Vie du droit

L'avis de la C.J.U.E. sur l'accord PNR Union européenne-Canada : une occasion ratée de réaffirmer le principe de finalité ?

Catherine Forget(*)

- La Cour de justice de l'Union européenne a récemment examiné l'accord conclu entre le Conseil de l'Union et le Canada
- En vertu de cet accord, les données « PNR » sont systématiquement transmises à l'Agence des services frontaliers de ce pays tiers en vue d'évaluer les risques potentiels que les passagers aériens pourraient présenter pour la sécurité publique
- Dans son avis 1/15, la Cour admet le traitement systématique de données traitées à des fins policières et judiciaires par une agence migratoire d'un pays tiers

1 Contexte

Depuis 2003, toutes les compagnies aériennes sont tenues, d'après le droit canadien, de fournir à un seul destinataire, à savoir l'Agence des services frontaliers du Canada (ASFC), tant les informations préalables sur les voyageurs (API)[1] que les dossiers passagers (PNR)[2]. Contrairement à la situation intra-européenne dans laquelle les traitements de données API et PNR sont régulés par des instruments législatifs différents[3] afin de distinguer leurs finalités respectives de politique migratoire et de répression pénale, la législation canadienne appréhende les données API/PNR sans réellement scinder les accès des autorités compétentes selon l'objectif poursuivi.

Diplomatiquement, le Conseil avalisa en 2006 un premier accord entre l'Union européenne et le Canada afin de permettre le transfert de l'ensemble des données API/PNR collectées par les transporteurs aériens à destination de l'ASFC à des fins de vérification des « voyages admissibles » — donc, *a priori* dans un but de politique migratoire. Paradoxalement, le texte de l'accord affiche néanmoins explicitement que la fin poursuivie est « d'identifier les personnes risquant d'importer des articles liés au terrorisme ou aux crimes de type terroriste, à d'autres délits graves (y compris le crime organisé) ». Par conséquent, une agence d'un pays tiers dont l'objet est régi par sa loi nationale sur les douanes, la loi sur l'immigration et la protection des réfugiés se fut délivrer une bénédiction d'adéquation par l'Union européenne pour traiter systématiquement des données à des fins policières et judiciaires. Cette schizophrénie ne manqua pas d'être relevée par le Groupe Article 29[4]. La validité du premier accord et de la décision d'adéquation y relative étant venues à échéance en 2009, des négociations furent entamées en 2013 pour les renouveler.

Le 23 juin 2014, le Canada et le Conseil de l'Union européenne signaient un nouvel accord concernant cette fois uniquement le transfert des données PNR et ne régissant pas les données API. En dépit des réserves émises par le Groupe Article 29 et le Contrôleur européen de la protection des données, le texte fut soumis pour approbation au Parlement en juillet 2014. Dans l'esprit du Traité de Lisbonne, le Parlement saisit la Cour de justice de l'Union européenne d'une demande d'avis. Le Parlement s'interrogea d'une part, sur la finalité de l'accord et d'autre part, sur les garanties nécessaires pour garantir une ingérence légale et proportionnée dans les droits à la vie privée et à la protection des données à caractère personnel.

2 La compatibilité de l'accord avec le droit de l'Union

L'accord prévoit le transfert systématique et continu des données PNR collectées initialement par les transporteurs aériens à des fins commerciales auprès de l'ASFC avant l'arrivée des voyageurs sur le sol du Canada[5]. L'ingérence de l'accord dans les droits au respect de la vie privée et à la protection des données à caractère personnel ne fait aucun doute[6]. Toutefois, ces droits n'étant pas

(*) L'auteure est avocate au Barreau de Bruxelles (DWL-LAW) et chercheuse au CRIDS (UNamur). Elle peut être contactée à l'adresse suivante : catherine.forget@unamur.be. L'auteure remercie vivement Franck Dumortier pour ses relectures et conseils avisés. (1) Les données API (*advanced passenger information*) sont les données biographiques extraites du passeport notamment, le nom, le lieu de naissance, le numéro de passeport et visent à identifier les personnes dans le cadre des contrôles aux frontières. (2) Les données PNR (*passenger name record*) sont les informations initialement collectées par les transporteurs aériens à des fins commerciales. Il s'agit notamment de l'itinéraire complet, l'agence de voyage, le numéro de siège, les informations relatives aux bagages, les données d'enregistrement et d'embarquement (type de document de voyage, numéro du document, nationalité, nombre poids et identification des bagages, numéro de transport, etc.), les modes de paiement, et de manière large, des remarques générales à l'égard de chaque passager. (3) Les données API sont régulées par la directive 2004/82/CE du Conseil du 29 avril 2004 concernant l'obligation pour les transporteurs de communiquer les données relatives aux passagers, *J.O.* L 261 du 6 août 2004, p. 24 (ci-après directive 2004/82/CE) tandis que les données PNR sont régulées par la directive (UE) 2016/681 du Parlement européen et du Conseil, du 27 avril 2016, relative à l'utilisation des données des dossiers passagers (PNR) pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière, *J.O.* L 119 du 4 mai 2016, p. 132 (ci-après directive (UE) 2016/681 ou directive PNR). Celle-ci fut finalement approuvée par le Parlement européenne dans un contexte marqué par les attentats de *Charlie Hebdo* à Paris en janvier 2015 après des négociations entamées en 2007. (4) Groupe Article 29, avis 3/2004 sur le niveau de protection assuré au Canada à la transmission, par les compagnies aériennes, des dossiers passagers et d'informations anticipées sur les voyageurs, 11 février 2004, p. 7. Les avis du Groupe Article 29 sont disponibles à l'adresse suivante : http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm. (5) Article 2, b), accord PNR. (6) En effet, il a déjà été jugé que la communication de données à ca-

Vie du droit

absolus, le droit de l'Union[7] autorise les États membres à limiter la portée de ceux-ci par voie législative pour autant que la mesure respecte le contenu essentiel desdits droits (A) et que, dans le respect du principe de proportionnalité, elle soit nécessaire et réponde effectivement à un objectif d'intérêt général (B). Afin de s'assurer que l'ingérence soit limitée au « strict nécessaire », la Cour examine dans son avis 1/15[8] la clarté et la précision des règles envisagées mais aussi les exigences minimales permettant de protéger efficacement les données contre les risques d'abus (C)[9].

A. Absence d'atteinte à l'essence des droits fondamentaux

La particularité du système PNR est l'exploration systématique de données afin de « situer » des passagers sur une échelle de risque et d'ainsi permettre l'identification de criminels « éventuels ou probables »[10]. Selon le Conseil de l'Europe, un tel mécanisme ciblant des personnes « qui n'ont commis aucune infraction » ne pourrait en aucun cas viser « un but légitime » d'autant qu'il existe un risque d'erreur inévitable susceptible de mener à du profilage discriminatoire[11].

Dans son analyse, la Cour met l'accent sur la lutte contre le terrorisme et la criminalité grave constituant un but d'intérêt général susceptible de justifier des ingérences « même graves » dans les droits fondamentaux[12]. Selon celle-ci, même si ces données sont de nature à révéler des informations très précises sur la vie privée d'une personne, ces informations sont limitées à certains aspects relatifs aux voyages aériens dont le traitement est encadré par des dispositions spécifiques. Suivant ce raisonnement, la Cour aboutit à la conclusion que l'accord n'est pas de nature à porter atteinte au contenu essentiel des droits à la vie privée et de la protection des données[13].

B. Le traitement systématique justifié par la finalité poursuivie

Un élément clé en matière de protection des données à caractère personnel est la limitation du traitement à des fins « déterminées, explicites et légitimes ». Ce principe permet de concrétiser celui de la minimisation des données : il s'agit premièrement de comprendre pourquoi des données sont traitées avant de pouvoir déterminer celles qui doivent l'être afin d'éviter le risque d'en traiter davantage que nécessaire pour atteindre l'objectif poursuivi[14]. Comme le souligne le Groupe Article 29, « ces principes de protection des données sont très étroitement liés à la notion de la proportionnalité dans le contexte du respect de la vie privée »[15].

En l'occurrence, les finalités précisées par l'accord sont en principe « la lutte contre le terrorisme » et la « criminalité transnationale grave »[16]. Pourtant, dans l'examen de la proportionnalité de l'ingérence, la Cour estime que le traitement systématique des données PNR se justifie par le contexte des « contrôles aux frontières » concernant toute personne voulant se rendre au Canada[17]. Ce faisant, la Cour prend le contre-pied de l'approche retenue dans l'arrêt *Tele2* où elle avait considéré que la conservation des métadonnées par les opérateurs télécoms excédait les limites du strict nécessaire en raison de son caractère généralisé et indifférencié[18].

La détermination de la finalité du traitement PNR par la Cour contraste avec celle ayant été mise en avant lors des négociations intra-européennes au sujet de la directive PNR[19]. À cette occasion, il y fut rappelé que même si les données des passagers sont liées aux déplacements, il s'agirait essentiellement d'un outil de « renseignement en matière criminelle », plutôt que d'un « instrument de contrôle aux frontières »[20].

Dans le cas canadien, cette confusion des objectifs poursuivis a d'importantes conséquences sur l'évaluation de la proportionnalité et de la nécessité de l'accord. À cet égard, l'appréciation de la Cour est assez symptomatique puisqu'elle justifie la proportionnalité du traitement systématique des données des passagers à des fins répressives par le fait que celui-ci « facilite et accélère grandement les contrôles de sécurité et les contrôles aux frontières »[21] sans pour autant, faire le lien avec la lutte contre le terrorisme et la criminalité transfrontalière grave. En effet, la Cour se réfère sans ambages aux informations soumises par la Commission reprenant les chiffres de l'ASFC selon laquelle le traitement des données PNR a, entre autres, permis l'arrestation de 178 personnes parmi les 28 millions de voyageurs ayant emprunté un vol entre l'Union et le Canada pendant la période allant du mois d'avril 2014 au mois de mars 2015[22].

À ce propos, il est regrettable que la Cour n'ait pas rappelé l'importance d'effectuer une analyse d'impact préalable sur base d'une étude cohérente fondée sur des éléments probants et convaincants. Selon le CEPD, celle-ci peut permettre de démontrer les motifs pour lesquelles la mesure envisagée est efficace et les raisons pour lesquelles d'autres mesures moins intrusives ne permettent pas d'atteindre l'objectif poursuivi[23].

C. Une validation de l'accord sous réserve de conditions strictes

On peut saluer l'examen méthodique par la Cour des règles matérielles et procédurales régissant la portée et l'application de l'accord PNR. La Cour dresse à la lumière de sa jurisprudence antérieure[24], une liste de points devant être revus, à savoir : la cla-

ractère personnel à un tiers, telle qu'une autorité publique, constitue une ingérence au droit au respect de la vie privée, quelle que soit l'utilisation ultérieure des informations communiquées. C.E.D.H., 4 décembre 2008, *S. Marper c. Royaume-Uni*, n^{os} 30562/04 et 30566/04. **(7)** Article 52, § 1, de la Charte. **(8)** Avis 1/15 de la Cour, 26 juillet 2017, ECLI:EU:C:2017:592. **(9)** Point 141 de l'avis 1/15. **(10)** Voy. en ce sens le rapport du Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé du Conseil de l'Europe, *Passenger Name Records, data mining & data protection : the need for strong safeguards*, 15 juin 2015, T-PD(2015)11. **(11)** *Ibidem*. **(12)** Point 149 de l'avis 1/15. **(13)** Point 150 de l'avis 1/15. **(14)** Groupe Article 29, avis 01/2014 du 27 février 2014 sur l'application des notions de nécessité et de proportionnalité et la protection des données dans le secteur répressif, point 5.7. Voy. également CEPD, *Guide pour l'évaluation de la nécessité des mesures limitant le droit fondamental à la protection des données à caractère personnel*, 11 avril 2017. **(15)** *Ibidem*. **(16)** Article 3 de l'accord PNR. **(17)** Point 188 de l'avis 1/15. **(18)** C.J.U.E., 21 décembre 2016, *Tele2 Sverige AB/Post-och telestyrelsen et Secretary of State for the Home Department c. Tom Watson* e.a., aff. jointes C-203/15 et C-698/15, ECLI:EU:C:2016:970, point 105. **(19)** Directive (UE) 2016/68. **(20)** Proposition de directive du Parlement européen et du Conseil relative à l'utilisation des données des dossiers passagers pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière (COM/2011/0032 final). **(21)** Point 151 de l'avis 1/15. **(22)** Point 152 de l'avis 1/15. **(23)** CEPD, *Guide pour l'évaluation de la nécessité des mesures limitant le droit fondamental à la protection des données à caractère personnel*, 11 avril 2017, p. 20. **(24)** C.J.U.E., 8 avril 2014, *Digital Rights Ireland Ltd & Michael Seitlinger* e.a., aff. C-293/12 et C-594/12, ECLI:EU:C:2014:238; C.J.U.E., 21 décembre 2016, *Tele2 Sverige AB/Post-och telestyrelsen et Secretary of State for the Home Department c. Tom Watson* e.a., aff. jointes C-203/15 et C-698/15 ; C.J.U.E., 6 octobre 2015, *Schrems*,

rification des catégories de données transférées[25], l'exclusion du traitement des données sensibles en raison de l'absence de justification précise et solide[26], l'utilisation de modèles et critères préétablis spécifiques, fiables et non discriminatoires[27], le recoupement de données avec d'autres bases de données présentant un lien avec le but visé[28], l'exclusion des finalités vagues et générales[29], la période de conservation de données en rapport avec l'objectif poursuivi[30], l'accès aux données basé sur une demande motivée des autorités compétentes répondant à des critères objectifs[31] couplé à un contrôle préalable par une juridiction ou une entité administrative indépendante[32], la communication des données PNR à un pays tiers sous réserve d'un accord entre l'Union et ce pays tiers équivalent à l'accord envisagé ou d'une décision d'adéquation de la Commission[33], l'existence des droits des personnes concernées (accès, rectification, information individuelle)[34] mais aussi le droit à un recours effectif[35] et enfin, le contrôle du respect des règles précisés par l'accord par une autorité de contrôle indépendante[36]. Selon la Cour, sous réserve du respect de l'ensemble de ces conditions, l'accord tel que stipulé rencontre les exigences de la Charte des droits fondamentaux.

Conclusion

L'avis de la Cour était particulièrement attendu en raison des nombreuses critiques relative à la nécessité et proportionnalité d'un dispositif imposant le transfert systématique et continu des données des passagers aériens en l'absence de motifs « fondés sur des circonstances individuelles permettant de considérer que les personnes concernées pourraient présenter un risque pour la sécurité publique ». Dans *Digital Rights*, la Cour avait censuré le caractère généralisé et indifférencié d'une réglementation imposant la conservation de données par les opérateurs sans préciser quelle eut été sa position si l'accès aux données avait été encadrée par la réglementation soumise à son contrôle. Dans *Tele2*, la Cour précisa sans ambiguïté cette fois, leur caractère cumulatif et ceci, indépendamment des modalités d'accès aux données. Dans l'arrêt *Schrems*, la Cour condamna également la conservation généralisée et indifférenciée des données à caractère personnel de toutes les personnes dont les données ont été transférées depuis l'Union vers les États-Unis.

In casu, par contre, la Cour admet le caractère généralisé et indifférencié du transfert des données PNR sous réserve de conditions strictes. On peut regretter une justification peu scrupuleuse par la Cour de la finalité du traitement jetant un doute sur la réalité de l'objectif invoqué et *a fortiori* sur les raisons de l'ingérence « même grave » dans les droits fondamentaux. En effet, si la lutte contre le terrorisme et la criminalité transnationale grave peut justifier l'utilisation de technologies particulièrement invasives, la gestion des frontières s'inscrivait traditionnellement dans un tout autre examen de proportionnalité et de nécessité. En revanche, on peut saluer que la Cour ait souhaité garder l'église au milieu du village en mettant l'accent sur les conditions matérielles et procédurales d'une ingérence « grave » dans les droits des personnes aboutissant néanmoins à une certaine procéduralisation du droit au respect de la vie privée.

aff. C-362/14, ECLI:EU:C:2015:650. **(25)** Point 163 de l'avis 1/15. **(26)** Point 165 de l'avis 1/15. **(27)** Point 174 de l'avis 1/15. **(28)** Point 174 de l'avis 1/15. **(29)** Point 181 de l'avis 1/15. **(30)** Points 190 à 203 de l'avis 1/15. **(31)** Point 200 de l'avis 1/15. **(32)** Point 202 de l'avis 1/15. **(33)** Point 214 de l'avis 1/15. **(34)** Point 221 de l'avis 1/15. **(35)** Point 227 de l'avis 1/15. **(36)** Point 230 de l'avis 1/15.