Le fichier

Actes du colloque
organisé les 26 et 27 novembre 2015
par le Centre de recherche juridique Pothier
de l'Université d'Orléans

Sous la direction
de Fouad EDDAZI
Maître de conférences à l'Université d'Orléans
et de Stéphanie MAUCLAIR
Maître de conférences à l'Université d'Orléans

LGDJ une marque de Lextenso

Les divergences transatlantiques dans l'exploitation des fichiers privés pour la lutte contre le terrorisme : droit positif et prospective

Philippe Ch.-A. Guillot

Professeur de relations internationales à l'École de l'Air
Membre associé du Centre universitaire rouennais d'études juridiques
CUREJ – EA 4703

La lutte contre le terrorisme utilise non seulement les divers fichiers de police établis par les autorités publiques nationales ou européennes[1], mais elle se sert aussi de fichiers privés – entendus comme les dossiers de clients détenus par des sociétés commerciales de droit privé – contenant des informations utiles à la prévention ou à la répression des actes terroristes. Si, en matière répressive, l'accès aux fichiers privés concernant des suspects en nombre limité se fait sous le contrôle d'un juge, il en va différemment en matière préventive où les services compétents peuvent se livrer à une surveillance de masse sans être nécessairement contrôlés. Dès lors, se pose la question du bon équilibre entre la liberté individuelle et les mesures sécuritaires.

L'Union européenne et ses États membres y répondent en privilégiant la liberté et en consacrant la protection des données personnelles comme un droit fondamental à l'article 8 de la Charte des droits fondamentaux de l'Union européenne (CDFUE) et à l'article 16 du Traité sur le

1. V. Gutirrez-Zarza A. (dir.), *Exchange of Information and Data Protection in Cross-border Criminal Proceedings in Europe*, Heidelberg, Springer, 2015 ; Kauff-Gazin F., « Les fichiers dans le cadre de la coopération policière européenne », *in* Plessix B., Deffains N. (dir.), *Fichiers informatiques et sécurité publique*, Nancy, PUN-Éditions universitaires de Lorraine, 2013, p. 223-241.

fonctionnement de l'Union européenne[2]. La protection de ces données est régie notamment par la directive 95/46/CE du 24 octobre 1995 complétée par la décision-cadre 2008/977/JAI du Conseil du 27 novembre 2008[3]. Ce régime interdit l'inclusion de données sensibles – race ou origine ethnique, opinions politiques, convictions religieuses ou philosophiques, appartenance syndicale, abus de drogue et d'alcool, santé ou vie sexuelle – dans les traitements de données et soumet ceux-ci à des contrôles par une autorité administrative indépendante – Commission nationale informatique et libertés (CNIL) en France, Contrôleur européen de la protection des données (CEPD) pour l'Union européenne. L'article 29 de la directive instaure un groupe européen des autorités nationales de protection des données – le « G29 » – pour contribuer à la mise en œuvre homogène des dispositions nationales.

En revanche, les États-Unis d'Amérique font relativement peu de cas du respect de la vie privée en dépit du Quatrième Amendement[4] – le Privacy Act de 1974 ne concernant que les fichiers détenus par les agences fédérales et la protection des données conservées par des opérateurs privés n'étant que sectorielle[5].

La coopération entre l'Europe et les États-Unis en matière de lutte contre le terrorisme doit donc concilier des approches divergentes ainsi

2. V. Peyrou S., « La protection des données à caractère personnel : un droit désormais constitutionnalisé et garanti par la CJUE », *in* Tinière R., Vial C. (dir.), *La protection des droits fondamentaux dans l'Union européenne*, Bruxelles, Bruylant, 2015, p. 213-231 ; Placco A. V., « La protection des données à caractère personnel dans le cadre de la Cour de justice de l'Union européenne relative aux droits fondamentaux », *in* Grosjean A. (dir.), *Enjeux européens et mondiaux de la protection des données personnelles*, Bruxelles, Larcier, 2015, p. 27-51.

3. En 2018, ces textes seront remplacés respectivement par le règlement 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données et la directive 2016/680 du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, *JOUE*, 4 mai 2016, L119/1 et L119/89 ; v. Bensoussan A. (dir.), *Règlement européen sur la protection des données. Textes, commentaires et orientations pratiques*, Bruxelles, Larcier, p. 39-459 et 461-510.

4. V. Herman S. N., *Taking Liberties. The War on Terror and the Erosion of American Democracy*, Oxford/New York, OUP, 2e éd., 2014, p. 105-120 ; Wicker S. B., *Cellular Convergence and the Death of Privacy*, Oxford/New York, OUP, 2013, p. 36-55.

5. V. Doutriaux C., « Cybersurveillance des citoyens et lutte contre le terrorisme », *in* Blandin-Obernesser A. (dir.), *Droits & souveraineté numérique en Europe*, Bruxelles, Bruylant, 2016, p. 192 ; Bellanova R., De Hert P., « Protection des données personnelles et mesures de sécurité : vers une perspective transatlantique », *Cultures & Conflits*, n° 74, 2009, p. 70-76 ; Tanaka H. *et alii*, *Transatlantic Information Sharing At a Crossroads*, Washington, Migration Policy Institute, 2010, p. 20-22, 27-31 pour une comparaison avec le système européen.

que l'illustrent les péripéties ayant entouré deux types d'accords euro-américains concernant les fichiers de passagers aériens (Passenger name Record – PNR) et ceux des messageries bancaires (Society for Worldwide Interbank Financial Transactions-Terrorist Finance Tracking Program – Swift-TFTP) qui ont donné lieu non seulement à une controverse transatlantique, mais aussi à un conflit au sein des institutions de l'Union européenne dû aux différences d'appréciation sur les concessions à faire par la Commission et le Conseil, d'une part, et par la Cour de justice et le Parlement européen, d'autre part, alors même que certains États membres ont adopté des mesures permettant à leurs services de sécurité d'avoir accès aux données des passagers aériens, à l'instar du « système API-PNR France », sans attendre que le Parlement européen accepte en 2016 la création d'un « PNR européen » (I). De même, le recueil de métadonnées[6] auprès des entreprises de communications électroniques et des fournisseurs d'accès à l'internet par la France avec les dispositions des lois de programmation militaire et relative au renseignement, inspiré des pratiques de la National Security Agency (NSA) que le USA Freedom Act du 2 juin 2015[7] vient pourtant de restreindre, s'avère difficile à concilier avec le droit fondamental à la protection des données personnelles tel qu'interprété par la Cour de justice (II).

I – LE RECUEIL PAR LES SERVICES DE LUTTE ANTI-TERRORISTE DES FICHIERS DES COMPAGNIES AÉRIENNES ET DES MESSAGERIES BANCAIRES

Afin de concilier les exigences du droit états-unien en matière de prévention du terrorisme avec celles de l'Union européenne, des accords ont été adoptés, mais le Parlement européen s'y est opposé au nom du droit fondamental à la protection des données personnelles, obligeant à leur renégociation (A). Certains États européens, dont la France, ont pourtant

6. Les métadonnées sont les « données sur les données » qui concernent le contenu (auteur du document, géolocalisation, etc.) ou la communication (émetteur, destinataire, date, heure et durée de la communication, canal ou protocole de communication utilisé, etc.); ces métadonnées de communication se subdivisent en métadonnées de téléphonie (facture détaillée) et métadonnées de l'internet (adresse électronique), v. Unité d'évaluation des choix scientifiques et technologiques du PE (STOA): *Mass Surveillance Part 1 – Risks, Opportunities and Mitigation Strategies*, janv. 2015, IP/G/STOA/FWC-2013-1/LOT9/C5/SC1, PE 527.409, p. 7.

7. *Uniting and Strenghtening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015*, Public Law 114-23, 129 Stat., p. 268-313.

choisi de mettre en œuvre une surveillance des passagers aériens (B) et ont finalement obtenu qu'un tel contrôle s'étende au niveau de l'Union européenne (C).

A. Les vicissitudes des accords PNR et Swift-TFTP

Les divergences d'appréciation sur la légalité des premiers accords PNR conclus avec les États-Unis au sein des institutions européennes (1) a conduit à l'adoption d'un dernier accord en 2011, plus respectueux de la protection des données personnelles (2). Le « bras de fer » interinstitutionnel s'est poursuivi avec l'adoption de l'accord Swift-TFTP (3).

1. Les accords de 2004 et de 2007

L'Aviation and Transportation Security Act du 19 novembre 2001 oblige les compagnies aériennes assurant des vols au départ, en transit ou à destination des États-Unis à permettre aux autorités états-uniennes d'accéder aux données PNR[8] sous peine de se voir infliger de lourdes amendes, voire de ne pouvoir pénétrer l'espace aérien américain. Les compagnies aériennes européennes assurant des liaisons régulières aux États-Unis exprimèrent leur réticence à se plier à ces exigences, car elles auraient ainsi été en infraction au regard du droit de l'Union européenne et de leur droit national. La situation était donc juridiquement intenable et la Commission engagea des négociations avec l'Administration états-unienne.

Un premier accord fut conclu en 2004[9], mais les décisions 2004/535 de la Commission et 2004/496 du Conseil le mettant en œuvre furent annulées le 30 mai 2006 par la Cour de justice[10]. Entre-temps, un deuxième accord avait été signé le 28 mai 2004 entre la Communauté européenne et les États-Unis. Il fut dénoncé et remplacé par un accord intérimaire du 19 octobre 2006 qui expira le 31 juillet 2007. Un nouvel accord fut alors conclu les 23 et 27 juillet 2007 pour sept ans[11]. Il prévoyait que les transporteurs aériens permettraient l'accès informatique des services du Department of Homeland Security (DHS) aux données PNR de tous les passagers à

8. La solution technique retenue consistait, pour les autorités états-uniennes, à extraire (*pull*) les informations dans les dossiers PNR des compagnies aériennes et non pas à demander que ces dernières exportassent (*push*) leurs informations vers lesdites autorités.

9. *JOUE* 2004, L 183/84.

10. CJUE, 30 mai 2006, aff. C-317/04, C-318/04, *Parlement européen c/ Conseil de l'Union européenne, Commission des Communautés européennes.*

11. *JOUE* 2007, L 204/18.

destination ou en provenance des États-Unis, mais le Parlement européen refusa de l'entériner et exhorta la Commission à négocier un nouveau texte.

2. L'accord de 2011

Le 14e alinéa du Préambule de l'Accord entre les États-Unis d'Amérique et l'Union européenne sur l'utilisation des dossiers (données PNR) et leur transfert au ministère américain de la Sécurité intérieure[12] reconnaît que le DHS garantit un niveau adéquat de protection des données pour le traitement et l'utilisation des dossiers passagers qui lui sont transférés ou qu'il va chercher lui-même dans les systèmes informatisés de réservation des compagnies aériennes. Ces dernières fournissent au DHS la vingtaine de données PNR visées à l'annexe de l'accord – le DHS supprimant les autres données éventuellement reçues – afin de prévenir ou détecter les infractions terroristes ou les infractions pénales y relatives, ainsi que les infractions transnationales passibles d'au moins trois ans de prison ou face à une menace grave ou encore si une juridiction l'impose pour tout autre motif[13] – ce qui peut donc impliquer des infractions pour lesquelles le droit européen ou le droit des États membres ne prévoient pas d'accès aux données personnelles et ce qui ne répond guère à l'impératif de prévisibilité de la règle de droit[14].

Le DHS protège les données personnelles – les données sensibles devant être filtrées et effacées définitivement dans les trente jours suivants leur réception, sauf en cas de menace à la vie d'une personne ou de procédure pénale spécifique – contre toute altération, destruction ou divulgation non autorisée, étant précisé que le DHS informe les autorités européennes des cas d'incidents graves portant atteinte au respect de la vie privée, impliquant les dossiers PNR de citoyens de l'Union européenne[15].

Les données sont conservées dans une base active pendant cinq ans puis transférés vers une base dormante pendant dix ans voire plus en cas d'enquêtes ou de poursuites Six mois après leur réception, ces dossiers sont dépersonnalisés, c'est-à-dire que les informations permettant une identification personnelle sont masquées. Toutefois, les données pourront être « repersonnalisées » en cas de menace ou de risque identifiable. À l'expiration

12. *JOUE* 2012, L 215/5; signé par le Conseil en déc. 2011 et approuvé le 26 avr. 2012, il est conclu pour une période initiale de 7 ans et ne s'applique ni au Danemark, ni au Royaume-Uni, ni à l'Irlande.

13. Art. 3 et 4.

14. V. Boehm F., Cole M. D., *Data Retention after the Judgement of the Court of Justice of the European Union, Münster/Luxembourg*, 30 juin 2014, étude pour le groupe Les Verts/Alliance libre européenne du PE, p. 60.

15. Art. 5 et 6.

du délai de quinze ans, les données ne seront pas effacées mais « complètement anonymisées » sans possibilité de « repersonnalisation »[16], néanmoins d'aucuns doutent de cette garantie, puisque si la repersonnalisation n'était pas techniquement possible, cela n'aurait pas de sens de conserver indéfiniment ces données. Cette conservation pérenne de données de passagers non visés par une procédure pénale – lesquels encourent ainsi un « risque de stigmatisation »[17] – va à l'encontre du principe de proportionnalité[18], mais l'Accord prévoit un certain nombre de garanties[19].

Le DHS ne peut partager les dossiers passagers qu'avec les autorités publiques nationales enquêtant sur ou poursuivant les infractions susmentionnées[20], cependant le transfert des données PNR à des États tiers peut avoir un champ plus vaste[21]. La coopération en matière policière, répressive et judiciaire avec l'Union européenne, ses États membres, Europol ou Eurojust fait l'objet de développements particuliers[22].

Cette dernière mouture de l'Accord est incontestablement plus acceptable, néanmoins, la durée de la détention des données est considérablement longue. De surcroît, l'utilisation des données PNR – diffusables à tous les organismes associés au DHS et non plus aux seules douanes[23] – présente aussi un risque d'extension car ces données peuvent être utilisées par les autorités états-uniennes à d'autres fins que la lutte contre le terrorisme. Il est donc à craindre que ne se mette en place un système global de profilage et de contrôle attentatoire aux droits des personnes dont l'efficacité n'est pas démontrée : le nombre de terroristes ayant pu être arrêtés grâce au transfert de données PNR s'élèverait à deux ! Les quelques déroutements d'avions à destination des États-Unis opérés sur le fondement d'informations extraites des PNR ne concernent que des cas d'homonymie[24] et quelques journalistes ou essayistes ayant eu le seul tort d'être trop critiques de la politique états-unienne[25].

---

16. Art. 8.

17. CEDH, 4 déc. 2008, n° 30562/04 & 30566/04, *S. & Marper c/ Royaume-Uni*, § 122.

18. V. Boehm F., Cole M. D., préc., p. 61-62.

19. Les articles 10 à 13 renvoient aux Administrative Procedure Act, Freedom of Information Act, Computer Fraud and Abuse Act, et Electronic Communication Privacy Act ainsi qu'au programme d'information des voyageurs du DHS, Traveler Redress Inquiry Program (TRIP), qui offre une voie de recours aux particuliers estimant avoir subi un préjudice en ayant été identifiés à tort comme terroristes.

20. Art. 16.

21. En effet, l'article 17 ne se réfère pas aux infractions visées à l'article 4.

22. Art. 18.

23. V. Camus C., *La lutte contre le terrorisme – Dérives sécuritaires et dilemme démocratique*, Paris, Le Félin, 2007, p. 106.

24. V. Martin J.-Ch., *Les règles internationales relatives à la lutte contre le terrorisme*, Bruxelles, Bruylant, 2006, p. 369-370.

25. V. *Le Monde*, 3 oct. 2012.

3. L'accord Swift-TFTP

Cet accord tire son nom de la Société de télécommunications financières interbancaires mondiales (Swift), une compagnie belge qui conduit presque 80 % des transferts bancaires internationaux dans 208 pays. Initialement, les autorités états-uniennes pouvaient accéder aux données Swift européennes parce que les serveurs de la société étaient situés sur le sol américain, mais sous la pression des agences européennes de protection des données[26], Swift opère désormais ses transferts de messagerie financière depuis les Pays-Bas et la Suisse.

Un premier accord euro-américain fut conclu, mais le Parlement européen le rejeta, le 11 février 2010, à cause de l'absence de proportionnalité entre les règles afférentes au transfert et au stockage de données et la sécurité supposément fournie. Un nouveau texte dut alors être négocié.

L'Accord entre l'Union européenne et les États-Unis d'Amérique sur le traitement et le transfert de données de messagerie financière de l'Union européenne aux États-Unis aux fins du programme de surveillance du financement du terrorisme[27] concerne la conciliation des règles européennes de respect de la vie privée et de protection des données personnelles[28] avec le programme du département du Trésor des États-Unis TFTP : à la demande du Trésor états-unien, les fournisseurs de services de messagerie financière internationale doivent transférer à celui-ci des données de messageries financières et des données connexes aux fins de la prévention et de la détection du terrorisme ou de son financement[29]. Les injonctions du Trésor doivent identifier aussi clairement que possible les données nécessaires au renseignement, aux enquêtes ou aux poursuites anti-terroristes. Une copie de ces injonctions est adressée à Europol qui doit vérifier d'urgence si la demande est recevable[30] ; dans l'affirmative, la demande devient juridiquement contraignante, obligeant le fournisseur à exporter directement au Trésor les données réclamées, or le rôle d'Europol a été très critiqué par l'Autorité de contrôle commune et par le Parlement européen car les demandes états-uniennes sont quasi automatiquement acceptées[31].

Les données transmises sont effacées au plus tard cinq ans après leur réception si elles n'ont pas été extraites entre-temps, tandis que les

---

26. Avis du 27 sept. 2006 de la Commission de la protection de la vie privée (Belgique) ; avis 2006/10 du G29 du 22 nov. 2006 ; avis du CEPD du 1er févr. 2007.

27. *JOUE*, 27 juill. 2010, L 195/5.

28. Elles sont rappelées dans le 6e alinéa du préambule de l'Accord.

29. Art. 3 : de fait, seule Swift est concernée en tant que « fournisseur de services ».

30. Art. 4. : l'art. 9 § 2 précise qu'Europol désigne un officier de liaison auprès du Trésor.

31. V. Billet C., « Le transfert de données à caractère personnel aux États tiers : l'évolution de la protection par l'UE », *in* Blandin-Obernesser A. (dir.), préc., p. 186-187.

informations extraites des données fournies sont conservées pendant la durée nécessaire aux enquêtes ou poursuites spécifiques[32].

Le Trésor peut partager ces données avec tout État ou organisation internationale, ainsi qu'avec Europol ou Eurojust, mais tout partage d'informations relatives à un ressortissant de l'Union européenne avec les autorités d'un pays tiers est soumis à l'accord préalable des autorités compétentes de l'État membre concerné, sauf lorsque ce partage est essentiel pour prévenir une menace grave et immédiate[33]. Europol, Eurojust ou une autorité compétente d'un État membre peuvent demander au Trésor une recherche d'informations pertinentes obtenues dans le cadre du TFTP[34].

Une coopération avec un futur système équivalent de l'Union européenne est envisagée[35], mais l'innovation de cet accord réside le suivi des garanties et contrôles par des contrôleurs indépendants, « y compris une personnalité désignée par la Commission européenne en accord avec les États-Unis »[36].

Enfin, l'Accord organise la transparence, le droit d'accès, de rectification, d'effacement ou de verrouillage, la préservation de l'exactitude des informations et les recours[37].

***

La faiblesse du contrôle demeure au centre des reproches adressés aux accords PNR et Swift-TFTP puisque, les États-Unis n'ayant pas d'autorité administrative indépendante compétente en matière de protection des données personnelles, le DHS opère sans surveillance. Tout au plus doit-il informer la Commission européenne dans les cas exceptionnels où des vies seraient en danger. Le DHS peut faire ce qu'il veut des données collectées, y compris les transférer à des États tiers peu regardants en matière de liberté individuelle. En dépit des efforts de la Cour de justice et du Parlement européen pour limiter les atteintes au droit fondamental à la protection des données personnelles, celui-ci est donc sacrifié sur l'autel de la lutte contre le terrorisme, car la Commission n'a pu obtenir des États-Unis ce qu'elle obtint de l'Australie ou du Canada[38]. En revanche, la mise en place

32. Art. 6.
33. Art. 7.
34. Art. 10.
35. Art. 11.
36. Art. 12.
37. Art. 14 à 18; les garanties applicables au traitement des données sont prévues aussi par l'article 5.
38. V. Labouz M.-F., « Le nouvel accord sur les données de passagers aériens (PNR) entre l'Union européenne et les États-Unis », *in* Saulnier-Cassia E. (dir.), *La lutte contre le terrorisme dans le droit et la jurisprudence de l'Union européenne*, Paris, LGDJ, 2014,

d'un système PNR en France ou au niveau de l'Union européenneapparaît plus respectueuse de l'article 8 de la CDFUE.

B. Les PNR nationaux : l'exemple français

Deux ans après que le Royaume-Uni mit en œuvre son *Semaphore Project*, la France autorisa à son tour la collecte des données PNR et *Advance Passenger Information* (API – données collectées par les compagnies aériennes lors de la phase d'enregistrement des passagers sur un vol) à l'occasion de déplacements internationaux en provenance ou à destination d'États tiers à l'Union européenne, ainsi que celle des documents de voyage, de la carte d'identité et des visas des passagers de transporteurs aériens, maritimes ou ferroviaires[39].

Un arrêté du 19 décembre 2006 institua, à titre expérimental, un fichier des passages aériens qui ne concerne que les données API des passagers de vols directs en provenance et à destination de l'Afghanistan, du Pakistan, de l'Iran, de la Syrie et du Yémen. Toutefois, l'expérimentation a surtout révélé « un manque de rigueur dans la transmission des données par certaines compagnies et (...) la multiplicité d'erreurs imputables à des homonymies ou à des transcriptions inexactes des noms »[40].

Enfin, la loi de programmation militaire de 2013 institue le *système API-PNR France*, dont les données sensibles sont expressément exclues, pour les vols au départ ou à destination de la France[41]. Ce système,

---

p. 269 ; v. Accord entre l'Union européenne et l'Australie sur le traitement et le transfert de données des dossiers de passagers (données PNR) par les transporteurs aériens au service australien des douanes et de la protection des frontières, *JOUE*, L 186/4 du 14 juill. 2012 qui prévoit une conservation de 5,5 ans (art. 16) et un contrôle par le commissaire australien à l'information (art. 10 § 1) ; Accord entre la Communauté européenne et le gouvernement du Canada sur le traitement des données relatives aux informations préalables sur les voyageurs et aux dossiers passagers, *JOUE*, L 82 du 21 mars 2006, assez vague, il doit être remplacé par un nouvel accord en cours d'adoption, v. proposition de décision du Conseil relative à la conclusion de l'accord entre le Canada et l'Union européenne sur le transfert et le traitement de données de passagers, COM(2013)528, prévoyant une durée de conservation de 5 ans et un contrôle par une autorité administrative indépendante à créer ; mais en nov. 2014, le PE a saisi la CJUE de sa conformité à la CDFUE ; le 8 septembre 2016, l'avocat général Paolo Mengozzi a présenté ses conclusions [ECLI :EU :C :2016 :656], d'où il ressort que l'accord n'est pas conforme mais, à ce jour, la Cour ne s'est pas prononcée.

39. Art. 7 de la loi n° 2006-64 du 23 janv. 2006 relative à la lutte contre le terrorisme ; par ailleurs, l'article 65 du Code des douanes permet à l'administration de requérir ponctuellement les données PNR de certains vols.

40. Guerrier C, « Passenger Name Record 2012 », 2 juill. 2012, http://www.juriscom.net/wp-content/documents/pnr20120702.pdf.

41. CSI, art. L. 232-7, mis en œuvre par les décrets n° 2014-1095 du 26 sept. 2014 portant création d'un traitement de données à caractère personnel dénommé « système

prévoyant que les données sont conservées pendant cinq ans mais qu'elles ne peuvent être communiquées aux services habilités que pendant deux ans, a été considéré comme satisfaisant par la CNIL car les garanties offertes réduisent le risque d'atteinte à la protection des données personnelles[42].

C. La directive PNR

Depuis 2007, la Commission tentait de faire adopter une proposition de directive pour établir un PNR européen aux fins de prévention du terrorisme, mais s'était heurtée à deux reprises au refus du Parlement européen. Suite aux attentats de janvier 2015, la France insista auprès du Parlement européen pour que la directive PNR soit adoptée, demande relayée par le président du Conseil européen. Après d'intenses négociations, la directive 2016/681 relative à l'utilisation des données de 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[43], est adoptée le 27 avril 2016. Elle prévoit la mise en place d'unités d'informations passagers (UIP) dans chaque État membre – à moins que des États membres choisissent de créer entre eux une UIP commune – qui sera chargée de contrôler le traitement des données PNR qui lui seront transmises (méthode *push*) par les transporteurs aériens sous la surveillance des autorités nationales de contrôle des données personnelles. Les échanges d'informations entre autorités compétentes habilitées des États membres ou vers Europol, voire des États tiers, transiteront par les UIP. Le délai de conservation des données sera de cinq ans, sachant que ces données seront dépersonnalisées six mois après leur transmission à l'UIP.

API-PNR France » – lequel crée les art. R.232-12 à R.232-18 du même code –, n° 2014-1566 du 22 déc. 2014 portant création d'un service à compétence nationale dénommé « Unité Information Passagers » (UIP) et n° 2015-1328 du 21 oct. 2015 portant modification de l'article 5 du décret n° 2010-569 du 28 mai 2010 relatif au fichier des personnes recherchées et des articles R. 232-14 et R. 232-15 du Code de la sécurité intérieure.

42. Délibération n° 2014-308 du 17 juill. 2014 portant avis sur un projet de décret relatif à la création d'un traitement de données à caractère personnel dénommé « système. API-PNR France » pris pour l'application de l'article L. 232-7 du Code de la sécurité intérieure et fixant les modalités de transmission au service à compétence nationale « Unité Information Passagers » des données relatives aux passagers par les transporteurs aériens. L'article R. 232-18 prévoit que les droits d'accès et de rectification des données API-PNR s'exercent directement auprès du directeur de l'UIP et que ceux concernant divers fichiers publics ainsi que les requêtes formulées par les services anti-terroristes s'exercent auprès de la CNIL.

43. *JOUE*, 4 mai 2016, L119/132; V. Bensoussan A. (dir.), préc., p. 511-529.

II – LE RECUEIL PAR LES SERVICES DE LUTTE ANTI-TERRORISTE DES FICHIERS DES OPÉRATEURS DE COMMUNICATIONS ÉLECTRONIQUES ET DES FOURNISSEURS D'ACCÈS À L'INTERNET

Les informations comprises dans les métadonnées étant très instructives, les services de lutte anti-terroriste cherchent à les obtenir des opérateurs privés parfois sans base légale (A), à moins que le législateur ne leur ait confectionné un droit sur mesure (B), mais la jurisprudence de la CJUE implique un rééquilibrage au profit de la protection des données personnelles (C).

A. Les pratiques de la National Security Agency

La NSA peut, sur décision de justice, mais selon une procédure secrète[44], accéder aux données des plus importantes sociétés de l'internet afin d'obtenir des renseignements sur des personnes suspectées de terrorismes, et ces entreprises – toutes états-uniennes – ne peuvent refuser de se plier à ces injonctions. Néanmoins, comme l'a révélé M. Edward Snowden[45], la NSA, hors de tout cadre juridique, intercepte aussi massivement les communications téléphoniques ou électroniques.

Le scandale découlant de ces révélations a mis en évidence, d'une part, une « perte de contrôle » de l'Union européenne et de ses États membres en matière de souveraineté numérique et, d'autre part, une méfiance des institutions européennes et des gouvernements nationaux envers la politique antiterroriste états-unienne[46]. La Commission des libertés civiles, de la justice et des affaires intérieures du Parlement européen n'hésite pas à fustiger « la mise en place d'un État "ultrapréventif" » et « un mélange d'activités de répression et de renseignement avec des garanties juridiques floues et affaiblies, allant bien souvent à l'encontre des freins et contrepoids démocratiques, en particulier de la présomption d'innocence »[47].

---

44. Foreign Intelligence Services Act, art. 702 ; en revanche la captation des communications d'étrangers résidant hors des États-Unis ne nécessitait pas une décision de justice.

45. V. Lefébure A., *L'affaire Snowden. Comment les États-Unis espionnent le monde*, Paris, La Découverte, 2014.

46. V. Bigo D. *et alii*, "Open Season for Data Fishing on the Web. The Challenges of the US PRISM Programme for the EU", *CEPS Policy Brief*, n° 293, 18 juin 2013, p. 4.

47. Moraes C., *Rapport sur le programme de surveillance de la NSA, les organismes de surveillance dans divers États membres et les incidences des droits fondamentaux des citoyens*

La réaction n'est pas moins vive au Conseil de l'Europe dénonçant une connivence entre la NSA et les services de renseignement de certains pays alliés[48] et à l'assemblée générale des Nations unies dont la résolution 68/167 du 18 décembre 2013 rappelle aux États qu'ils doivent « respecter pleinement les obligations que leur impose le droit international des droits de l'homme »[49], tandis que la résolution 68/178 du même jour les encourage à préserver le droit au respect de la vie privée[50].

Aux États-Unis aussi, les programmes clandestins d'interception de la NSA ont choqué l'opinion et le Congrès a finalement adopté l'USA Freedom Act qui interdit les captations massives de métadonnées et oblige désormais la NSA à solliciter, après autorisation de la Foreign Intelligence Surveillance Court, un opérateur pour accéder aux métadonnées d'une personne précisément désignée ou d'un terminal de communication clairement identifié.

L'enquête sur les attentats de San Bernardino est à l'origine d'une controverse entre la police fédérale (Federal Bureau of Investigation – FBI) et la société Apple, soutenue par les autres entreprises de téléphonie et de l'internet, au sujet de l'accès aux informations contenues dans l'iPhone de l'auteur des tueries. Apple a été sommée par une juridiction californienne de développer un logiciel capable de pénétrer ce type d'appareil sans code mais la société refuse de mettre en place une « porte dérobée » (*backdoor*) au profit des autorités à cause de l'inconstitutionnalité d'une telle mesure[51] et parce que d'autres opérateurs – États étrangers, criminels, terroristes, etc. – pourraient utiliser ladite porte pour leurs propres intérêts[52]. Le 29 février 2016, dans une affaire similaire mais liée au trafic de stupéfiants, un juge new-yorkais a tranché que l'All Writs Act de 1789 sur lequel se

européens et sur la coopération transatlantique en matière de justice et d'affaires intérieures, 21 févr. 2014, A7-0139/2014, p. 24, § 12.

48. Omtzigt P., *Les opérations massives de surveillance*, rapport pour la Commission des questions juridiques et des droits de l'homme de l'Assemblée parlementaire du Conseil de l'Europe, 26 janv. 2015, § 38.

49. *Le droit à la vie privée à l'ère du numérique*, A/RES/68/167, p. 2 ; le texte pertinent est l'article 17 du Pacte international relatif aux droits civils et politiques du 16 déc. 1966 sur le respect de la vie privée.

50. A/RES/68/178, p. 4, point 6 g.

51. Apple argue qu'un code informatique est une forme d'expression écrite protégée par le Premier Amendement relatif à la liberté d'expression et que le FBI ne peut contraindre l'entreprise à s'exprimer en produisant un logiciel contre sa volonté.

52. V. *Le Figaro*, 24 févr. 2016 ; le FBI est néanmoins parvenu à déchiffrer l'iPhone et a cessé ses poursuites contre Apple, v. *Le Figaro*, 29 mars 2016, mais n'entend pas révéler à l'opérateur la faille utilisée pour débloquer l'appareil, v. *Le Monde*, 27 avril 2016.

fondait le FBI ne permet pas l'accès aux données téléphoniques du suspect, ce qui semble donner raison aux opérateurs de télécommunications[53].

B. Les dispositions du Code français de la sécurité intérieure

Les services de renseignement peuvent recueillir auprès des opérateurs de communications électroniques des informations traitées ou conservées par leurs réseaux ou services, « y compris les données techniques relatives à l'identification des numéros d'abonnement ou de connexion à des services de communications électroniques, au recensement de l'ensemble des numéros d'abonnement ou de connexion d'une personne désignée, à la localisation des équipements terminaux utilisés ainsi qu'aux communications d'un abonné portant sur la liste des numéros appelés et appelants, la durée et la date des communications. »[54]. Un tel recueil en temps réel ne peut être autorisé pour une durée de deux mois renouvelable que « pour les seuls besoins de la prévention du terrorisme »[55]

Ces services peuvent aussi imposer aux opérateurs la mise en place sur leurs réseaux de « boîtes noires » destinées à détecter, grâce à des algorithmes, des communications suspectes[56] et qui mettent en œuvre des technologies d'inspection des « paquets en profondeur ». Les opérateurs sont tenus d'autoriser, à des fins de contrôle, les membres et les agents de la Commission nationale de contrôle des techniques de renseignement à entrer dans leurs locaux où sont mises en œuvre ces « boîtes noires »[57].

C. La portée de la jurisprudence de Cour européenne de justice

La directive 2006/24/CE du 15 mars 2006 relative à la conservation des données, adoptée après les attentats de Madrid et de Londres, harmonisait les mesures nationales obligeant les fournisseurs de télécommunication et de services informatiques à conserver les métadonnées de leurs clients pour les transmettre sur requête aux services de police ou de renseignement. Saisie de deux questions préjudicielles sur la compatibilité de cette directive avec la CFDUE, la Cour de justice la jugea incompatible notamment

53. V. *Le Monde*, 1er mars 2016; le texte de l'ordonnance du juge James Orenstein (US District Court, Eastern District of New York) https://cdn1.vox-cdn.com/uploads/chorus_asset/file/6124209/Orenstein-Order-Apple-iPhone-02292016.pdf.

54. CSI, art. L. 851-1.

55. CSI, art. L. 851-2.

56. CSI, art. L. 851-3.

57. CSI, art. L. 871-4.

parce qu'elle couvrait « de manière généralisée toute personne et tous les moyens de communication électronique », ne prévoyait « aucun critère objectif permettant de délimiter l'accès des autorités nationales compétentes aux données et leur utilisation ultérieure » et que la durée de conservation était fixée sans tenir compte de l'utilité de la conservation par rapport aux objectifs poursuivis[58].

Le principe de proportionnalité a donc été rappelé avec force, en conséquence les derniers textes adoptés par les États membres ou en cours d'adoption par l'Union européenne s'efforcent de préserver la protection des données personnelles avec des mesures utiles de prévention du terrorisme.

Tel n'est pas le cas des accords conclus avec les États-Unis, lesquels n'offrent d'ailleurs pas de garanties adéquates, comme l'a affirmé la Cour de justice[59] ou comme l'a précisé le CEPD à propos d'un projet de traité dans un domaine voisin[60].

La lutte antiterroriste tend à privilégier les solutions technologiques au risque d'aller à l'encontre des valeurs que l'on défend. Une approche plus respectueuse de la protection des données personnelles est nécessaire afin non seulement de mieux défendre la modèle de société que nous voulons, mais aussi pour se prémunir de toujours possibles dérives, et ce, d'autant que, comme le notait le juge de la Cour suprême William Brennan, il y a plus d'un demi-siècle « la surveillance électronique (...) rend la police omnisciente ; et l'omniscience de la police est l'un des outils les plus efficaces de la tyrannie »[61].

58. CJUE, 8 avr. 2014, aff. C-293/12, C-594/12, *Digital Rights Ireland* & *Seitlinger*, § 57-64 ; v. la contribution de CAZALA J. dans le présent ouvrage.

59. CJUE, Gr. Ch., 6 oct. 2015, aff. C-362/14, *Maximillian Schrems c/ Data Protection Commissioner*.

60. V. *Preliminary Opinion on the Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection and prosecution of criminal offenses*, Opinion 1/2016, 12 févr. 2016.

61. Opinion dissidente dans l'affaire *Lopez c/ États-Unis* de 1963, citée par HERMAN S.N., préc., p. 120 [ma traduction].