12 octobre 2023

Cour constitutionnelle

COMMUNIQUÉ DE PRESSE
ARRÊT 131/2023

La Cour annule partiellement la loi qui impose la communication des données des passagers, et juge cette loi pour le reste conforme à la Constitution et au droit européen pour autant qu'elle soit interprétée d'une certaine manière

La Cour a posé dix questions préjudicielles à la Cour de justice de l'Union européenne (CJUE) dans le cadre de l'examen du recours en annulation introduit par la Ligue des droits humains contre la loi qui impose la communication des données des passagers.
La CJUE a validé dans son principe le système PNR (*Passenger Name Record*), sur lequel la loi attaquée repose, moyennant plusieurs réserves d'interprétation.
À la suite de cet arrêt de la CJUE, la Cour juge qu'il est justifié que le système PNR s'applique à tous les passagers, mais que le traitement des données PNR n'est possible que pour la lutte contre le terrorisme et les formes graves de criminalité, en lien avec le transport concerné. La Cour valide plusieurs mesures attaquées (création de la banque de données, *pre-screening*, durée de conservation des données), moyennant des réserves d'interprétation. La Cour annule d'autres mesures, telles que la possibilité pour le procureur du Roi et les services de renseignement et de sécurité d'accéder aux données. Dans l'attente d'une intervention du législateur, l'Autorité de protection de données est compétente pour autoriser un tel accès. La Cour annule aussi les dispositions qui organisent le traitement des données API (*Advanced Passenger Information*) dans une banque de données unique avec les données PNR.

1. Contexte de l'affaire

La loi du 25 décembre 2016 « relative au traitement des données des passagers » impose aux transporteurs et aux opérateurs de voyage de communiquer les données des passagers (**données PNR**). Ces données sont enregistrées dans une banque de données gérée par l'Unité d'information des passagers (UIP), un organe au sein du SPF Intérieur. Cette loi transpose la directive 2016/681/UE « PNR » (*Passenger Name Record*). En Belgique, le système PNR s'applique non seulement au transport aérien (comme le prévoit la directive PNR), mais aussi au transport ferroviaire et par bus. La loi précitée transpose également la directive 2004/82/CE « API » (*Advanced Passenger Information*), qui impose aux compagnies aériennes de transmettre certaines données, notamment pour lutter contre l'immigration illégale et améliorer le contrôle aux frontières.

L'ASBL « Ligue des droits humains » demande l'annulation de la loi du 25 décembre 2016. Par son arrêt n° 135/2019, la Cour a validé plusieurs mesures attaquées. Elle a également posé dix questions préjudicielles à la Cour de justice de l'Union européenne (CJUE), notamment sur l'interprétation et la validité des directives PNR et API.

La CJUE a répondu à ces questions par son arrêt du 21 juin 2022 (C-817/19). La CJUE y valide le système PNR dans son principe, mais assortit la directive PNR de plusieurs réserves d'interprétation en vue d'assurer sa conformité à la Charte des droits fondamentaux de l'UE.

2. Examen par la Cour

Dans le présent arrêt, la Cour examine les critiques de la partie requérante qu'elle n'a pas examinées dans l'arrêt n° 135/2019, en tenant compte des réponses de la CJUE.

2.1. Le droit au respect de la vie privée et à la protection des données à caractère personnel

Selon la partie requérante, plusieurs aspects de la loi attaquée violent le droit au respect de la vie privée et à la protection des données à caractère personnel.

2.1.1. Les données visées (B.24-B.34)

Selon la partie requérante, la collecte d'un grand nombre de données de passagers est disproportionnée. En outre, ces données pourraient révéler des données sensibles.

La Cour relève que la loi du 25 décembre 2016 poursuit un **but d'intérêt général, qui est d'assurer la sécurité publique**. Ensuite, les données collectées sont identifiées clairement et les opérateurs et transporteurs en disposent en principe déjà ; elles doivent être liées à un voyage particulier et être limitées à la lutte contre les infractions terroristes et les formes graves de criminalité ; enfin, il est garanti que des données sensibles ne soient pas collectées ni conservées. À l'instar de la CJUE, la Cour précise cependant que **certaines données** (adresse et coordonnées, informations sur les modes de paiement, informations relatives aux mineurs non accompagnés) **doivent être interprétées restrictivement**. La Cour admet en outre la collecte des données relatives au numéro de siège et aux bagages. Moyennant ces interprétations, la Cour conclut que la critique de la partie requérante n'est pas fondée.

2.1.2. La notion de passager (B.35-B.41)

La partie requérante critique le caractère large de la notion de « passager », qui donne lieu à un traitement automatisé systématique, non ciblé, des données de tous les passagers.

La Cour relève que la collecte, le transfert et le traitement des données PNR s'applique à tout passager, indépendamment de la question de savoir s'il a commis une infraction ou s'il est susceptible d'en commettre, et indépendamment d'un franchissement des frontières extérieures de l'UE. La CJUE a jugé que **l'extension du système PNR** (applicable en principe seulement aux vols franchissant les frontières extérieures de l'UE) **aux vols intra-UE est admissible pour autant qu'il y ait une menace actuelle, réelle et prévisible, évaluée périodiquement par un organe indépendant**. Sur cette base, la Cour juge que la menace terroriste était réelle et actuelle lors de l'adoption de la loi et qu'elle l'est toujours aujourd'hui, compte tenu de la situation géographique centrale de la Belgique et des nombreuses institutions européennes et internationales qu'elle abrite. La Cour précise que **le législateur devra évaluer périodiquement la loi sur la base de l'évaluation de la menace par l'OCAM**, la première évaluation devant avoir lieu au plus tard dans trois ans. Compte tenu notamment de cette obligation de réexamen, la critique n'est pas fondée.

2.1.3. Les finalités du traitement PNR (B.42-B.56)

La partie requérante soutient que les finalités du traitement des données PNR excèdent les limites du « strict nécessaire ».

La CJUE a admis la collecte et le traitement des données PNR mais **uniquement pour la lutte contre le terrorisme et les formes graves de criminalité et uniquement s'il y a un lien objectif, à tout le moins indirect, avec le transport concerné**.

La Cour juge que certaines finalités de traitement concernent des formes graves d'infraction, qu'elles sont définies clairement et qu'elles sont limitées au strict nécessaire. La Cour relève que d'autres finalités s'ajoutent à celles qui sont prévues par la directive PNR :

- La **finalité de « prévention des troubles graves à la sécurité publique dans le cadre de la radicalisation violente »** est admissible pour autant qu'elle soit interprétée comme strictement limitée à la lutte contre le terrorisme et la criminalité grave et comme présentant un lien objectif, à tout le moins indirect, avec le transport concerné.

- En ce qui concerne la **finalité liée au « suivi des activités visées par les services de renseignement et de sécurité »**, la Cour relève que les missions de ces services ne se limitent pas à la prévention des infractions terroristes et de la criminalité grave et que cette finalité ne présente pas un lien objectif, fût-ce indirect, avec le transport de passagers. Cette finalité **dépasse les limites du strict nécessaire et doit être annulée**.

- Par son arrêt n° 135/2019, la Cour a admis que les données PNR soient traités **en vue d'améliorer les contrôles de personnes aux frontières extérieures et de lutter contre l'immigration illégale**. La Cour constate que la CJUE semble l'exclure. La Cour juge qu'elle ne peut cependant pas revenir sur ce qu'elle a définitivement jugé. Le législateur doit donc harmoniser la loi attaquée sur ce point avec l'arrêt de la CJUE. La Cour précise cependant qu'elle examine les critiques dirigées contre le traitement des données API plus loin (ci-dessous, point 2.2).

2.1.4. La gestion de la banque de données des passagers et le traitement des données dans le cadre de l'évaluation préalable des passagers et des recherches ponctuelles (B.57-B.70)

La partie requérante critique la création de la banque de données des passagers et sa gestion par l'UIP. Elle critique également le lien entre les bases de données et la méthode de *pre-screening*, ainsi que la possibilité pour les membres détachés des services compétents de se prononcer sur une requête d'accès individuelle dans le cadre de recherches ponctuelles.

La Cour relève que la CJUE conditionne la validité de la directive PNR au respect de différentes garanties. Il faut dès lors interpréter la loi du 25 décembre 2016 comme intégrant ces garanties, et l'UIP et les autorités compétentes devront veiller au respect de ces garanties.

Selon la Cour, **la création d'une banque de données** des passagers, sous la responsabilité de l'UIP, est un élément essentiel du système PNR. Les agents détachés de la sûreté de l'Etat, des services de police, de renseignement et de sécurité exercent leurs fonctions sous la seule autorité du fonctionnaire dirigeant de l'UIP. L'UIP offre ainsi des garanties d'expertise et d'indépendance et dispose des compétences requises pour poursuivre les seules finalités visées dans la directive PNR. La Cour conclut que la mesure n'est pas disproportionnée.

En ce qui concerne **l'évaluation préalable du risque représenté par les passagers (*pre-screening*)**, la Cour précise que les données PNR ne peuvent être croisées, techniquement, qu'avec les bases de données concernant les personnes ou les objets recherchés ou faisant

l'objet d'un signalement, que ces bases de données doivent être exploitées par les autorités compétentes de manière non discriminatoire, et seulement en matière de terrorisme et de criminalité grave en lien avec le transport des passagers. L'élaboration des critères préétablis est soumise aux mêmes limitations. La Cour précise que l'UIP ne peut pas utiliser des technologies d'intelligence artificielle dans le cadre de systèmes d'autoapprentissage (*machine learning*), susceptibles de modifier le processus d'évaluation sans intervention et contrôle humains. Enfin, en cas de concordance positive (*hit*), le **réexamen** individuel par l'UIP dans les 24 heures doit être effectué selon des règles claires et précises garantissant une pratique administrative cohérente qui assure le respect des règles qui précèdent.

La Cour précise enfin que les personnes concernées doivent être suffisamment informées, pour pouvoir décider d'introduire ou non un recours juridictionnel.

En ce qui concerne **les recherches ponctuelles**, qui permettent au procureur du Roi et aux services de renseignement et de sécurité d'accéder aux données des passagers, la Cour juge que les membres de l'UIP présentent des garanties d'indépendance suffisantes pour répondre aux demandes d'accès. La Cour annule toutefois la faculté pour les services de renseignement et de sécurité de faire des recherches ponctuelles pour le suivi de leurs activités, dès lors que cette finalité dépasse les exigences du strict nécessaire, comme il est dit au point 2.1.3.

La CJUE a jugé que la communication des données PNR ne peut être décidée que sur la base de circonstances nouvelles et d'éléments objectifs en vue de lutter contre le terrorisme et la criminalité grave, en lien avec le transport des passagers. Selon la Cour, la loi du 25 décembre 2016 doit être interprétée de la même manière. La CJUE a également jugé que la communication des données PNR doit être autorisée par une juridiction ou par une autorité administrative indépendante autre que l'UIP, sur demande motivée des autorités compétentes. La Cour juge que ni le procureur du Roi ni le fonctionnaire des douanes ne sont des autorités nationales indépendantes. La loi doit donc être annulée dans la mesure où elle ne désigne pas l'organe indépendant chargé d'un tel contrôle préalable. Dans l'attente de la détermination de cet organe indépendant par le législateur, l'Autorité de protection des données peut exercer cette fonction. La disposition concernée peut donc continuer à être appliquée dans cette interprétation.

2.1.5. La durée de conservation des données PNR (B.71-B.75)

La partie requérante soutient qu'il est excessif de conserver les données pendant cinq ans.

Selon la CJUE, il est justifié que les données PNR de l'ensemble des passagers soient conservées au cours d'une période initiale de six mois, mais pas au-delà de cette période. Au-delà de cette période de six mois, seules peuvent être conservées les données relatives aux personnes présentant un risque terroriste ou criminel grave, en lien avec le voyage effectué.

Selon la Cour, la disposition attaquée peut être interprétée en ce sens qu'**après six mois, seules sont conservées, pendant cinq ans, les données des personnes présentant un risque, tandis que les autres données doivent être détruites**. Moyennant cette interprétation, la Cour rejette la critique de la partie requérante.

2.2. La libre circulation des personnes au sein de l'Union européenne (B.76-B.79)

La partie requérante estime qu'en étendant le système PNR aux vols intra-UE, les dispositions attaquées rétablissent indirectement des contrôles aux frontières qui seraient contraires à la liberté de circulation des personnes garantie en droit européen.

Comme il est dit au point 2.1.2, compte tenu de l'arrêt de la CJUE, la Cour juge que la réalité de la menace terroriste justifie l'application du système PNR à différents moyens de transport à l'intérieur des frontières de l'Union. La Cour considère que, pour des motifs similaires, la restriction à la liberté de circulation qu'emporterait la loi du 25 décembre 2016 est justifiée.

Selon la CJUE, la possibilité de reprendre, parmi les données PNR, les données API ne change rien au fait que la directive API ne s'applique pas aux vols intra-UE. Le traitement des données API ne peut concerner que des passagers qui franchissent les frontières extérieures de l'Union. Selon la CJUE, vu le caractère exhaustif des finalités de la directive PNR, les données PNR ne peuvent pas être conservées dans une base de données unique pouvant être consultée pour la poursuite tant de ces finalités que d'autres finalités.

La Cour conclut que, vu l'existence d'une base de données unique contenant tant les données PNR que les données API, il n'est pas possible d'interpréter sur ce point la loi du 25 décembre 2016 conformément au droit de l'Union. **La Cour annule donc les dispositions qui autorisent le traitement des données API dans le cadre du système PNR pour des vols intra-UE**, dès lors qu'elles visent des vols intra-UE. La Cour annule également la finalité liée à l'amélioration des contrôles de personnes aux frontières extérieures et à la lutte contre l'immigration illégale, qui est indissociable des dispositions annulées. Il appartient au législateur d'organiser la collecte des données API dans une banque de données distincte de la banque de données PNR et selon les conditions qui respectent la directive API.

3. Conclusion

La Cour annule plusieurs dispositions, comme indiqué plus haut. Elle précise que ces annulations ont pour effet que les traitements des données qui ont été effectués sur la base des finalités annulées ou les communications des données effectuées sans contrôle préalable doivent être considérés comme illégaux mais que cette annulation partielle n'affecte pas les autres traitements des données des passagers. La Cour rejette le recours pour le surplus, moyennant les réserves d'interprétation mentionnées.

Il ressort de l'arrêt de la CJUE que le maintien provisoire des effets des dispositions annulées n'est pas possible. La Cour précise qu'il appartient au juge pénal compétent de statuer, le cas échéant, sur l'admissibilité des preuves qui ont été recueillies lors de la mise en œuvre des dispositions annulées, conformément aux règles de procédure pénale applicables et à la lumière des précisions apportées par la CJUE.

Contact presse : Martin Vrancken | 02/500.12.87 | Romain Vanderbeck | 02/500.13.28

Suivez la Cour via Twitter @ConstCourtBE