USA « *n'ont jamais prouvé de façon concluante que la quantité considérable de données passagers collectée est véritablement nécessaire à la lutte contre le terrorisme et la grande criminalité (…) Les seules informations fondées disponibles à cette fin indiquent que les données API*[16] *sont davantage utilisées que les données PNR* ». Au demeurant, le G29 fait remarquer que l'Union européenne dispose déjà du système d'information Schengen[17].

2.2) Réciprocité et démocratie

Le G29 se soucie des conséquences éventuelles de l'accord et, notamment, des conséquences de la réciprocité automatique avec les pays tiers qui ont recours à un système PNR : « *Il faut se rendre compte que l'existence d'un régime PNR européen pourrait inciter des régimes non démocratiques ou corrompus à exiger la communication de PNR sur la base du principe de réciprocité. Il convient dès lors de se demander si les conséquences de cette réciprocité ont été suffisamment étudiées* ». Le G29 mentionne en particulier la détention d'informations relatives aux cartes de crédit par des fonctionnaires d'un Etat membre incapable de supprimer la corruption. Par ailleurs, la lutte contre le terrorisme peut revêtir une acception différente de celle qui prévaut au sein de l'Union européenne : « *La réciprocité pourrait ainsi permettre à une dictature d'établir une évaluation des risques présentés par les dissidents, à partir des données PNR* ».

2.3) Le contrôleur européen pour la protection des données[18] et le profilage

Le CEPD critique la technique du profilage qui élabore des hypothèses de risque à partir de données à caractère personnel ne correspondant pas à une infraction. La mise en forme de déplacement et de comportement conduit à fonder des décisions à l'encontre de personnes physiques qui auraient par la suite beaucoup de difficultés à se défendre contre ces décisions. Surtout, selon le contrôleur européen pour la protection des données, les principes de finalité et de proportionnalité ne seraient pas observés. Le droit afférent à la protection des données est flou ou inexistant. La durée de conservation semble excessive.

3) Le Parlement européen

Il a manifesté des réserves.

3.1) A l'occasion de l'Accord de Washington

L'Accord de Washington en date du 28 mai 2004 entre les USA et l'Union européenne a été critiqué par le Parlement européen. Cet Accord de Washington permet aux USA de récupérer dans les systèmes de réservation, des informations personnelles supplémentaires susceptibles de l'intéresser. L'accord établit une liste de données PNR auxquelles le CBP a accès : « *Le CBP extraira des informations des systèmes de réservation des compagnies aériennes jusqu'à ce que celles-ci puissent exporter ces données vers le CBP ». L'Accord de Washington peut largement rentrer en conflit avec la législation européenne sur la protection des données à caractère personnel. L'Union européenne s'est alignée sur la législation américaine en matière de transport aérien* ». L'article 4 de l'Accord de 2004 concernant les dossiers PNR rappelle que « *le CBP traite les données PNR reçues et les personnes concernées par ce traitement conformément aux lois et exigences constitutionnelles américaines* ». Aussi, en s'appuyant sur l'article 230 CE, le Parlement européen demande l'annulation de la décision du Conseil d'approuver l'accord avec les USA d'une part et la décision d'adéquation à cet accord de la Commission d'autre part. Parmi les éléments sur lesquels s'appuie le Parlement européen pour contester la décision du Conseil, il convient de mettre l'accent sur les points suivants :

[16] Advanced Passengers System
[17] SIS
[18] Avis du 1er mai 2008

-La violation du droit à la protection des données à caractère personnel du point de vue de la directive-cadre 95/46/CE, la violation du principe de proportionnalité qui implique que les actions menées et les moyens utilisés par l'Union européenne ne sont pas disproportionnés et n'excèdent pas les objectifs des traités de l'Union

-La violation du principe de coopération loyale prévu par l'article 10 CE

-Le choix fallacieux d'utiliser l'article 95 CE comme base juridique pour la décision du Conseil. En effet, l'article 95 CE vise l'adoption par le Conseil « *de mesures relatives au rapprochement des dispositions législatives, réglementaires et administratives des Etats membres qui ont pour objet l'établissement et le fonctionnement du marché intérieur* ». Il ne peut donc servir de base pour le rapprochement de législation entre l'Union européenne et un pays tiers tel que les USA.

Dans l'affaire concernant la décision d'adéquation de la Commission aux accords PNR, le Parlement européen soulève entre autres, les éléments suivants pour la contester :

-Un excès de pouvoir, la violation des droits fondamentaux et la violation du principe de proportionnalité.

-La violation de l'article 300 de la directive-cadre 95/46 afférente à la protection des données à caractère personnel. Une modification de cette directive implique que le transfert de ces données à un pays tiers n'est possible que si celui-ci a un niveau de protection adéquat. Si la Commission décide que ce présupposé est rempli par les USA[19], qu'en sera-t-il si les USA décident de transférer ces données à un partenaire étranger ?

-La violation des principes essentiels de la directive 95/46 et notamment de son article 25 qui stipule que « *les personnes dont les données font l'objet d'un traitement ont le droit d'être informées sur celui-ci, de pouvoir accéder aux données, de pouvoir demander leur rectification, voire de s'opposer au traitement dans certaines circonstances* ».

Enfin, la législation européenne donne un cadre très clair concernant la collecte des données à caractère personnel. Cette collecte peut en effet se faire dans le cadre de la sécurité publique et à des fins répressives. Or ici, les données contenues dans les dossiers PNR sont collectées dans le cadre d'une prestation de service effectuée par les compagnies aériennes. Par conséquent, on peut considérer que la collecte des données PNR dans le cadre d'une activité économique est juridiquement infondée dans le droit européen. Et le Parlement ne vote pas l'accord de 2004.

3.2) L'accord PNR 2007

Un avis négatif sur l'accord n'est pas pris en compte. Le Parlement adopte une résolution en date du 20 novembre 2008[20]. Il partage le jugement du contrôleur européen pour la protection des données sur l'imprécision du texte mais il est plus nuancé sur l'utilité des données PNR pour les services en charge de la lutte contre le terrorisme et la grande criminalité. Le Parlement européen considère que ces données peuvent être utiles comme éléments de preuve dans une enquête. En revanche, il nourrit des doutes quant à la pertinence d'un éventuel profilage préventif.

Les contrôles ont donc largement mis en exergue les insuffisances des accords de 2004 et 2007.

II) Le texte adopté par le Parlement en 2012 met l'accent sur la sécurité et des critiques subsistent[21]

A) Le nouveau texte reflète un souci de sécurité

[19] Safe Arbor Principles
[20] Résolution n°2008/0561
[21] http://register.consilium.europa.eu/pdf/fr/11:st17/st7434.FR11.pdf

1) Il souhaite parvenir à un équilibre

L'Union européenne et les USA ont paraphé le 17 novembre 2011 un accord nouveau afférent au transfert des données des passagers aériens des vols originaires de l'Union européenne à destination des USA, qui doit se substituer à l'accord de 2007.

1.1) Un partage avec l'Union européenne

Les autorités américaines sont tenues de partager les dossiers passagers et les informations analytiques tirées de ces données avec les autorités répressives et judiciaires de l'Union européenne afin de prévenir et de détecter la criminalité transnationale ou les infractions terroristes, de mener des poursuites.

1.2) Utilisation et durée de conservation

Les autorités américaines utilisent les données PNR pour la prévention et la détection du terrorisme et des infractions transnationales passibles d'une peine d'emprisonnement d'au moins trois ans. Les infractions mineures sont exclues ; sont concernées des infractions graves telles le trafic de drogue, la traite des êtres humains, le terrorisme. Les données PNR sont dépersonnalisées six mois après leur réception par les autorités américaines. Au bout de cinq ans, les données dépersonnalisées sont transférées dans une base de données non active, à laquelle les responsables américains ont accès sous conditions. La durée totale de conservation des données est limitée à dix ans d'une manière générale mais les données seront accessibles pendant quinze ans pour les affaires de terrorisme. Il est rappelé que les données PNR sont transférées aux autorités américaines à partir des bases de données des transporteurs aériens[22] et non à partir des systèmes de réservation[23], sauf dans certaines circonstances limitativement énumérées[24], comme lorsque les transporteurs aériens se trouvent dans l'incapacité technique de transmettre les données.

1.3) La protection des données à caractère personnel

Elle est le sujet qui a donné lieu à de nombreuses controverses juridiques. Mme Cecilia Malmström[25] a mis l'accent sur cet aspect : « *La protection des données à caractère personnel a été ma priorité dès le début des négociations en décembre 2010, et je suis satisfaite du résultat obtenu, car il représente une nette amélioration par rapport à l'accord de 2007 actuellement en vigueur. Ce nouvel accord contient des garanties solides pour le respect de la vie privée des citoyens européens sans porter atteinte à l'efficacité de l'accord en ce qui concerne la sécurité de l'Union européenne et des USA*[26]. »
Le Congrès a exigé la nomination d'un responsable de la vie privée au ministère de la sécurité intérieure qui doit rendre compte de l'état des lieux au Congrès chaque année et dont les conclusions sont contraignantes pour le ministère. Le responsable de la vie privée a accepté de recevoir et de traiter en urgence les démarches des autorités chargées de la protection des données dans l'Union européenne pour le compte des citoyens qui considèrent que le ministère de la sécurité intérieure n'a pas statué de manière satisfaisante sur leurs plaintes.

Les passagers peuvent obtenir l'accès à leurs données PNR, les corriger et les supprimer. Ils ont également le droit de former des recours administratifs et judiciaires tels qu'ils sont prévus par la législation américaine. Les transporteurs aériens doivent en outre informer avec précision les passagers de l'utilisation des dossiers PNR et des modalités de l'exercice de leurs droits. L'accord interdit aux autorités américaines de prendre des décisions pouvant porter préjudice à quelqu'un sur le seul fondement d'un traitement automatisé des données : cela correspond aux craintes de

[22] Selon la méthode de transfert « *push* »
[23] Selon la méthode « *pull* »
[24] Exemple : les transporteurs aériens se trouvent dans l'incapacité technique de transmettre les données
[25] Commissaire chargée des affaires intérieures
[26] Déclaration de Cecilia Malmström, Source : communiqué de presse de la Commission européenne sur l'accord des données PNR, 18 novembre 2011

profilage. L'accord fixe également des conditions limitant l'utilisation des données sensibles pouvant révéler, par exemple, la religion ou l'orientation sexuelle des passagers. Pour ce faire, sont mis en place des mécanismes de filtre et masque des données sensibles.

1.4) Sécurité des données

Des mesures techniques appropriées et des aménagements organisationnels doivent être mis en place afin de protéger les données à caractère personnel contenues dans les PNR, des accidents, destructions, pertes, modifications, accès, traitements ou utilisations illégales. La protection, la confidentialité et l'intégrité des données avec le cryptage, les procédures d'autorisations et de documentation doivent être assurées. Des sanctions disciplinaires sont engagées à l'égard de toute personne responsable d'un incident relatif à des données privées : appropriation, refus d'accès au système, suspensions.

2) L'option sécuritaire

Même si un souci d'équilibre apparaît et si les USA ont pris en compte, du moins partiellement, le droit de l'Union européenne en matière de protection des données à caractère personnel, l'accord reflète une prééminence de l'exigence de sécurité. Les crimes et délits pour lesquels les USA peuvent utiliser les données PNR afin d'enquêter, de poursuivre en justice sont assez nombreux : ils comprennent d'une part les offensives terroristes et certains autres crimes[27], d'autre part les crimes internationaux graves. Les crimes qui sont adjoints à la rubrique « *offensives terroristes* » sont les comportements dangereux à l'égard de la vie humaine, propriété ou infrastructure, ou supposés vouloir intimider une population civile, influencer par l'intimidation la politique d'un gouvernement ou affecter la conduite d'un gouvernement par la destruction massive, l'assassinat, le kidnapping, la prise d'otages, les collectes de fonds réalisées dans l'intention, directe ou indirecte, de prodiguer l'un des actes mentionnés précédemment, la tentative, la complicité la menace de commettre l'un des actes précédents. Les crimes internationaux graves sont définis par l'article quatre de l'accord sur l'extradition entre les USA et l'Union européenne. La liste des crimes et des délits concernés est donc assez longue.

B) Des critiques subsistent, notamment au niveau du Parlement européen

En mai 2010, le Parlement européen avait repoussé son vote sur un accord PNR avec les USA, appliqué de manière provisoire depuis 2007, principalement en raison de son inquiétude au sujet de la protection des données à caractère personnel. Les euro-députés avaient alors instamment invité la Commission européenne à négocier un nouvel accord, ce qu'elle a fait en 2011. L'accord est devenu effectif après avoir été adopté le 19 avril 2012 par 409 voix pour, 226 voix, 33 abstentions, en raison des mots d'ordre en faveur de ce texte des principaux groupes parlementaires. Le président du groupe social-démocrate a indiqué qu'il soutenait l'accord en dépit de ses lacunes, mais il respectera la liberté de vote des membres de son groupe. Néanmoins, la très grande majorité des euro-députés sociaux-démocrates s'est prononcée en faveur de l'accord. Comme les groupes conservateurs[28] soutenaient l'accord, le résultat était acquis.

1) Une minorité d'euro-députés contre l'accord

Cependant, une minorité significative d'euro-députés a rejeté l'accord dans la mesure où ces parlementaires n'étaient pas convaincus par les garanties prises dans le domaine de la protection des données à caractère personnel. La rapporteure, Sophie In't Veld[29] a retiré son nom du rapport car ses réserves étaient nombreuses. Le groupe des libéraux s'est engagé contre le texte et son président, Guy Verhofstadt l'a fait savoir. Les libéraux ont été rejoints par les Verts. Pour ces partis, un coup a

[27] Cf ci-dessous
[28] Notamment le *PPE*
[29] *ADLE*,NL

été porté au droit européen, et, en particulier, au droit européen en matière de données à caractère personnel : « *La décision prise aujourd'hui par les conservateurs et les sociaux-démocrates de voter en faveur de l'accord constitue un pas vers un Etat*[30] *policier* » et « *Pour la première fois depuis dix ans, le Parlement avait l'opportunité d'arrêter le profilage… mais une majorité a choisi de passer à côté* ». Sophie in'T Veld explique : « *Certaines choses ne sont pas négociables comme les droits fondamentaux et le respect de la législation de l'Union européenne*[31]*. Apparemment, le Parlement estime que les relations transatlantiques sont plus importantes* ». Elle s'interroge aussi : pourquoi le Parlement « *qui recale les accords en 2007, puis en mai 2010 et a même saisi la cour de justice a fini par accepter un accord encore plus mauvais*[32] *? Pourquoi le Parlement accepte-t-il PNR et refuserait-il ACTA*[33] ? » Remarquons que le mouvement d'opinion contre ACTA a été en partie pris en compte dans la mesure où une pétition contre ACTA a été signée par plus de deux millions de personnes.

2) Le contrôleur européen des données, Peter Hustinx, a exprimé ses réserves

Il l'a fait vivement, et il a essayé de se faire entendre par les euro-députés, mais en vain. Il a précisé la ligne de conduite du CEPD : « *Les données personnelles des passagers aériens pourraient certainement être nécessaires à des fins répressives dans des cas bien déterminés, quand survient une menace sérieuse appuyée par des indicateurs concrets. C'est leur utilisation de façon systématique et sans discernement pour tous les passagers qui soulève des préoccupations particulières*[34] ». Le CEPD admet que des améliorations relatives à la protection des données par rapport à l'accord de 2007 sont notables, notamment en ce qui concerne la restriction du champ d'application et les conditions de traitement des données PNR.

Néanmoins, le nouvel accord n'est pas conforme à la législation européenne. Le fait même d'imposer aux transporteurs aériens de fournir aux Etats membres de l'Union européenne les données des dossiers passagers de vols à destination ou en provenance du territoire de l'Union afin de lutter contre le terrorisme et des formes graves de criminalité est contestable. Un tel système ne serait pas nécessaire, et le texte ne fournit pas d'élément démontrant le contraire. En effet, la nécessité de recueillir ou de stocker d'importantes quantités de données à caractère personnel doit s'appuyer sur une démonstration de la relation entre l'utilisation et le résultat[35].

Le CEPD regrette donc que le champ d'application des données collectées demeure trop vaste. En outre, aucune donnée ne devrait être conservée au-delà de trente jours sous une forme identifiable.

Le G29, quant à lui, critique le manque de dispositions visant à assurer la sécurité des données personnelles quant à la vie privée : « *Dans sa rédaction actuelle, […] prévoit la collecte d'un grand nombre de données à caractère personnel*[36] *relatives aux passagers aériens entrant ou sortant de l'Union européenne, indépendamment du fait qu'ils soient soupçonnés ou innocents. Ces données seront ensuite conservées (…), en vue d'un éventuel usage ultérieur, permettant ainsi le profilage des voyageurs. Cela s'ajoute au relevé des empreintes digitales de tous les citoyens demandant un passeport, et à la conservation de toutes les données liées au trafic des télécommunications au sein de l'Union européenne. Un régime PNR ne saurait aboutir à la surveillance généralisée de tous les passagers* ».

3) Les critiques des juristes

Certains juristes mettent l'accent sur certains points-qui leur paraissent discutables-de l'accord.

---

[30] Déclaration de Jan Philip Albrecht
[31] Recommandation de la rapporteure contraire au rapport, D66, Pays-Bas, 19 avril 2012
[32] Depuis le traité de Lisbonne, le Parlement européen doit se prononcer
[33] L'accord sur la contrefaçon conclu entre pays occidentaux et anciennement industrialisés, et critiqué par les pays émergents qui ne sont pas partie prenante
[34] Avis du contrôleur européen de la protection des données Peter Hustinx, 19 avril 2012
[35] Principe de nécessité
[36] Avis du G29, 29 mars 2012

3.1) PNR et extradition

La référence aux crimes passibles d'extradition n'a pas sa place dans un accord sur les PNR puisque cette notion vise seulement des suspects ou des coupables et non des personnes a priori innocentes. Cette clause serait susceptible d'élargir l'utilisation des données PNR à n'importe quel but, à condition qu'elle soit ordonnée par un tribunal. Les données PNR seraient également susceptibles, dans certains cas, de servir pour assurer la sécurité des frontières, alors que leur utilisation est censée servir à la prévention du terrorisme et des crimes graves, et non pour traquer des migrants clandestins ou pour combattre des délits de douane. De plus, ces procédés ne sont pas toujours efficaces, notamment en matière de terrorisme, étant entendu que c'est la lutte contre le terrorisme qui a justifié les PNR et les accords PNR. Les USA ont indiqué que grâce au PNR, deux « *dangereux terroristes* » ont pu être arrêtés[37]. Deux terroristes en dix ans ne constituent pas un bilan très convaincant. Les autorités indiennes se sont par ailleurs indignées de la facilité avec laquelle l'un des « *terroristes* »[38] était parvenu à prendre si souvent l'avion entre le Pakistan, l'Inde et les USA.

3.2) La durée d'utilisation

Elle va bien au-delà du projet d'accord avec l'Australie[39]. Ce dernier accord est réputé équilibré et plus favorable à l'Union européenne. La période de rétention des données n'est pas de quinze ans, mais indéfinie. Il est exact que l'accès aux données par le ministère américain de la sécurité intérieure sera progressivement restreint. Néanmoins, les données ne seront pas effacées. Il est même possible de parler de recul par rapport à l'accord de 2004 si l'on envisage la durée de stockage. Enfin, des critiques se sont élevées contre la réversibilité de la dépersonnalisation. L'accord prévoit de masquer les données PNR après six mois mais elles peuvent être re-personnalisées par des personnes ayant les droits d'accès spéciaux.

3.3) Les données sensibles

L'accord ne prévoit pas l'effacement immédiat des données dites « *sensibles* », contrairement à l'accord de 2004. Ainsi une préférence alimentaire peut être révélatrice d'une appartenance religieuse. Une réservation d'hôtel ou un choix d'itinéraire sont susceptibles de donner des indications sur une orientation sexuelle. Une demande d'assistance médicale peut laisser deviner un état de santé. Désormais, ces données sensibles ne seront pas effacées dans tous les cas au bout de trente jours, si elles entrent dans le cadre d'une enquête spécifique. Il y a donc un risque potentiel de dérive.

3.4) La sécurité des données et les erreurs

Plusieurs pays, dont l'Allemagne, l'Autriche, la Belgique sont inquiets des risques de fuites de données lors de leur transmission à des pays tiers, notamment en ce qui concerne le transfert des données PNR. De plus, des erreurs peuvent se produire et se sont déjà produites dans le traitement des données relatives aux passagers aériens[40].

3.5) Le droit de recours

Les tenants du nouvel accord insistent sur le droit de recours, qui protégerait les passagers contre d'éventuelles violations de leurs droits. Les passagers disposeront d'un droit de recours *« administratif et judiciaire dans les cas où les règles de protection des données auraient été violées, ainsi que le droit à indemnisation* ». Mais il n'est guère possible de déterminer comment des particuliers pourraient savoir s'il y a eu ou non violation. Aussi la possibilité de recours paraît-elle limitée.

---

[37] Il s'agissait de Faisal Shahzad et David Headley

[38] David Headley, auteur de l'attentat à Mumbai en 2008

[39] Accord du 27 Octobre 2011

[40] Les medias se sont emparé du cas de Maher Arar, ce Canadien d'origine syrienne qui fut arrêté à l'aéroport Kennedy de New York puis emprisonné, avant d'être relâché et d'obtenir judiciairement la reconnaissance qu'aucune preuve de la moindre infraction ne pouvait être retenue contre lui.

Conclusion

L'accord de 2012, sur certains points qui ont été signalés ici, semble traduire quelques progrès, mais ce n'est pas vrai dans tous les domaines. Il s'agit notamment de la mise en cause du principe de proportionnalité et des questions induites par la territorialité.

Le principe de proportionnalité est au centre du droit des données à caractère personnel. Les données à caractère personnel permettent d'identifier, directement ou indirectement, les personnes physiques et, éventuellement de porter atteinte à leur vie privée. Pour pallier ce danger d'immixtion dans la vie privée, les finalités des fichiers informatisés de données nominatives doivent être en phase avec le danger encouru par la sécurité. C'est ainsi que la CNIL est en général défavorable à l'utilisation, en matière d'applications biométriques, aux empreintes digitales, en raison de leur traçabilité, de leur caractère intrusif. Néanmoins, le recours aux empreintes digitales est généralisé pour les visas, les passeports, la circulation dans les zones « *réservées* » des aéroports car le principe de proportionnalité justifie, au vu des dangers encourus par la sécurité, ce recours aux empreintes digitales. A l'opposé, la CNIL estime que le principe de proportionnalité ne s'applique pas quand la finalité est la bonne observance des horaires de travail au sein d'une entreprise, prévue par le règlement intérieur, et que l'entreprise souhaite utiliser, pour contrôler les horaires de travail, les empreintes digitales. L'objectif de gestion des ressources humaines ne doit pas porter atteinte aux libertés individuelles dans ce contexte. La durée de conservation des données PNR dans l'accord approuvé par le Parlement de l'Union européenne pose réellement problème. Il est trop long et il semble disproportionné de prôner le droit à l'oubli et, dans le même temps, de garder aussi longtemps des données PNR, bien que certaines garanties aient été négociées et octroyées, d'autant que le Parlement dispose d'un véritable pouvoir et ne se contente plus de donner un avis. Et les 19 données PNR sont susceptibles de donner lieu à un profilage, ce qui ne correspond guère non plus au principe de proportionnalité.

L'accord PNR USA/Union européenne de 2012 induit aussi des questions de territorialité. Les dispositions s'appliquent à l'ensemble des citoyens des divers Etats de l'Union européenne, à l'exception du Danemark, du Royaume-Uni, de l'Irlande. Elles sont plus souvent inspirées par la *common law*[41] que par le droit romano-germanique qui englobe pourtant l'Allemagne, l'Italie, l'Espagne, la France, le Portugal. Le système juridique PNR dans son ensemble est nettement d'inspiration « *common law* ». Et il n'y a guère de compatibilité entre l'accord PNR 2012 et La Charte des droits fondamentaux de l'Union européenne, la Convention européenne de sauvegarde des droits de l'homme, et les traditions juridiques des pays de l'Union européenne, en matière de protection des données à caractère personnel. En raison de la dimension de territorialité, l'accès effectif à la justice en cas de litige interprétatif reste pendant et les coûts judiciaires éventuels générés par l'interprétation ou un éventuel contentieux ne sont pas évoqués. Le rattachement juridique selon les différentes obligations légales est posé, bien posé, sans qu'aucune réponse convaincante n'apparaisse.

Enfin s'inscrit en filigrane la problématique du consentement des passagers. Ce consentement est présumé. A partir du moment où une personne physique est enregistrée pour un voyage, elle est censée accepter les fondements et les clauses de l'accord PNR. En réalité, la plupart des passagers ignorent certaines clauses des accords PNR même si les transporteurs ont une obligation d'information. Le consentement n'est pas toujours pleinement éclairé.

Si l'on se réfère au droit français, la proposition de résolution n° 252 (2008-2009) présentée par M. Simon Sutour au nom de la commission des affaires européennes sur la proposition de décision-cadre relative à l'utilisation des données des dossiers passagers à des fins répressives[42] avait été examinée le 13 mai 2009[43] par la commission des lois. La proposition de résolution a été approuvée

[41] Qui s'applique, avec des différences notables, aux USA, au Royaume-Uni, à l'Irlande notamment
[42] E3697
[43] Sous la présidence de M. Jean-Jacques Hyest, spécialisé dans les questions afférentes à la sécurité, aux technologies de l'information, à la protection de la vie privée. M. Hyest fut notamment membre de la CNCIS

pour l'essentiel, mais des critiques ont été émises sur le droit au respect de la vie privée et la protection des données à caractère personnel ne semblait pas présenter des garanties suffisantes. Ce qui était vrai en 2009 et apparaissait dans le rapport des lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale l'est aussi en 2012 au niveau européen. Les garanties, certes existantes semblent insuffisantes en matière de données à caractère personnel.

L'accord PNR approuvé par le Parlement ne présente pas le même degré de sécurité juridique que les accords PNR passés avec le Canada, pays où, il est vrai, la *common law* est en partie contrebalancé par la tradition civiliste et de protection des données à caractère personnel dans la province du Québec, et avec l'Australie. Est-il possible de parvenir à un accord PNR véritablement équilibré entre l'exigence de sécurité prégnante aux USA et au sein de l'Union européen et le droit au respect de la vie privée ? La question est posée et la réponse n'est pas évidente.

Les USA n'ont jamais prouvé de façon concluante que la quantité considérable de données passagers collectée soit nécessaire à la lutte contre le terrorisme et la grande criminalité. Le G29 avait aussi indiqué que l'existence d'un régime PNR européen pourrait inciter des régimes non démocratiques à exiger la communication de PNR sur la base du principe de réciprocité. En 2012, il convient encore de se demander si les conséquences de cette réciprocité ont été suffisamment étudiées.

L'approbation du Parlement européen, qui considère en fait que les garanties pour l'accord PNR en matière de données à caractère personnel sont suffisantes pour les personnes physiques s'inscrit, peut-être temporairement dans la remise en cause du respect du droit à la vie privée, y compris sur le territoire de l'Union européenne. Cette remise en cause, qu'on peut espérer non définitive s'inscrit dans l'option en faveur du tout sécuritaire. Selon Mireille Delmas-Marty[44], « *Il reste aux juristes à trouver les instruments de mise en œuvre. Envisagée comme bien public mondial, la sécurité pourrait être ainsi à la fois dédramatisée et strictement encadrée. Cela suffira-t-il pour préserver les libertés face à la radicalisation des procédures de contrôle social ? […] Si (cela ne se) fait pas, c'est un homme bien différent, infiniment moins libre, bien plus formaté, qui verra le jour*[45] ». Espérons que le recul du Parlement européen en matière de PNR 2012 n'annonce pas l'arrivée de cet homme formaté.

Claudine Guerrier, enseignant-chercheur à Institut Mines/Télécom, Télécom école de management

Claudine.Guerrier@telecom-em.eu

[44] Mireille Delmas-Marty, « Libertés et sûreté dans un monde dangereux », La couleur des idées, Le Seuil, 2010, pp 246-247

[45] Cf. Axel Türk, « Le réveil sera très douloureux », *Libération,* 28-29 mars 2009