Cour de justice de l'Union européenne
COMMUNIQUE DE PRESSE n° 89/16
Luxembourg, le 8 septembre 2016

Presse et Information

Conclusions de l'avocat général dans la demande d'avis 1/15

Selon l'avocat général Mengozzi, l'accord sur le transfert des données des dossiers passagers, prévu entre l'Union européenne et le Canada, ne peut pas être conclu sous sa forme actuelle

Plusieurs dispositions du projet d'accord sont en effet contraires aux droits fondamentaux de l'Union

À compter de 2010, l'Union européenne et le Canada ont négocié un accord sur le transfert et le traitement des données des dossiers passagers (accord PNR). L'accord envisagé vise à permettre le transfert des données PNR aux autorités canadiennes en vue de leur utilisation, de leur conservation et, le cas échéant, de leur transfert ultérieur, dans le but de lutter contre le terrorisme et les formes graves de criminalité transnationale. Le projet d'accord prévoit également des exigences en matière de sécurité et d'intégrité des données PNR, un masquage immédiat des données sensibles, des droits d'accès aux données, de rectification et d'effacement, la possibilité d'introduire des recours administratifs ou judiciaires et une durée de stockage des données limitée à cinq ans.

L'accord ayant été signé en 2014, le Conseil de l'Union européenne a demandé au Parlement européen de l'approuver. Ce dernier a alors décidé de saisir la Cour de justice pour savoir si l'accord envisagé était conforme au droit de l'Union garantissant le respect de la vie privée et familiale ainsi que la protection des données à caractère personnel. Le Parlement européen se demande notamment si, malgré les garanties inscrites dans l'accord, l'ingérence dans le droit fondamental à la protection des données est justifiée[1]. On notera que c'est la première fois que la Cour doit se prononcer sur la compatibilité d'un projet d'accord international avec la Charte des droits fondamentaux de l'UE.

Dans ses conclusions de ce jour, l'avocat général Paolo Mengozzi considère tout d'abord que **l'accord envisagé est compatible avec la charte des droits fondamentaux de l'UE** (notamment le droit au respect de la vie privée et familiale et le droit à la protection des données à caractère personnel) **à condition que** :

- les catégories de données PNR des passagers aériens soient libellées de manière claire et précise et que les données sensibles soient exclues du champ d'application de l'accord ;
- les infractions relevant de la définition des formes graves de criminalité transnationale soient énumérées de manière exhaustive dans l'accord ;
- l'accord identifie de manière suffisamment claire et précise l'autorité chargée du traitement des données PNR, de manière à assurer la protection et la sécurité de ces données ;

[1] Le Parlement souhaite également savoir si l'accord envisagé doit se fonder juridiquement sur les articles 82 et 87 TFUE (coopération judiciaire en matière pénale et coopération policière) ou bien sur l'article 16 TFUE (protection des données à caractère personnel). À cet égard, l'avocat général répond que l'accord doit être conclu à la fois sur la base des articles 16 et 87 TFUE. En effet, l'accord envisagé poursuit deux objectifs indissociables et d'importance égale (à savoir d'une part la lutte contre le terrorisme et la criminalité transnationale grave – qui ressort de l'article 87 TFUE – et d'autre part la protection des données à caractère personnel – qui ressort de l'article 16 TFUE).

- le nombre de personnes « ciblées » puisse être délimité dans une large mesure et de manière non discriminatoire de sorte qu'il ne concerne que les personnes sur lesquelles pèse un soupçon raisonnable de participation à une infraction terroriste ou de criminalité transnationale grave ;

- l'accord spécifie que seuls les fonctionnaires de l'autorité canadienne compétente sont habilités à accéder aux données PNR et prévoit des critères objectifs permettant d'en préciser le nombre ;

- l'accord indique les raisons objectives justifiant la nécessité de conserver toutes les données PNR des passagers pour une période maximale de cinq ans, étant entendu que, dans le cas où les données PNR devraient être conservées pendant cinq ans, celles permettant d'identifier directement un passager aérien doivent être dépersonnalisées par masquage ;

- une autorité indépendante ou une juridiction du Canada soit habilitée à contrôler, au préalable, si l'autorité canadienne compétente peut, au cas par cas, divulguer les données PNR à d'autres autorités publiques canadiennes ou étrangères (dans le cas où les données portent sur un citoyen de l'Union, une information préalable doit également être envoyée aux autorités compétentes de l'État membre concerné et/ou à la Commission) ;

- l'accord garantisse, de manière systématique, par une règle claire et précise, qu'une autorité indépendante puisse contrôler le respect de la vie privée et de la protection des données à caractère personnel des passagers dont les données PNR sont traitées ;

- l'accord précise clairement que les demandes d'accès, de rectification et d'annotation effectuées par des passagers non présents sur le territoire canadien puissent être portées devant une autorité publique indépendante.

En revanche, l'avocat général Mengozzi considère que **certaines dispositions de l'accord envisagé sont, en leur état actuel, contraires à la charte des droits fondamentaux de l'UE**. Plus précisément, il s'agit des dispositions qui

- permettent, au-delà de ce qui est strictement nécessaire, d'élargir les possibilités de traitement de données PNR, indépendamment de la finalité de sécurité publique poursuivie par l'accord, à savoir la prévention et la détection des infractions terroristes et des formes graves de criminalité transnationale ;

- prévoient le traitement, l'utilisation et la conservation par le Canada de données PNR contenant des données sensibles ;

- accordent au Canada, au-delà de ce qui est strictement nécessaire, le droit de divulguer toute information, sans que ne soit requis un lien quelconque avec la finalité de sécurité publique poursuivie par l'accord ;

- autorisent le Canada à conserver des données PNR pour une période maximale de cinq ans pour, notamment, toute action, vérification, enquête ou procédure juridictionnelle, sans que ne soit requis un lien quelconque avec la finalité de sécurité publique poursuivie par l'accord ;

- admettent que le transfert de données PNR à une autorité publique étrangère puisse être réalisé sans que l'autorité canadienne compétente, sous le contrôle d'une autorité indépendante, se soit préalablement assurée que l'autorité étrangère en question ne puisse pas elle-même ultérieurement communiquer les données à une autre entité étrangère.

De manière générale, l'avocat général parvient à ces conclusions sur la base des enseignements issus des arrêts Digital Rights Ireland[2] et Schrems[3]. Selon lui, il y a lieu de suivre la voie tracée par ces arrêts et de soumettre l'accord envisagé à un contrôle strict au regard du droit au respect de la vie privée et familiale et du droit à la protection des données à caractère personnel. Il est en effet nécessaire que, au moment où les technologies modernes permettent aux autorités publiques, au nom de la lutte contre le terrorisme et la criminalité transnationale grave, de développer des méthodes extrêmement sophistiquées de surveillance de la vie privée des individus et d'analyse de leurs données à caractère personnel, la Cour s'assure que les mesures projetées, fussent-elles sous la forme d'accords internationaux envisagés, reflètent une pondération équilibrée entre le souci légitime de préserver la sécurité publique et celui, non moins fondamental, à ce que toute personne puisse jouir d'un niveau élevé de protection de sa vie privée et de ses propres données.

RAPPEL: Les conclusions de l'avocat général ne lient pas la Cour de justice. La mission des avocats généraux consiste à proposer à la Cour, en toute indépendance, une solution juridique dans l'affaire dont ils sont chargés. Les juges de la Cour commencent, à présent, à délibérer dans cette affaire. L'arrêt sera rendu à une date ultérieure.

RAPPEL: Un État membre, le Parlement européen, le Conseil ou la Commission peut recueillir l'avis de la Cour de justice sur la compatibilité d'un accord envisagé avec les traités. En cas d'avis négatif de la Cour, l'accord envisagé ne peut entrer en vigueur, sauf modification de celui-ci ou révision des traités.

Contact presse: Gilles Despeux ☎ (+352) 4303 3205

---

[2] Arrêt de la Cour du 8 avril 2014, *Digital Rights Ireland e.a.* (C-293/12 et C-594/12, voir CP n° 54/14 : la Cour de justice déclare la directive sur la conservation des données invalide).

[3] Arrêt de la Cour du 6 octobre 2015, *Schrems* (C-362/14, voir CP n° 117/15 : la Cour déclare invalide la décision de la Commission constatant que les États-Unis assurent un niveau de protection adéquat aux données à caractère personnel transférées).