No.2 | Juillet 2015
| Numéro spécial : «Privacy»

Montesquieu Law Review

Lutte contre le terrorisme et protection des données personnelles

Philippe Ch.-A. Guillot, Professeur de relations internationales à l'École de l'Air

© Ivan Eastwood

Programme financé par l'ANR
n°ANR-10-IDEX-03-02

Forum Montesquieu
Faculté de droit et science politique
université de BORDEAUX

Lutte contre le terrorisme et protection des données personnelles

Philippe Ch.-A. Guillot, Professeur de relations internationales à l'École de l'Air

Citation suggérée : Philippe Ch.-A. Guillot, *Lutte contre le terrorisme et protection des données personnelles,* 1 Montesquieu Law Review (2015), n° 2, disponible sur le site http://www.montesquieulawreview.eu/review.htm

Les attentats parisiens de janvier 2015 ont relancé le débat sur les dossiers de passagers aériens – *Passenger Name Records* (PNR) fichiers créés par les compagnies aériennes pour chaque voyage réservé par un passager – très intrusifs en matière de vie privée puisqu'ils concernent des données à caractère personnel (ci-après « données personnelles ») – données nominatives, moyens de paiement et, éventuellement, régime alimentaire ou état de santé, voire contacts du passager. Un fichage généralisé se profile menaçant, selon l'ancien président de la Commission nationale informatique et libertés (CNIL), de mettre « la vie privée en péril » (1).

En effet, la lutte contre le terrorisme pose la question de l'équilibre entre la protection de la vie privée et les mesures préventives opérées sans contrôle d'un juge ou d'une autorité indépendante. Les États-Unis d'Amérique font relativement peu de cas du respect de la vie privée – le *Privacy Act* de 1974 ayant une faible portée (2) – alors que l'Union européenne et ses États membres considèrent la protection des données personnelles comme un droit fondamental – art. 8 de la Charte des droits fondamentaux de l'Union européenne (CDFUE) et art. 16 du Traité sur le fonctionnement de l'Union européenne. Consacrée aussi par la Convention n° 108 du Conseil de l'Europe du 28 janvier 1981 et son protocole additionnel n° 181 du 8 novembre 2001 et par l'interprétation de l'art.8 de la Convention européenne des droits de l'Homme par la cour éponyme (3) à laquelle font écho, en France, les décisions du Conseil constitutionnel (4) et du Conseil d'État (5), la protection des données personnelles 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. Le régime inspiré de la loi française *Informatique & Libertés* (6) interdit l'inclusion de données sensibles – relatives à la race ou à l'origine ethnique, aux opinions politiques, aux convictions religieuses ou philosophiques, à l'appartenance syndicale et celles concernant l'abus de drogue et d'alcool, la santé ou la vie sexuelle – dans les traitements de données et soumet ceux-ci à des contrôles par une autorité administrative indépendante – CNIL en France, Contrôleur européen de la protection des données (CEPD) pour l'Union européenne. L'art.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. La personne dont des données personnelles ont été enregistrées dans un fichier a un droit de s'informer, un droit d'accès direct, un droit de rectification, un droit d'opposition et, depuis peu, un « droit au déréférencement » (7). Ce ne sont pas des droits réels sur les données personnelles mais des droits personnels sur les traitements qui s'exercent par l'intermédiaire d'un tiers (8), même si le Conseil d'État préconise de « concevoir le droit à la protection des données comme un droit à « *l'autodétermination informationnelle* », c'est-à-dire le droit de l'individu de décider de la communication et de l'utilisation de ses données à caractère personnel » (9).

La coopération anti-terroriste entre l'Europe et les États-Unis doit concilier des approches

contradictoires comme l'illustrent les péripéties entourant les accords PNR mais aussi les accords dits *Society for Worldwide Interbank Financial Transactions – Terrorist Finance Tracking Program* (*SWIFT-TFTP*), lesquels ont généré un conflit au sein même des institutions de l'Union européenne du fait des différences d'appréciation sur les concessions à faire par la Commission et le Conseil, d'une part, et, d'autre part, par la Cour de justice et le Parlement [I]. Cette opposition interinstitutionnelle a empêché l'adoption d'un PNR européen, mais la France a décidé de suivre l'exemple britannique en élaborant un PNR national. Au niveau de l'Union européenne comme de la France, d'autres mesures de prévention du terrorisme menacent la vie privée par la surveillance et la collecte généralisées de données personnelles [II].

I – La coopération entre l'Union européenne et les États-Unis en matière de prévention du terrorisme au défi du droit fondamental à la protection des données personnelles

La directive 95 /46 définit un niveau de protection *adéquat* devant être atteint dans chaque État membre et interdit le transfert de données vers un pays ne présentant un tel niveau de protection. Les États-Unis n'offrent pas de garanties adéquates – à la différence de l'Australie ou du Canada avec lesquels des accords PNR ont été adoptés (10) – ce qui explique que de longues tractations ont été nécessaires pour aboutir aux accords PNR [A] et *SWIFT-TFTP* [B].

A – Les accords PNR

Les divergences d'appréciation au sein des institutions européennes sur la légalité des premiers accords conclus avec les États-Unis [a] ont conduit à l'adoption d'un accord en 2011, plus respectueux de la protection des données personnelles [b].

a –Les accords de 2004 et de 2007

La loi du 19 novembre 2001 sur la sûreté de l'aviation et des transports (*Aviation and Transportation Security Act*) 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 sous peine de lourdes amendes, voire de ne pouvoir pénétrer l'espace aérien américain, mais les compagnies européennes ne pouvaient alors pas se plier à ces exigences incompatibles avec le droit communautaire et leur droit national.

Un premier accord fut donc conclu le 28 mai 2004, mais les décisions 2004/535/CE de la Commission et 2004/496/CE du Conseil le mettant en œuvre en droit communautaire furent annulées le 30 mai 2006 par la Cour de justice (11) qui toutefois maintint en vigueur les effets de l'accord jusqu'au 30 septembre 2006. Après un accord intérimaire du 19 octobre 2006 qui expira le 31 juillet 2007, un nouvel accord fut conclu les 23 et 27 juillet 2007. Il prévoyait que les transporteurs aériens permettraient l'accès informatique des services du *Department of Homeland Security* (DHS) aux données des passagers à destination ou en provenance des États-Unis, cependant, en mai 2010, le Parlement européen (PE) repoussa son vote sur l'accord et appela la Commission à négocier un nouveau texte.

b – L'accord de 2011

Le nouvel accord PNR (12) dispose que les transporteurs fournissent au DHS leurs données pour 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. Le DHS doit filtrer et effacer dans les 30 jours – sauf en cas de menace à la vie d'une personne ou de procédure pénale spécifique – les données sensibles, et

protéger les autres données contre toute altération, destruction ou divulgation non autorisée. Le DHS doit informer les autorités européennes des cas d'incidents graves portant atteinte au respect de la vie privée de citoyens de l'Union. Les dossiers PNR sont conservés 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, mais, six mois après leur réception, ces dossiers sont « dépersonnalisés » (occultation des informations permettant l'identification).

L'accord prévoit que le DHS ne peut partager les PNR qu'avec Europol, Eurojust ou les autorités publiques nationales enquêtant sur les infractions susmentionnées, ainsi, l'utilisation des données PNR présente un risque d'extension à d'autres fins que la lutte contre le terrorisme. Il est à craindre que ne se mette en place un système global de profilage 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 et les déroutements d'avions à destination des États-Unis ne concernent que des cas d'homonymie (13) et de journalistes trop critiques de la politique états-unienne (14).

B – L'Accord *SWIFT-TFTP*

Dans ce cas aussi, le PE a fait obstacle à un texte contredisant le droit fondamental à la protection des données personnelles [a] obligeant l'UE à renégocier un accord acceptable [b].

a – Historique

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. Initialement, les autorités états-uniennes pouvaient adresser des injonctions (*administrative subpoenas*) à *SWIFT* pour obtenir des données parce que ses serveurs étaient situés sur le sol américain, mais influencée par les agences de protection des données (15), *SWIFT* opère désormais ses transferts de messagerie financière depuis les Pays-Bas et la Suisse.

Afin de concilier la lutte contre le terrorisme et le droit européen de la protection des données, un accord provisoire (*Interim Agreement*) fut négocié et accepté par la décision du Conseil 2010/PESC/JAI du 30 novembre 2009. En dépit des pressions états-uniennes (16), ce premier accord *SWIFT-TFTP* fut rejeté le 11 février 2010 par le PE à cause de l'absence de proportionnalité entre les règles afférentes au transfert de données et à leur stockage et la sécurité supposément fournie et parce que les citoyens européens n'auraient pas pu former un recours contre les autorités états-uniennes en cas de mauvaise utilisation de leurs données personnelles car le *Privacy Act* réserve ces actions aux ressortissants américains (17).

b – L'Accord

Le nouvel accord *SWITF-TFTP* (18) prévoit que les fournisseurs de services de messagerie financière doivent, à la demande du Trésor états-unien, transférer à celui-ci des données aux fins de la prévention et de la détection du terrorisme ou de son financement. Les injonctions du Trésor doivent identifier clairement les données nécessaires au renseignement, aux enquêtes ou aux poursuites anti-terroristes. Une copie de ces injonctions est adressée à Europol qui doit vérifier si la demande est recevable ; dans l'affirmative, la demande devient juridiquement contraignante, obligeant le fournisseur à exporter vers le Trésor les données réclamées. Néanmoins, le contrôle d'Europol a été très critiqué, car peu efficace, par l'Autorité de contrôle commune (19) et par le PE (20).

Les données transmises sont effacées au bout de cinq ans, tandis que les informations extraites des données fournies sont conservées pendant la durée nécessaire aux enquêtes ou poursuites spécifiques.

Le Trésor peut partager les données avec tout État ou organisation internationale, ainsi qu'avec Europol ou Eurojust, mais tout partage d'informations afférentes à un citoyen de l'UE avec les autorités d'un pays tiers est soumis à l'accord préalable des autorités de l'État membre concerné, sauf lorsque ce partage est essentiel pour prévenir une menace grave et immédiate. Le Trésor peut aussi communiquer des informations pertinentes obtenues dans le cadre du TFTP à la demande d'Europol, d'Eurojust ou d'une autorité compétente d'un État membre de l'UE.

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, mais son innovation réside dans le suivi des garanties par des contrôleurs indépendants, dont une personnalité désignée par la Commission européenne en accord avec les États-Unis.

Le PE accepta ce nouvel accord plus équilibré – et aussi parce que la Fédération bancaire européenne avait insisté sur nécessité de revenir à la sécurité juridique que le vote du 11 février 2010 avait mise à mal (21).

Les accords PNR et SWIFT-TFTP continuent d'être critiqués du fait de l'absence d'autorité administrative indépendante chargée de la protection des données personnelles aux États-Unis et suscitent une crainte de dérives que les révélations de M. Edward SNOWDEN ne font que renforcer. Le droit fondamental à la protection des données personnelles est sacrifié sur l'autel de la prévention du terrorisme car la Commission n'a pu obtenir des États-Unis ce qu'elle obtint de l'Australie ou du Canada (22).

II – Le droit à la protection des données personnelles et les mesures préventives européennes et françaises

L'instauration d'un système PNR mais aussi d'autres modalités de surveillance massive et indiscriminée de la population sont d'actualité au sein de l'UE [A] et en France [B].

A – Les mesures de l'Union européenne

L'élaboration d'un PNR européen revient à l'ordre du jour [a], pourtant l'invalidation de la directive sur la rétention des données devrait faire réfléchir quant à la compatibilité avec la CFDUE des mesures préventives systématisées [b].

a – La question du PNR européen

En novembre 2007, la Commission avait présenté une proposition de directive pour établir un PNR européen aux fins de prévention du terrorisme qui fut rejetée l'année suivante par le Parlement européen. La Commission présenta une nouvelle proposition en 2011 (23), mais le PE s'y opposa le 24 avril 2013, ce qui n'a pas empêché la Commission de participer au financement de projets PNR nationaux dans 14 États membres (24).

Le 11 janvier 2015, le ministre français de l'Intérieur a exhorté le PE à adopter le PNR européen, demande relayée le surlendemain par le Président du Conseil européen qui craint qu'en l'absence d'une telle directive ne se mettent en place 28 systèmes nationaux formant un « patchwork rempli

de lacunes ». Le changement de position des députés ADLE et S&D sera déterminant pour l'adoption de cette directive PNR, mais beaucoup subordonnent leur vote à la prochaine décision de la Cour sur l'accord PNR avec le Canada (25).

De surcroît, la directive 95/46 devant être remplacée par un règlement (26) et la décision-cadre 2008/977/JAI par une directive (27), il semble plus logique d'attendre que ces textes soient adoptés avant d'envisager le vote d'une directive PNR qui devra être compatible avec eux.

b – Autres mesures préventives

Suite aux attentats de Madrid et de Londres, a été adoptée la directive 2006/24/CE du 15 mars 2006 *relative à la conservation des données* afin d'harmoniser les mesures nationales obligeant les fournisseurs de télécommunication et de services informatiques à conserver les métadonnées – et non le contenu des communications ou des sites internet visités – de leurs clients pour les transmettre sur requête aux services de police ou de renseignement.

La Cour de justice fut saisie de deux questions préjudicielles sur la compatibilité de cette directive avec la CFDUE ; elle trancha en faveur de l'incompatibilité étant donné que *« ces données, prises dans leur ensemble,* [étaient] *susceptibles de permettre de tirer des conclusions très précises concernant la vie privée des personnes dont les données ont été conservées… »* (§ 27), ce qui constituait une *« ingérence […] d'une vaste ampleur […] susceptible de générer dans l'esprit des personnes concernées […] le sentiment que leur vie privée fait l'objet d'une surveillance constante »* (§ 37), d'autant plus que la directive couvrait *« de manière généralisée toute personne et tous les moyens de communication électronique »* (§ 57), ne prévoyait *« aucun critère objectif permettant de délimiter l'accès des autorités nationales compétentes aux données et leur utilisation ultérieure »* (§ 60) et que la durée de conservation était fixée sans tenir compte de l'utilité de la conservation par rapport aux objectifs poursuivis (§ 63 & 64) (28).

Cette surveillance indiscriminée et disproportionnée diffère des mesures opérationnelles d'Europol ou de la coopération et de l'échange d'informations entre les autorités répressives (29) qui ciblent des personnes déjà condamnées ou fortement suspectées dans le cadre de procédures contrôlées par des magistrats. Les règles strictes en matière de protection des données personnelles – qui devraient se renforcer avec l'adoption des propositions de règlement et de directive (30) – s'imposant à EUROPOL offrent des garanties satisfaisantes, conciliant lutte contre le terrorisme et vie privée (31).

B – Les mesures françaises

La France s'est dotée d'un système PNR qui n'est pas encore opérationnel [a], et de mesures de surveillance, dont les plus récentes n'ont été adoptées que par l'Assemblée nationale – le Sénat et le Conseil constitutionnel, que le Président de la République devrait saisir, ne s'étant pas encore prononcé [b].

a – Le PNR français

L'art.7 de la loi n° 2006-64 du 23 janvier 2006 *relative à la lutte contre le terrorisme* autorise 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'UE. Sont également concernées les données directement collectées à partir de la bande de lecture optique des

documents de voyage, de la carte d'identité et des visas des passagers de transporteurs aériens, maritimes ou ferroviaires.

Un arrêté du 19 décembre 2006 institue, 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 » (32).

Par ailleurs, l'art.65 du code des douanes permet à l'administration de requérir ponctuellement et expressément les données PNR de certains vols.

L'art.L. 232-7 du code de la sécurité intérieure (CSI), résultant de 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, mis en œuvre par le décret n° 2014-1095 du 26 septembre 2014. Dans un avis du même jour, la CNIL a considéré que les garanties réduisaient le risque d'atteinte à la protection des données personnelles (33).

b - L'extension de la surveillance

La loi de programmation militaire permet aussi aux services de renseignement de créer un traitement automatisé des données personnelles (art.L.232-7-I CSI), sous le contrôle de la Commission nationale de contrôle des interceptions de sécurité (CNCIS).

Les articles L.246-1 à L.246-5 CSI obligent les opérateurs de communication à conserver pendant un an l'ensemble des métadonnées pour répondre aux demandes des services de lutte anti-terroriste ou de renseignement. Ce traitement de ces « données de trafic » par ces services constituant de pures opérations de police administrative ne peut relever du juge judiciaire (34).

Le projet de loi sur le renseignement énumère sept motifs d'intérêt public (35) qui autorisent, selon le futur article L 853-1 CSI, l'*« utilisation de dispositifs techniques permettant [... l]a captation, la transmission et l'enregistrement de données informatiques transitant dans un système automatisé de données ou contenues dans un tel système. »* Ces mesures seront surveillées par la Commission nationale de contrôle des techniques de renseignement (CNCTR) - autorité administrative indépendante substituée à la CNCIS - qui rendra au Premier Ministre un avis sur l'autorisation des captations, sauf en cas d'urgence absolue.

Le projet de loi introduit aussi dans le CSI d'appréciables innovations, dont la garantie de la vie privée et - grâce à un amendement parlementaire - la protection des données personnelles et la référence au principe de proportionnalité (36) (art.L.811-1), la destruction des extraits ou exploitations des traitements n'étant plus indispensables (art.L.822-3) et, surtout, le recours devant le Conseil d'État saisi par toute personne ayant un intérêt direct et personnel, par la CNCTR ou par toute juridiction à titre préjudiciel. Le Conseil d'État ne pourra pas se voir opposer le « secret défense », même s'il ne divulguera pas les informations ainsi classifiées (art.L.841-1).

Il est encore trop tôt pour savoir ce que sera finalement la loi sur le renseignement, néanmoins, la France tente l'équilibrisme entre prévention du terrorisme et protection des données personnelles.

Les futures interprétations prétoriennes de l'arrêt *Digital Rights*, en France ou dans l'UE, pourraient faire pencher la balance en faveur de cette dernière au détriment des articles L.246-1 à L.246-5 CSI. Même si l'air du temps est aux mesures sécuritaires, tout n'est donc pas perdu pour le respect de la vie privée.

Notes

(1) A. Türk, La vie privée en péril. Des citoyens sous contrôle, Odile Jacob, 2011.

(2) Cf. S. Preuss-Laussinotte, « Bases de données personnelles et politiques de sécurité », Culture & Conflits, n° 64, 2006, p. 83 ; Conseil d'État, Libertés et numérique, La documentation française, 2014, p. 72-74.

(3) CEDH, 26.03.87, Leander c/ Suède ; 25.03.98, Amman c/ Suisse ; 04.05.00, Rotaru c/ Roumanie ; 14.02.06, Turek c/ Slovaquie ; 04.12.08, S. & Marper c/ Royaume-Uni ; 10.02.11, Dimitrov-Kazakov c/ Bulgarie ; 24.05.11, Association « 21 Décembre 1989 » e.a. c/ Roumanie ; 18.09.14, Brunet c/ France. La Cour reconnaît cependant que la lutte contre le terrorisme peut justifier des restrictions au secret de la correspondance et des télécommunications (06.09.79, Klass e.a. c/ Allemagne) ou la conservation de certaines données par les services de sécurité (06.06.06, Segerstedet-Wiberg e.a. c/ Suède). Cf. A. Petropoulou, Liberté & sécurité : Les mesures anti-terroristes et la Cour européenne des droits de l'Homme, Pédone, 2014, p. 443-461.

(4) 2012-652 DC du 22.03.12, Loi relative à la protection de l'identité, § 8 ; le C. const. a jugé conforme à la Const. les fichiers de police judiciaire (2003-467 DC du 13.03.03, Loi sur la sécurité intérieure, § 17-46) et le fichier national automatisé des empreintes génétiques (FNAEG) concernant notamment l'identification des auteurs d'actes de terrorisme (2010-25 QPC du 16.09.10).

(5) CE, Ass., 26.08.11, Association pour la promotion de l'image, Rec., p. 505.

(6) Loi n° 78-17 du 06.01.78 révisée par la loi n° 2004-801 du 06.08.04 ; cf. J. Harivel, « La difficile protection des données à caractère personnel dans une société numérique », in I. Bouhadana & W. Gilles (dir.), Droit et gouvernance des données publiques et privées à l'ère du numérique, IMODEV, 2015, p. 57-64 ; Conseil d'État, op. cit., p. 70-76 & 86-87.

(7) CJUE, 13.05.14, Google Spain SL & Google Inc. c/ AEPD & Mario Costeja Gonzalez, C-131/12 ; Cf. B. Hardy, « La géographie du droit à l'oubli », R. trim. droit eur., 2014, p. 879-897 ; H. Kranenborg, « Google and the right to be forgotten », Euro. Data Protec. L. R., 2015, p. 70-79 ; Conseil d'État, op. cit., p. 184-189.

(8) Cf. Th. Saint-Aubin, « Les droits de l'opérateur de données sur son patrimoine numérique informationnel », in I. Bouhadana & W. Gilles (dir.), op. cit., p. 143-144 ; J. Eynard, Les données personnelles. Quelle définition pour une protection efficace ?, Michalon, 2013, p. 141-182.

(9) Conseil d'État, op. cit., p. 337 ; présentation détaillée, p. 264-269.

(10) Accord UE-Australie du 13.09.11, dossier interinstitutionnel 2011/0126 (NLE) ; Accord UE-Canada du 30.11.13, dossier interinstitutionnel 2013/0250 (NLE) – ce dernier n'a pas n'a pas encore été approuvé par le PE qui a saisi la CJUE de sa compatibilité avec la CFDUE, en attendant un précédent accord conclu entre l'UE et le Canada en 2006 demeure en vigueur. En outre, un accord UE-Mexique est envisagé et la Russie et la Corée du Sud ont fait des demandes en ce sens.

(11) CJUE, 30.05.06, Parlement européen c/ Conseil de l'Union européenne & Commission des Communautés européennes, C-317/04 & C-318/04. Cet arrêt porte seulement sur la base légale de la décision 2004/535.

(12) Dossier interinstitutionnel 2011/0382 (NLE), 08.12.11.

(13) Cf. J.-C. Martin, Les règles internationales relatives à la lutte contre le terrorisme, Bruylant, 2006, p. 369-370.
(14) Cf. Le Monde, 03.10.12.
(15) Avis du 27.09.06 de la Commission de la Protection de la Vie Privée (Belgique) ; avis 2006/10 du G.29 du 22.11.06 ; avis du CEPD du 01.02.07.
(16) Cf. J. Santos Vara, The Role of the European Parliament in the conclusion of the Transatlantic Agreements on the Transfer of Personal Data after Lisbon, CLEER Working Papers, 2013/2, p. 16.
(17) Cf. C. Pouliquen, Le cadre européen de protection des données en matière pénale, Bruges Pol. Res. Pap., n° 29, 2013, p. 17.
(18) JOUE, L.195/5, 27.07.10.
(19) http://europoljsb.consilium.europa.eu.media/111009/terrorist%20finance%20tracking%20program%2028tftp%29%20inspection%20report%20-%20public%20version.pdf (paywall)
(20) www.europarl.europa.eu/en/pressroom/content/20110314IPR15463/html/SWIFT
(21) Cf. H. Farrell & A. Newman, « The New Politics of Interdependence », Comp. Pol. Stud., 2014, p. 12.
(22) Cf. M.-F. Labouz, « Le nouvel accord sur les données de passagers aériens (PNR) entre l'Union européenne et les États-Unis », in E. Saulnier-Cassia (dir.), La lutte contre le terrorisme dans le droit et la jurisprudence de l'Union européenne, LGDJ, 2014, p.269.
(23) COM(2011) 32 final.
(24) Cf. N. Vandystadt, « PNR still divisive in European Parliament », Europolitics, n° 4971, 13.11.14, p. 13.
(25) Cf. S. Peyrou, www.gdr-elsj.eu/2015/01/25/cooperation-judiciaire-penale
(26) COM(2012)11 final.
(27) COM(2012)10 final.
(28) CJUE, 08.04.14, Digital Rights Ireland & Seitleinger, C-293/12 & C-594/12 ; cf. Conseil d'État, op. cit., p. 197-201.
(29) Cf. C. Castets-Renard, Droit de l'internet, Montchrestien, 2e éd., 2012, p. 469-470.
(30) Cf. A. Gattolin e. a., Rapport d'information fait au nom de la commission des affaires européennes sur Europol et Eurojust, Sénat, 17.04.14, p. 17-19. .
(31) Cf. A. Gutirrez-Zarza (dir.), Exchange of Information and Data Protection in Cross-border Criminal Proceedings in Europe, Springer, 2015, p. 95.
(32) Cl. Guerrier, « Passenger Name Record 2012 », 02.07.12, www.juriscom.net/wp- content/documents/pnr20120702.pdf
(33) www.cnil.fr/les-themes/deplacements-transports/du-systeme-api-pnr-france/
(34) C. const., 2005-532 DC du 19.01.05, Loi relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers, § 5.
(35) Sécurité nationale ; intérêts essentiels de la politique étrangère et l'exécution des engagements européens et internationaux de la France ; intérêts économiques et scientifiques essentiels de la France ; prévention du terrorisme ; prévention de la reconstitution ou du maintien de groupement dissous ; prévention de la criminalité et de la délinquance organisées ; prévention des violences collectives de nature à porter gravement atteinte à la paix publique.
(36) Sur les principes de nécessité et de proportionnalité, cf. avis 01/2014 du G29 du 27.02.15.