Les limites de la récolte de données personnelles des passagers aériens

Lauris Loat, le 22 août 2022

La Cour de justice de l'Union européenne (CJUE) a dû se pencher sur les limites autorisées par le droit de l'Union à ce qu'une législation nationale prévoie le transfert et le traitement des données Passenger Name Record (PNR) des vols au sein de l'UE, ainsi que de tous transports effectués par d'autres moyens en son sein. Elle a conclu à une limitation strict de cette possibilité, afin d'éviter que les données des passagers effectuant des vols intra-européens soient constamment collectées.

Arrêt CJUE C-817/19 du 21 juin 2022

La Directive (UE) 2016/681 du Parlement européen et du Conseil, du 27 avril 2016, relative à l'utilisation des données des dossiers passagers (plus connu sous l'acronyme anglais PNR pour *Passenger Name Record*) 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 (Directive PNR), impose aux compagnies aériennes le traitement systématique d'un nombre important de données PNR des vols extra-UE, à l'entrée et à la sortie de l'Union, dans un but de lutte contre le terrorisme et les formes graves de criminalité. L'art. 2 de cette directive octroie aux États membres la possibilité d'appliquer cette directive également aux vols intra-UE.

En Belgique, les autorités ont adopté une loi du 25 décembre 2016, qui transposait en droit belge à la fois la Directive PNR, la Directive API (qui concerne l'obligation pour les transporteurs de communiquer les données relatives aux passagers) et la Directive 2010/65 (qui a pour objet les formalités déclaratives applicables aux navires à l'entrée et/ou à la sortie des ports des États membres). La loi du 25 décembre 2016 utilise notamment la possibilité d'étendre la collecte des données PNR à l'ensemble des passagers de vols intra-UE, ainsi qu'à conserver ces données de manière générale pour une durée de cinq ans.

En juillet 2017, la Ligue des droits humains (LDH) a saisi la Cour constitutionnelle belge d'un recours en annulation contre la loi du 25 décembre 2016 précitée. La LDH soutenait que la loi méconnaissait le droit au respect de la vie privée et à la protection des données à caractère personnel. Elle critiquait notamment le caractère général de la collecte, du transfert et du trai-

tement de ces données. Par ailleurs, cette loi limiterait également la libre circulation des personnes au sein de l'UE, en ce sens qu'elle rétablit indirectement des contrôles aux frontières en étendant le système PNR aux vols intra-UE.

Suite à cette saisine, la Cour constitutionnelle belge a posé à la CJUE dix questions préjudicielles portant sur la validité de la Directive PNR, ainsi que sur la compatibilité de la loi belge avec le droit de l'UE.

Dans son arrêt du 21 juin 2022, la CJUE a considéré que la Directive PNR était pleinement valide et qu'elle entrait en conflit avec la loi belge du 25 décembre 2016 sur certains points.

La CJUE a tout d'abord rappelé qu'un acte de l'Union doit être interprété d'une manière qui ne remette pas en cause sa validité et en conformité avec l'ensemble du droit primaire, précisément avec les dispositions de la Charte des droits fondamentaux de l'Union européenne (la Charte).

Dans son arrêt, la CJUE a retenu que la Directive PNR comportait des ingérences d'une gravité certaine dans les droits garantis par la Charte. Elle a ainsi conclu que le transfert, le traitement et la conservation des données PNR prévus par la Directive PNR sont limités au strict nécessaire aux fins de la lutte contre les infractions terroristes et les formes graves de criminalité, à condition que les pouvoirs prévus par la directive fassent l'objet d'une interprétation restrictive.

Pour ce faire, l'application de la Directive PNR ne saurait notamment s'étendre à d'autres domaines que les infractions terroristes et aux formes graves de criminalité ayant un lien objectif avec le transport aérien de passagers.

Ainsi, l'extension possible de la Directive PNR à tout ou partie des vols intra-UE, qui est laissée aux États membres, doit être limitée. Pour que l'extension soit valable, elle doit pouvoir faire l'objet d'un contrôle effectif par une juridiction ou par une entité administrative indépendante, dont la décision est dotée d'un effet contraignant, et à des conditions restrictives.

Qui plus est, l'évaluation des données PNR par l'unité d'information passagers (UIT) ne peut confronter ces données qu'aux seules bases de données concernant les personnes ou les objets recherchés faisant l'objet d'un signalement.

Ensuite de cela, la communication et l'évaluation postérieures des données PNR, soit après l'arrivée ou le départ de la personne concernée, ne peuvent être effectuées que sur la base

de circonstances nouvelles et d'éléments objectifs qui, soit sont de nature à fonder un soupçon raisonnable d'implication de cette personne dans des formes graves de criminalité présentant un lien objectif avec le transport aérien des passagers, soit permettent de considérer que ces données pourraient, dans un cas concret, apporter une contribution effective à la lutte contre des infractions terroristes présentant un tel lien.

Dans un deuxième temps, la CJUE a considéré que la Directive PNR, en rapport avec la Charte, s'oppose à une législation nationale qui autoriserait le traitement des données PNR recueillies conformément à la Directive, mais à des fins autres que celles visant des infractions terroristes et des formes graves de criminalité présentant un lien objectif avec le transport aérien.

Si l'on en vient à la question du délai de conservation, la CJUE a jugé que l'art. 12 de la Directive PNR, en rapport avec la Charte, s'oppose à une législation nationale qui prévoit une durée générale de conservation de ces données de cinq ans, applicable indifféremment à tous les passagers aériens. La Directive PNR prévoit pour sa part une période de conservation initiale de six mois. Passé ce délai, il n'est pas possible de conserver des données PNR en ce qui concerne les passagers aériens pour lesquels ni l'évaluation préalable, ni les éventuelles vérifications effectuées au cours de la période de conservation initiale de six mois, ni aucune autre circonstance, n'ont révélé l'existence d'éléments objectifs de nature à établir un risque en matière d'infractions terroristes ou de formes graves de criminalité. À l'inverse, la CJUE a estimé que la conservation des données PNR de l'ensemble des passagers aériens soumis au système instauré par cette directive au cours de la période initiale de six mois est proportionnée.

En dernier lieu, la CJUE a considéré que le droit de l'UE s'oppose à ce qu'une législation nationale prévoie, en l'absence de menace terroriste réelle et actuelle ou prévisible, un système de transfert par les transporteurs aériens et les opérateurs de voyage, ainsi que de traitement par les autorités compétentes, des données PNR de l'ensemble des vols intra-UE.

La CJUE a ainsi clarifié les limites qu'une loi nationale ne doit pas dépasser dans le cadre de la transposition de la Directive PNR, et particulièrement restreint l'application aux vols intra-UE.

Parallèle avec le droit suisse

En Suisse, les autorités fédérales ont mis en consultation le 13 avril 2022 l'avant-projet de loi sur les données relatives aux passagers aériens (AP-LDPa). La genèse de cette loi est la

même que la Directive PNR, à savoir que les entreprises de transport aérien récoltent des données PNR.

À ce jour, les entreprises de transport aérien actives en Suisse ont l'obligation de récolter ces données sur la base de la Directive PNR pour tout vol qui est opéré à destination d'un pays qui utilise le PNR, soit 62 pays, dont ceux de l'UE, les États-Unis et le Canada. Ainsi, ces informations doivent être transmises par les compagnies aériennes au pays de destination. Mais, en l'absence de base légale, la Suisse ne peut pas traiter les données collectées.

Selon le Conseil fédéral, les données PNR permettront d'identifier avant le départ, ou à l'arrivée d'un vol à destination de la Suisse, des terroristes ou des personnes ayant commis une infraction pénale grave, permettant alors à la police de prendre les mesures nécessaires. Ces données permettront également de recevoir des informations relatives aux déplacements d'une personne dans le cadre d'une enquête de police. Qui plus est, il serait alors possible de détecter des organisations et des réseaux criminels, ainsi que d'identifier précisément des suspects, ou encore des victimes potentielles de la traite d'êtres humains.

Selon l'AP-LDPa, c'est l'Unité d'information des passagers, composée de collaborateurs de la Confédération et de personnel détaché par les cantons, qui pourra accéder aux données pour accomplir les tâches de traitement des données relatives aux passagers aériens issues de Suisse et de l'étranger, et pour transmettre les résultats obtenus aux autorités compétentes.

L'AP-LDPa ne compilera pas de données sensibles, telles que les convictions religieuses qui pourraient être déduites du choix d'un repas spécifique. Qui plus est, les données relatives aux passagers aériens seront automatiquement pseudonymisées après six mois, ce qui a pour conséquence que les informations personnelles identifiables, telles que le nom, les coordonnées ou la date de naissance ne seront plus visibles. La seule possibilité de lever la pseudonymisation sera, en cas de soupçon concret, sur décision du Tribunal administratif fédéral. Finalement, les données PNR seront entièrement effacées après cinq ans.

L'art. 6 AP-LDPa prévoit que les données relatives aux passagers aériens peuvent être traitées uniquement à des fins de prévention, de détection, d'enquête et de poursuite en matière d'infractions terroristes et autres infractions pénales graves. L'alinéa 3 de cet article précise ce que sont des infractions pénales graves, à savoir :

1. les infractions visées à l'annexe 1 LEIS (loi sur l'échange d'informations Schengen) qui sont passibles d'une peine privative de liberté de plus de trois ans et qui peuvent être attribuées à une catégorie d'infraction énoncée à l'annexe 2 de la présente loi ;

2. les infractions relevant de la compétence de l'Office fédéral de la douane et de la sécurité des frontières en matière de poursuite pénale et qui sont passibles d'une peine privative de liberté d'au moins trois ans.

On constate que l'AP-LDPa va plus loin que la Directive PNR de l'UE, qui se cantonne à traiter des données en cas de menace terroriste et d'infraction pénale grave uniquement liée au trafic aérien. Or, l'AP-LDPa souhaite également traiter les données PNR pour toutes infractions pénales graves listées ci-dessus, ce qui a une incidence bien plus importante que le seul trafic aérien.

Qui plus est, la Suisse n'étant pas partie à l'UE, les données PNR récoltées concerneront tous les vols à destination de l'étranger depuis la Suisse, et inversement. Ceci a ainsi le même impact que l'application de la Directive PNR aux vols intra-europe, et risque de réinstaurer une forme de contrôle aux frontières abolie à ce jour dans l'espace Schengen, tel que l'a soulevé la LDH dans son recours contre la loi belge.

Il ressort de cela que, quand bien même la Suisse n'est pas soumise au droit européen, ni aux décisions de la CJUE, il serait cohérent d'avoir un droit homogène avec la Directive PNR, et ne pas chercher à utiliser ces données à des fins plus étendues que le terrorisme, ou des infractions pénales liées au trafic aérien. Il en va de même en ce qui concerne la durée de conservation des données prévue par l'AP-LDPa qui impactera plus lourdement les passagers qu'en application de la Directive PNR.

Proposition de citation : Lauris Loat, Les limites de la récolte de données personnelles des passagers aériens, 22 août 2022 *in* www.swissprivacy.law/166