Les fichiers PNR et les transports aériens internationaux

par Xavier LATOUR

Professeur de droit public à l'Université Côte d'Azur,

CERDACFF (EA 7267)
Faculté de droit et de science politique de Nice
Secrétaire général de l'AFDSD

En matière de sécurité, en particulier dans les transports internationaux de voyageurs, les États et les opérateurs sont contraints de coopérer.

Les transports traduisent l'exposition à des menaces communes, d'intensité variable et transcendant les frontières. Cela concerne prioritairement le transport aérien dont la croissance en termes de flux et de personnes transportées se poursuit[1]. En raison de sa fragilité et de la symbolique d'une attaque forcément massive, l'avion demeure une cible de choix[2], désormais rejoint par les navires.

Dans un contexte de recours massif aux technologies, la tentation est grande de ficher. Depuis les attentats du 11 septembre 2001, l'échange d'informations s'est accéléré. Les moyens de stockage et de transmission offerts par l'informatique ont fait entrer la sûreté des transports dans l'ère de la surveillance de masse.

Les États ont rapidement perçu l'intérêt d'exploiter les fichiers pour mieux limiter les menaces inhérentes au transport aérien. L'accès aux données ne se fait pas uniquement sur réquisition judiciaire, il aide à l'anticipation. En matière de transport en général, et de transport aérien en particulier, ils ont recours à la collecte et à l'exploitation des *passenger name record* (PNR).

Les transporteurs (et parfois les agences de voyages[3]) recueillent les données relatives à chaque passager, et les transmettent obligatoirement aux

1. 108 millions de passagers en 1960, plus de 3 milliards en 2016, 6 milliards prévus en 2030.
2. X. Latour (dir.), *La sécurité et la sûreté des transports aériens,* Paris, L'Harmattan, 2005, 213 p.
3. En France, depuis la loi n° 2015-917 du 28 juillet 2015 actualisant la loi de programmation militaire 2013-2019.

administrations de sécurité des États. Au-delà des éléments basiques constitutifs des données *Advance Passenger Information system* – API- (identité et coordonnées, nationalité, sexe, documents d'identité), d'autres sont collectés (dates, itinéraires, moyen de paiement, bagages), y compris plus personnels (repas pris, services ajoutés, contacts au sol…). Les fichiers PNR ont acquis une finalité préventive opérationnelle, ou d'enquête postérieurement à un acte illicite.

Ce mouvement de fichage peut être spécifique à un État. La Grande-Bretagne a développé son programme en 2004. De son côté, la France a d'abord créé, à titre expérimental jusqu'au 31 décembre 2017, un fichier « API-PNR France »[4] (articles L 232-7, R 232-12 et s. du code de la sécurité intérieure – CSI). La loi n° 2017-1510 renforçant la sécurité intérieure et la lutte contre le terrorisme, du 30 octobre 2017, l'a pérennisé, tout comme un fichier propre au secteur maritime. Non lié à une initiative européenne, ce dernier s'inspire du PNR aérien, sans que les données collectées soient identiques (article L 232-7-1 CSI).

Dans un registre comparable et sur le fondement de la loi n° 2015-912 du 24 juillet 2015 relative au renseignement, l'article L. 561-26 du code monétaire et financier impose aux transporteurs routier, maritime, ferroviaire et aérien, ainsi qu'aux opérateurs de voyage de transmettre à TRACFIN, à sa demande, les informations relatives à l'identité, au déplacement et aux bagages des personnes transportées.

Dans un cadre international, les États-Unis soutiennent la circulation des informations PNR. Après les attentats de 2001, l'État américain a pesé de tout son poids pour obtenir l'accès aux fichiers d'autres États[5].

Au sein même de l'Union européenne, les ministres de l'Intérieur ont promu l'idée d'un fichier européen pour construire une réponse coordonnée à la montée en puissance des périls terroristes. Ce processus initié au début des années 2000 s'est accéléré après les attentats en France (2015) et en Belgique (2016). Après de longues tergiversations, la directive PNR a été adoptée le 27 avril 2016 (2016/681)[6] pour être appliquée au plus tard le 25 mai 2018 (la loi n° 2017-1510 en assure la transposition).

Les échanges de données démultiplieraient les effets du fichage. Pourtant, les fichiers PNR ne font pas l'unanimité. Au contraire, ils soulèvent de nombreuses interrogations juridiques et pratiques. Juridiquement, les plus importantes portent sur leur compatibilité avec le respect des libertés[7]. Force est de constater qu'en raison de leur ampleur, ses fichiers relèvent d'une

4. Décret n° 2014-1095 du 26 septembre 2014 ; N. Catelan, « Lutte contre le terrorisme », *RS Crim.* 2015, p. 425.
5. *Aviation and Transportation Security Act* du 19 novembre 2001 et *Enchanced Border Security and Visa Entry Reforme Act* du 5 mai 2002.
6. R. Brett, « La directive "PNR" du 27 avril 2016, nouvelle étape de la politique européenne de lutte contre la criminalité », *Europe,* janv. 2017, ét. 1.
7. B. Pauvert, « La difficile conciliation de la sûreté aérienne et du respect des libertés individuelles ? », dans *La sécurité et la sûreté des transports aériens, op. cit.*, p. 81.

surveillance généralisée. Cette ingérence dans la sphère privée des passagers ne doit pas être ignorée. En pratique, ils renvoient à la complexité des relations étatiques dans le domaine sensible de la sécurité.

Dès lors, si les fichiers PNR sont appréhendés comme étant des vecteurs d'une coopération nécessaire (**I**), celle-ci s'avère être aussi difficile (**II**).

I. Les fichiers PNR, vecteurs d'une coopération nécessaire

Dans un domaine régalien, la coopération entre les États ne constitue pas toujours une évidence. Pourtant en matière de données PNR, de solides arguments la justifient (**A**), et expliquent qu'elle se concrétise de plus en plus (**B**).

A. Les justifications de la coopération

Après les attentats du 11 septembre, les États-Unis sollicitent les premiers l'Union européenne afin d'établir un programme de transferts des données. Ils étaient décidés à ériger un mur électronique et informationnel anti-terroriste pour empêcher d'agir sur leur sol des passagers en provenance d'une Europe perçue, déjà, comme étant dangereuse.

Les États membres ont plutôt bien accepté la demande américaine et la Commission européenne a engagé rapidement les négociations. Dès 2004, elle a donné son accord aux transferts des données PNR[8].

Pour l'Europe, il s'agissait d'une part d'écarter le risque d'un blocage de l'activité économique des compagnies aériennes. Les autorités américaines menaçaient, en effet, d'interdire de vol les compagnies des États ne répondant pas à leurs sollicitations, en plus de leur infliger des pénalités financières.

D'autre part, les enjeux sécuritaires ont achevé de convaincre le Conseil et la Commission de trouver une solution. L'argument de la lutte contre le terrorisme s'imposait avec la force de l'évidence. L'évidence était telle que rien ne justifiait de souligner ce point à l'excès. Ainsi, en une phrase dans la décision de la Commission du 14 mai 2004, le considérant n° 8 précise que « *La Communauté soutient entièrement les États-Unis dans leur lutte contre le terrorisme, dans les limites imposées par le droit de la Communauté* ». Les statistiques tendraient, en effet, à prouver l'efficacité des fichiers PNR[9]. La lutte contre le terrorisme ne motive pas seulement la collecte des données. Elle vise aussi à endiguer la criminalité organisée (voir par exemple l'accord avec le Canada), voire l'immigration clandestine laquelle fait pourtant, en Europe, l'objet d'une approche spécifique dans le cadre du dispositif

8. C (2004) 1914.
9. Guy Geffroy, Rapport d'information AN sur la proposition de directive relative à l'utilisation des données des dossiers passagers pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière, n° 3961, 2011.

SETRADER[10]. Les éléments collectés représenteraient des éléments importants de surveillance aux frontières extérieures.

Depuis 2013, la nécessité de mieux contrôler le retour de combattants étrangers des zones de conflit djihadistes renforce la démarche européenne.

Les points 5 et 6 (sur 41) de l'exposé des motifs de la directive européenne synthétisent les objectifs[11] et recoupent la liste des infractions graves qui justifient une prévention par l'intermédiaire d'un fichier PNR (Annexe II de la directive). La loi n° 2017-1510 du 30 octobre 2017 poursuit les mêmes buts, sans pour autant que l'étude d'impact n'apporte d'éléments précis sur les résultats obtenus pendant la phase d'expérimentation.

Si la souveraineté étatique marque le transport aérien de son empreinte, comme en témoigne la convention de Chicago du 7 décembre 1944, les impératifs de coopération existent sans aucun doute. La coopération constitue un impératif du transport aérien, tant les États sont dans l'incapacité de réagir isolément. Dans un cadre intergouvernemental ou plus intégré, bilatéral ou multilatéral, les solutions se recherchent de manière coordonnée.

En droit, l'Organisation de l'Aviation civile internationale (OACI) a rendu obligatoires les recommandations originelles de la Convention de Chicago. Dans un cadre régional, des normes de l'Union européenne interviennent également, tandis que des instruments bilatéraux complètent le dispositif.

Parce que l'OACI soutient la coopération, elle a publié, à partir de 2005, des pratiques recommandées et des lignes directrices destinées à structurer le transfert des données PNR[12]. Pour l'OACI, la technique des données PNR est conforme à l'Annexe17 de la Convention de Chicago qui cherche à concilier la sûreté et la circulation des passagers.

Justifiée par l'intensité des menaces, la coopération en matière d'échanges de données PNR se concrétise de différentes manières.

B. La concrétisation de la coopération

La coopération s'inscrit aussi bien le cadre des relations de l'Union européenne avec des États tiers que dans celui des relations entre les États membres de l'Union européenne.

---

10. Système européen de traitement des données d'enregistrement et de réservation, arrêté du 11 avril 2013 (article L 232-1 CSI).

11. Point 5 : « les objectifs de la présente directive sont, entre autres, d'assurer la sécurité, de protéger la vie et d'assurer la sécurité des personnes » ; Point 6 : « *L'utilisation effective des données PNR, par exemple la confrontation des données PNR à diverses bases de données de personnes ou d'objets recherchés, est nécessaire 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, et donc pour renforcer la sécurité intérieure, pour rassembler des preuves et, le cas échéant, pour trouver les complices de criminels et démanteler des réseaux criminels* », PE et Cons. UE, dir. 2016/681/UE, 27 avril 2016.

12 P. Dupont, « Les données des dossiers passagers (PNR) dans le transport aérien », *Rev. fr. de droit aérien et spatial* 2016/2, p. 111.

La première coopération d'envergure résulte d'une volonté appuyée des États-Unis.

Pour des raisons pratiques, les Américains ont préféré négocier directement avec l'Union européenne, plutôt que de se lancer dans des négociations bilatérales longues. Cette démarche a ouvert un débat juridique difficile au sein des institutions européennes et n'a abouti qu'en 2012.

Après plusieurs années de négociations et de divergences au sein même des institutions européennes, un accord a été conclu pour une durée de sept ans.

Peu de temps auparavant, en 2011, l'Australie obtenait le même droit d'accès. Des négociations sont en cours avec le Canada et le Mexique.

L'idée d'un PNR européen n'est, quant à elle, pas nouvelle. La Commission européenne l'avance au début des années 2000 afin d'améliorer les moyens de lutte contre le terrorisme, des infractions graves et l'immigration clandestine.

L'objectif d'une coordination des PNR nationaux motive les instances européennes et les États membres.

Les premiers travaux ont réellement débuté en 2007 avec, à l'époque, une proposition de décision-cadre par la Commission. En raison de la communautarisation du pilier « sécurité » par le Traité de Lisbonne, une proposition de directive a suivi, en 2011.

Par la suite et au nom des impératifs de sécurité, les États n'ont eu de cesse de demander l'aboutissement du projet ralenti par des divergences au sein des institutions européennes et entre certains États.

Malgré la lenteur regrettable de l'adoption du fichier PNR, l'Union et ses États ont enfin abouti. Comment pourrait-il en être autrement en raison de l'intensité de la menace ?

Les attentats de Paris de novembre 2015 et ceux de Bruxelles de mars 2016 ont accéléré la prise de conscience d'un besoin de coopération accrue. Elle s'exprime dès le 20 novembre 2015 dans les conclusions du Conseil de l'Union européenne, tandis que dans la foulée le Parlement européen parvient à surmonter ses réticences à l'égard du fichier PNR. Il adopte, le 16 avril 2016, la directive sur le transfert des données relatives aux passagers[13]. Le texte n'emporte pas complètement la conviction. Il n'appréhende pas, en principe, les vols intra-européens et les moyens de transport autres qu'aériens. En outre, la directive vise davantage à harmoniser les PNR nationaux qu'à créer un véritable PNR européen. Malgré tout, le texte s'inscrit dans une dynamique positive.

Les travaux sur le PNR ont stimulé la réflexion sur d'autres sujets. La comptabilisation des passagers entrés et sortis est une option sérieuse malgré son coût de plusieurs centaines de millions d'euros. Des efforts sont,

13. PE et Cons. UE, dir. 2016/681/UE, 27 avril 2016.

également, envisagés en matière de fonctionnement des banques de données nationales et européennes pour en améliorer l'interopérabilité.

En dépit du bien-fondé de la coopération, le transfert de données PNR se heurte à de nombreuses difficultés.

II. Les fichiers PNR, vecteurs d'une coopération difficile

Les obstacles à la circulation des données PNR sont divers. Les demandes formulées par les États-Unis après 2001 ont reflété une tendance marquée à vouloir imposer au monde leur vision de la sécurité des transports. Entre la négociation et la sanction, les États concernés n'avaient guère de choix.

Surtout, tout travail sur les fichiers nominatifs renvoie à la nécessité de prendre en considération la protection des libertés individuelles. Dès lors, la conciliation exigeante entre sécurité et liberté complique l'utilisation des données personnelles (**A**), et remet en cause la légalité même des fichiers PNR (**B**).

A. L'utilisation des données personnelles

Rapidement, la négociation de l'accord de transfert avec les États-Unis s'est heurtée à la question centrale de la protection de la vie privée des personnes fichées. De vives critiques[14] ont accompagné les travaux. Aux côtés du G29 (groupe européen rassemblant des organes nationaux compétents en matière de protection des données), le Parlement européen était très en pointe dans la contestation de la demande américaine. Il a même remporté une victoire symbolique, mais éphémère. La Cour de justice de la Communauté européenne[15] a en effet annulé, en 2006, un premier accord conclu avec les États-Unis. Cela n'a pas empêché qu'un autre texte aboutisse plus tard. Les opposants à l'accord saluèrent cette victoire, tandis que d'autres ont surtout insisté sur une perte de temps[16].

L'expérience américaine a mis en lumière plusieurs points de tension. Certains s'inscrivent dans le contexte propre aux relations des États de l'Union européenne avec des États tiers, d'autres rejoignent les doutes sur un PNR européen.

La protection des libertés motive une vigilance particulière à l'égard des données PNR. Les critiques scrutent toutes les composantes du dispositif au prisme des principes de proportionnalité et de nécessité. Ils sont les gardiens

14. S. Peyrou, « Droits fondamentaux versus diplomatie, ou le pot de terre contre le pot de fer : réflexions sur la conclusion de l'accord PNR entre les États-Unis et l'Union européenne », *Europe* 2012, ét. 8.
15. CJCE 30 mai 2006, aff. jointes. C-317/04 et C-318/04, *Parlement c/ Conseil et Commission* ; F. Mariatte, « La sécurité intérieure des États-Unis… ne relève pas des compétences externes des Communautés », *Europe* 2006, ét. 8.
16. P. Bonnecarrère et S. Sutour, Rapport d'information du Sénat, *L'Union européenne et la lutte contre le terrorisme*, n° 442, 4 mars 2016, p. 19.

sourcilleux du droit à la protection des données personnelles consacré, initialement, par la directive 95/46, puis par le règlement 2016/679 du 27 avril 2016 dans le prolongement de la Charte européenne des droits fondamentaux.

Cela commence par les données collectées. Alimenté par des éléments trop largement appréciés, le fichier s'apparenterait à une ingérence excessive et susceptible de créer une suspicion abusive. Trop strictement considérées, les données perdraient de leur intérêt sécuritaire. Pour ce qui est du PNR européen et afin de prévenir tout risque de discrimination, l'Union européenne a tiré les leçons des discussions avec les Américains. Elle a pris soin d'interdire la collecte des informations qui révèlent la race, l'ethnie, la religion, les opinions… pour se centrer sur le seul déplacement. En revanche, les données sont rassemblées par l'intermédiaire des transporteurs et des opérateurs de voyage. Dans un même ordre d'idées, le champ des vols concernés est important. L'Union européenne a ainsi discuté de l'application aux seuls vols extra-européens ou de son élargissement aux vols intra-européens. Elle a finalement admis cette dernière possibilité à titre dérogatoire (avec information écrite de la Commission).

Les services de sécurité bénéficient, naturellement, du transfert des données collectées. Dans le cas des États-Unis, il était apparu rapidement que les bénéficiaires iraient bien au-delà de la seule administration du contrôle aux frontières. La tentation est réelle d'interconnecter des moyens technologiques pour construire un vaste réseau de surveillance de masse (profilage[17]). La redirection des données vers des États tiers à un accord retient aussi l'attention en raison des niveaux inégaux de protection des données selon les cas. La directive européenne tente de limiter ce risque en conditionnant strictement (article 11) les transferts.

Dans le même temps, l'utilisation des données dépasserait le strict contrôle aux frontières. Les objectifs poursuivis deviendraient flous, malgré des finalités textuellement énumérées, mais suffisamment vagues pour être malléables. À ces questionnements juridiques s'ajoutent des interrogations opérationnelles relatives à la possibilité d'exploiter réellement et efficacement une telle quantité d'informations, sauf à utiliser des algorithmes d'analyse qui soulèvent de nouvelles interrogations (biais, fiabilité…).

Cette crainte est à corréler avec le choix de la méthode de transfert. La technique du « push » (les transporteurs envoient les données) a la préférence des défenseurs des libertés. Retenue dans le cadre européen, elle favorise une meilleure maîtrise des éléments transférés. La technique du « pull » (accès direct aux données du transporteur par l'État demandeur) n'est pas complètement exclue, notamment dans l'accord avec les États-Unis et même si cela doit rester exceptionnel.

L'attention se porte, également, sur les durées de conservation des données et leur archivage avec une anonymisation progressive. Dans le cas américain,

17. Alex Türk, Pierre Piazza, « La difficile quête d'un équilibre entre les impératifs de sécurité publique et la protection de la vie privée », *Cultures et Conflits,* 2009, n° 76, p. 124.

la durée de quinze ans paraît excessive en dépit d'une dépersonnalisation des données puisque celle-ci est rétractable. Au-delà de 15 ans, les données, bien qu'anonymisées, ne sont pas effacées, ce qui ne semble pas justifié. L'Union européenne fait preuve, quant à elle, de davantage de raison en retenant une période de 5 ans, et une dépersonnalisation après 6 mois (article 12).

Enfin, si l'individu adhère à la collecte des données en concluant un contrat de transport, il ne perd pas tout droit de regard sur celles qui le concernent. Cela implique de lui garantir un droit d'accès, de rectification, voire d'effacement et d'indemnisation des préjudices subis.

L'effectivité de la protection dépend, cependant, de l'existence de mécanismes appropriés par des autorités indépendantes et par le juge (article 13 de la directive 2016/681). Dans le cas européen, les États ont accompli de sérieux efforts et adopté des standards communs. La situation est plus délicate pour des États tiers. L'indépendance des autorités de contrôle est parfois discutée (c'est le cas pour les États-Unis). Quant à l'accès au juge, la compétence des tribunaux des États d'utilisation des données accentue la complexité d'un recours.

Malgré ces difficultés, les accords PNR ne sont pas voués à l'échec. La Commission a ainsi salué la bonne application du dispositif par les États-Unis[18]. Elle souligne les progrès obtenus dans des domaines aussi essentiels que la dépersonnalisation des informations, l'accès aux données par les particuliers, le partage avec des États tiers et les recours offerts. Tout cela contribue d'ailleurs à une meilleure coopération des autorités américaines avec Europol et Eurojust.

Des améliorations sont encore nécessaires. Elles concernent, essentiellement, le nombre trop important d'agents ayant un accès aux données, des temps de réponse trop longs aux demandes des particuliers, ou encore une augmentation des procédures répressives qui empêche la dépersonnalisation.

Parce qu'aux besoins de sécurité répondent des obligations, non moins importantes, de protection des données personnelles, la légalité des fichiers PNR est remise en cause.

B. La remise en cause de la légalité des fichiers PNR

En plus des difficultés techniques qui laissent augurer une concrétisation longue et compliquée[19], le PNR s'inscrit dans un environnement juridique très attaché aux libertés.

18. COM(2017) 29 final.
19. J.-C Requier et F.-N. Buffet, « Les frontières européennes, le contrôle des flux des personnes et des marchandises en Europe et l'avenir de l'espace Schengen », Rapport d'enquête de l'AN, n° 484, 2017.

L'Union européenne construit un droit de plus en plus protecteur des données personnelles. Elle a amorcé ce travail en 1995 avec la directive 95/46. Elle l'a approfondi, en 2016, avec le règlement 2016/679. Parallèlement, le juge a fait preuve d'audace à l'occasion de plusieurs arrêts à l'occasion desquels, il s'est démarqué de l'optimisme du Conseil et de la Commission.

Dans le premier arrêt (CJUE, 8 avril 2014, *Digital Rights Ireland*, C-293/12 et C-594/12), les juges de Luxembourg ont strictement limité les conditions d'archivage des données dans le temps en annulant la directive 2006/24/CE du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE.

Dans le deuxième arrêt (CJUE, 6 octobre 2015, *Schrems,* C- 362-14), ils ont franchi une étape supplémentaire en ne reconnaissant pas les dispositions du droit américain pourtant validées par la Commission européenne (*Safe Harbour*) comme étant assez protectrices des données personnelles. Selon les juges, les mécanismes américains d'auto-certification et l'absence de recours effectif susceptible de contester la prééminence absolue des exigences de sécurité sur les exigences de respect de la vie privée obèrent la possibilité de transfert des données personnelles par des entreprises vers les États-Unis, faute d'une équivalence avec les standards de protection européens.

Dans le troisième, la CJUE a encore fait preuve d'audace en s'opposant à l'obligation imposée par les États aux fournisseurs d'accès de conserver toutes les données relatives au trafic et à la localisation. Seule une conservation ciblée et limitée au strict nécessaire est possible sous le contrôle préalable d'une autorité indépendante (21 décembre 2016, C 203/15 *Tele 2* et C698/15, *Watson*).

Dans le cas des relations avec les États-Unis, le remplacement du *Safe Harbour* par le *Privacy Shield Principles* constitue une avancée, même si l'amélioration des garanties en matière d'utilisation commerciale des données ne se retrouve pas nécessairement en matière de sécurité. Le G29 regrette d'ailleurs un manque de progrès substantiel sur la question de l'accès aux données par des autorités publiques.

La victime immédiate d'une approche rigoriste de la protection des données personnelles a été l'accord PNR entre l'Union européenne et le Canada (Avis 1/15 du 26 juillet 2017). Saisie par le Parlement européen et dans le prolongement des conclusions de l'Avocat général Mengozzi, la Cour a procédé en deux temps.

D'un côté, elle ne condamne pas le principe du transfert des données PNR. Les impératifs de sécurité justifient la collecte de données relatives à des personnes qui empruntent volontairement les transports aériens. En dépit de la rigueur de la jurisprudence *Digital Rights,* l'ingérence dans les libertés fondamentales demeure justifiée par des motifs d'intérêt général.

Par ailleurs, le juge préserve des éléments essentiels inhérents au PNR.

Ainsi, dans un contexte sécuritaire incertain, la Cour valide l'existence d'un fichier PNR. Ce type de collecte respecte les exigences de proportionnalité, ce qui constitue une inflexion par rapport à la jurisprudence précédente. À propos du Canada, la Cour n'a pas repris les arguments sur les effets potentiellement contre-productifs d'un fichier difficile à exploiter. Les juges n'ébranlent pas la logique même du dispositif. Toutefois, après avoir validé le principe d'un fichier PNR, la Cour adresse un avertissement aux États. Les incertitudes quant à la fiabilité de l'outil aggravent le risque d'atteinte aux libertés. Non seulement le ciblage des individus ne doit pas conduire à des erreurs, mais encore il représente le meilleur moyen de ne pas développer une surveillance de masse pour rien.

De même, la durée de conservation de cinq n'est pas, par principe, excessive au regard des finalités poursuivies. Là encore, le juge européen fait preuve de compréhension.

D'un autre côté, la Cour ne donne pas un blanc-seing à l'accord avec le Canada. Elle suit en grande partie l'Avocat général pour considérer que le texte, en l'état, n'est pas conforme au droit de la protection des données. La Commission a d'ailleurs admis, le 18 octobre 2017, qu'une renégociation s'impose. L'accord doit ainsi gagner en précision sur la nature des données collectées et réparties en 19 catégories. Prises isolément, elles ne poseraient pas forcément de difficulté, mais combinées entre elles, elles constituent une ingérence certaine. L'exclusion de certaines données, trop liées à la vie privée, s'imposerait alors (informations sur les repas ou liens entre les personnes par exemple).

L'accord manque, aussi, de précision en ce qui concerne les infractions transnationales qu'il aide à combattre. L'imprécision se retrouve encore à propos des conditions de conservation, et d'utilisation des données. Ces points doivent être appréciés au regard des insuffisances des articles consacrés aux conditions d'accès aux données par les services de sécurité (personnes habilitées, nombre…). Les équilibres entre liberté et sécurité s'en trouvent déstabilisés.

Si ces éléments sont *a priori* modifiables, des critiques plus fondamentales sont formulées et transposables à d'autres transferts de données PNR.

D'abord et en application de la jurisprudence *Digital Rights* et *Tele 2*, elle conteste la conservation en continu des données pour des passagers qui ne présentent plus aucun risque pour la sécurité, en particulier lorsqu'ils ont quitté le Canada. Un tri entre les passagers selon leur dangerosité s'impose par conséquent afin de rester dans le strict nécessaire.

De plus, les juges ne cessent de rappeler la nécessité pour les États qui entretiennent des relations avec l'Union européenne de démontrer l'indépendance des autorités de contrôle en application de la jurisprudence *Schrems.* À des divergences de conception sur cette indépendance, des

difficultés législatives propres aux États qui souhaiteraient améliorer leur équivalence avec l'Union européenne pourraient entraver les rapprochements.

En outre, les transferts demandés par des États tiers ont tendance à élargir excessivement les finalités de la collecte des données PNR. De futures négociations n'achopperont-elles pas sur ce sujet ?

Enfin, la question du transfert de données à des États tiers soulève la question de fond de l'équivalence par ricochet des standards de protection européens. Dans quelles conditions les autorités des destinations ayant conclu un accord avec l'Union européenne transmettent-elles les éléments recueillis ?

Dans ce contexte, la rigueur de la jurisprudence européenne pourrait aussi s'appliquer à la directive PNR, comme cela a été le cas pour la directive annulée à l'occasion de l'affaire *Digital Rights.* La nécessité et la proportionnalité constituent des angles privilégiés de contestation qui bénéficient du renfort de poids de la Charte des droits fondamentaux.

Par ricochet, les textes nationaux qui en assureraient la transposition ne seraient pas non plus à l'abri d'une contrariété avec le droit de l'Union européenne. De manière convaincante, le Défenseur des droits dans son avis n° 17-07 du 27 juillet 2017 relatif au projet de loi sur la sécurité intérieure et la lutte contre le terrorisme a fait part de ses réserves compte tenu de l'ampleur du fichage entrepris et de la possibilité de partager des données sensibles entre États membres et avec des États tiers. Cette directive contreviendrait aux articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne, et à l'article 8 de la CEDH. Force est de constater que l'avis de la CJUE du 26 juillet 2017, d'ailleurs repris par le Défenseur, conforte son analyse.

L'imprécision des infractions visées par la directive et amplifiée par une référence aux intérêts fondamentaux de la Nation dans la loi fragiliserait les deux textes. Sur ce point, le Défenseur rejoint le Conseil d'État. Ce dernier, dans son avis du 16 juin 2017 (n° 393348) relatif au projet de loi, a rappelé que la finalité d'un fichier PNR est la prévention des actes de terrorisme et des formes graves de criminalité. Les craintes augmentent avec la perspective, bien réelle, de l'utilisation des données personnelles à des fins prédictives. Cela justifierait une conservation massive des données de manière prolongée et interconnectée à d'autres fichiers, bien éloignée des exigences de proportionnalité, de nécessité et de non-discrimination.

En définitive, le respect de conditions exigeantes au regard de la protection des libertés conditionne la construction de fichiers de données personnelles dans un cadre national. Déjà à ce stade, les obstacles ne manquent pas.

Les transferts de données PNR dans un cadre international se heurtent à des difficultés encore plus grandes, à tel point qu'elles font parfois douter de

la faisabilité d'une coopération efficace. Le bien-fondé sécuritaire, lui-même discuté en l'absence d'une évaluation empirique fiable, se heurte à des principes juridiques désormais solidement établis et protégés par les juges.

Tout cela laisse planer une incertitude quant à la poursuite de cette forme de coopération, surtout lorsque se profilent des demandes de transferts par des États aux standards démocratiques contestés.