Proposition de résolution sur la proposition de décision-cadre relative à l'utilisation de données des dossiers passagers (Passenger Name Record - PNR) à des fins répressives (E 3697)

Date de mise en ligne : dimanche 8 mars 2009

À plusieurs reprises, la commission des affaires européennes a émis de très fortes réserves sur les accords passés entre l'Union européenne et les États-Unis pour le transfert de données concernant les passagers des vols aériens. Elle a souligné les graves insuffisances de ces accords au regard de la protection de la vie privée et des libertés fondamentales.

Le Sénat doit exercer une même vigilance sur la proposition présentée en novembre 2007 par la Commission européenne de mettre en place un système PNR au niveau européen.

I/ Quel est l'objet de la proposition de décision-cadre ?

La proposition de décision-cadre tend à faire obligation aux transporteurs aériens assurant des vols vers le territoire d'au moins un État membre ou à partir de celui-ci, de transmettre aux autorités compétentes les renseignements relatifs aux passagers aux fins de prévenir et de combattre les infractions terroristes et la criminalité organisée. Ne sont visés que les vols en provenance de pays tiers vers l'Union européenne et de l'Union européenne vers les pays tiers. En revanche, les vols intracommunautaires ne seront pas concernés.

La Commission européenne fait valoir la valeur ajoutée qu'apporterait un système PNR en réduisant le risque de voir se produire sur le territoire de l'Union européenne des attentats terroristes, des infractions graves ou une criminalité transnationale organisée. En outre, une approche européenne permettrait d'harmoniser les différents aspects des systèmes d'échange et d'utilisation des données PNR et les garanties pour le respect de la vie privée.

Cette proposition viendrait compléter une directive du 29 avril 2004 qui fait obligation aux transporteurs aériens de communiquer les données relatives aux passagers, afin de lutter contre l'immigration clandestine et d'améliorer les contrôles aux frontières. Ces données - dites données API (« Advance passenger information ») - permettent d'identifier une personne préalablement à son arrivée dans un pays.

Contrairement à ces données API qui répondent à un objectif d'identification, les données PNR (« Passenger Name Record »), doivent permettre de procéder à une évaluation des risques présentés par certaines personnes, de recueillir des informations et d'établir des liens entre des personnes connues et d'autres qui ne le sont pas. Par exemple, elles peuvent permettre de constater qu'une carte de crédit utilisée par une personne est identique à celle utilisée par une personne connue des services répressifs.

Les données PNR comprennent en effet des données telles que les numéros de téléphone, l'agence de voyage, le numéro de la carte de crédit, l'historique des modifications du plan de vol, les préférences de siège et d'autres informations. En général, seules figurent les données PNR fournies par un passager sur base volontaire au moment de la réservation ou lors de l'embarquement. Il convient de noter que les transporteurs aériens enregistrent déjà les données des dossiers passagers pour leur propre usage commercial.

Plusieurs pays se sont dotés d'un système de données PNR, en particulier les États-Unis, le Canada et l'Australie. Au sein de l'Union européenne, le Royaume-Uni est le seul État membre à avoir un système PNR complet dans le cadre du programme e-Borders. Des législations ont été adoptées en France et au Danemark. En France, la loi du 23 janvier 2006 relative à la lutte contre le terrorisme a autorisé la collecte et le traitement de données passagers, recueillies à l'occasion de déplacements internationaux en provenance ou à destination d'État n'appartenant pas à l'Union européenne. Mais sa mise en oeuvre ne concerne actuellement que les seules données API.

II/ Quel est l'état d'avancement des discussions en cours ?

La proposition de la Commission européenne a reçu un soutien de principe à l'occasion de la réunion informelle des ministres de la justice et de l'intérieur en janvier 2008. En juillet 2008, le Conseil a confirmé sa volonté de faire progresser ce dossier et donné son accord à la présidence française sur une méthode de travail destinée à approfondir une liste de questions et fondée sur une concertation avec les principales parties prenantes.

En octobre 2008, le Conseil a discuté, sans parvenir à ce stade à des conclusions définitives, quelques caractéristiques d'un futur système de collecte de données personnelles (PNR). Ces données, qui seraient transmises aux autorités publiques avant l'embarquement des passagers, alimenteraient l'analyse de la menace terroriste et criminelle, et pourraient être utilisées dans le cadre d'enquêtes particulières. Un consensus se dessinerait autour de la création d'un système décentralisé, avec une montée en charge progressive accompagnée d'un dispositif d'évaluation et de révision. Serait couvert par ce système le transport aérien de voyageurs reliant l'Union européenne aux États tiers.

Tant le contrôleur européen pour la protection des données (avis du 1er mai 2008), que l'agence des droits fondamentaux (avis du 3 décembre 2008) et le groupe de l'article 29 sur la protection des données (avis du 5 décembre 2007) ont en revanche émis des réserves sur la nécessité d'un tel système. Dans une résolution adoptée le 20 novembre 2008, le Parlement européen a reconnu que la collecte et le traitement de données pouvaient être un outil utile pour lutter contre le terrorisme. Mais il a exprimé de fortes réserves sur la nécessité et la valeur ajoutée de la proposition.

Conformément au mandat donné par le Conseil le 25 juillet, un rapport de la présidence française a fait un bilan de la concertation qui a été conduite. Les transporteurs aériens ont souligné que, dans un contexte où les exigences de transmission diffèrent d'un État à l'autre, ils aspiraient à trouver l'appui de l'Union européenne pour oeuvrer vers une harmonisation la plus large possible afin de limiter au strict nécessaire la charge financière et le poids des responsabilités légales qui leur sont imposées. Le coordinateur anti-terroriste a fait état de l'expérience des services de lutte contre le terrorisme qui témoignent de l'utilité des PNR en raison, d'une part, de la vulnérabilité particulière des terroristes lors du franchissement des frontières et, d'autre part, du potentiel important et tout à fait spécifique offert par le PNR. Les autorités policières et douanières ont considéré que le PNR était un moyen précieux de combattre les nombreuses formes de criminalité organisée. Selon la douane française, 60 à 80% des produits stupéfiants annuellement saisis dans les aéroports internationaux de Paris (soit environ 2 tonnes par an) sont directement à mettre au compte des PNR. Le rapport de la présidence française indique que ces travaux entre les États membres établiraient l'utilité d'un PNR européen qui offre un potentiel propre, complémentaire et non redondant avec d'autres outils de contrôles existants. La constitution d'un PNR européen constituerait une alternative au développement progressif de solutions nationales divergentes et répondrait en outre à l'intérêt des compagnies aériennes.

Sur la base du rapport de la présidence française faisant un bilan des travaux thématiques, le Conseil a conclu, lors de sa réunion de novembre 2008, que la méthode suivie avait débouché sur une perception de plus en plus précise de la portée utile et des caractéristiques essentielles d'un système PNR européen.

III/ Quelles sont les principales difficultés soulevées par cette proposition ?

Si nous devons prendre acte des discussions en cours, nous devons aussi faire preuve d'une très grande vigilance sur le respect de la vie privée et les garanties des droits fondamentaux. À cet égard, les observations du contrôleur européen de la protection des données, de l'Agence des droits fondamentaux de l'Union européenne et du groupe de l'article 29, qui regroupe les autorités de contrôle sur la protection des données, soulignant les lacunes de la proposition en matière de sécurité juridique et de protection des données, méritent une grande attention. À titre

principal, plusieurs difficultés peuvent être identifiées.

1/ Les finalités du système

La proposition initiale de la Commission européenne retient pour finalités la prévention et la lutte contre le terrorisme et la criminalité organisée. Dans le cadre des discussions en cours au Conseil, les finalités retenues seraient la prévention, la détection, l'instruction, la poursuite et la répression du terrorisme ainsi qu'un ensemble d'infractions graves à définir par référence à la liste de 32 infractions, établie dans la décision-cadre relative au mandat d'arrêt européen.

Le Sénat devrait marquer que ces finalités doivent être exclusives de tout autre finalité. En particulier, un système PNR ne peut avoir vocation à traiter des questions d'immigration, lesquelles relèvent d'autres dispositifs tels que le Système d'Information Schengen (SIS) ou le Système d'Information sur les Visas (VIS). En outre, sur le plan juridique, la lutte contre l'immigration illégale relève du premier pilier communautaire et ne pourrait être traitée dans le cadre d'un instrument du troisième pilier tel que celui qui est proposé.

Si la notion d'infractions graves peut permettre de couvrir un champ plus large que celle de criminalité organisée, qui répond à une définition juridique précise, encore faut-il que la pertinence de l'utilisation des données PNR pour poursuivre ou réprimer des infractions prévues pour le mandat d'arrêt européen soit vérifiée au préalable.

2/ Le fonctionnement du système

Pour mettre les données à disposition, les transporteurs aériens sont invités à utiliser la méthode dite « PUSH » par laquelle ce sont eux-mêmes qui transmettront les données aux autorités compétentes. À défaut, ils devront autoriser l'unité de renseignements passagers à extraire les données de leur base de données en utilisant la méthode dite « pull ».

Comme la commission des affaires européennes l'avait relevé dans le cadre de l'accord entre l'Union européenne et les États-Unis, seule la méthode dite « PUSH » peut offrir les garanties nécessaires, en permettant aux transporteurs aériens de garder le contrôle de la qualité des données transmises et des conditions de transmission. Le contrôleur européen pour la protection des données a fait opportunément valoir que l'utilisation de différentes modalités de communication des données en fonction des transporteurs concernés ne ferait qu'augmenter les difficultés de contrôle de la conformité de la transmission avec les règles de protection des données et risquerait en outre d'entraîner des distorsions de concurrence entre les transporteurs. Les transporteurs aériens devraient donc être appelés à adopter un système « PUSH » afin de garantir une approche uniformisée.

Par ailleurs, chaque État membre devra désigner une autorité compétente, dénommée « unité de renseignements passagers », chargée de collecter auprès des transporteurs aériens les données PNR. En l'état néanmoins, la proposition initiale de la Commission européenne demeure très elliptique sur la qualité de cette unité, même s'il est vraisemblable que les États membres la confieront à des services tels que les douanes ou ceux chargés du contrôle aux frontières.

Le rapport de la présidence française précise qu'il s'agirait d'une autorité publique gardienne de la base de données PNR et garante du respect des règles en vigueur. L'accès à cette base de données serait réservé à des agents individuellement désignés et spécialement formés. Une définition claire des usages pouvant être faits de la base devrait être donnée. Il paraît indispensable que des précisions et des garanties soient apportées sur ce point dans le texte même de la proposition.

En outre, le rôle des autorités indépendantes sur la protection des données devrait être précisé. Elles devraient être habilitées à effectuer des contrôles au sein de l'Unité.

Enfin, le rôle des intermédiaires doit être clarifié. Une société privée pourrait se voir confier la mission de recueillir les données et de les transmettre ensuite à l'unité d'information passagers. C'est le cas dans le cadre de l'accord passé avec le Canada. La SITA, société commerciale créées en 1949 par onze transporteurs aériens, est chargée du traitement des informations. Le rôle de ces intermédiaires devrait donc être strictement précisé et encadré.

3/ Les données utilisées

Annexée à la proposition, la liste des données qui devront être transmises est similaire à celle des données qui doivent être mises à la disposition des autorités américaines en vertu de l'accord entre l'Union européenne et les États-Unis. Elle comprend 19 rubriques. Mais le groupe de l'article 29 juge que cette liste - qui, en réalité, recouvre 35 types d'informations - est excessive et que la proposition n'explique pas en quoi une telle quantité de données est nécessaire à la lutte contre le terrorisme et la criminalité organisée. Il relève que l'accord avec le Canada ne prévoit que 25 types d'informations. Il paraît donc nécessaire que cette liste fasse l'objet d'un examen supplémentaire afin que l'utilité des données collectées soit avérée au regard des finalités poursuivies.

La proposition de la Commission européenne prévoit, par ailleurs, l'effacement immédiat, soit par l'unité de renseignements passagers soit par l'intermédiaire proposé, des données sensibles pouvant révéler les origines raciales ou ethniques, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance à un syndicat, ou des données concernant la santé ou l'orientation sexuelle des individus. Le groupe de l'article 29 fait valoir que l'un des grands principes de la protection des données est le rôle du responsable du traitement dans le traitement des données à caractère personnel. Il estime en conséquence qu'il devrait incomber aux transporteurs aériens de filtrer les données sensibles.

Le rapport de la présidence française indique que l'exclusion des données sensibles devrait plutôt reposer sur un effacement ou un verrouillage individuellement pratiqué au sein de l'Unité de renseignements. Mais il a été relevé au cours des discussions entre États membres que si l'utilisation de données sensibles est en principe interdite, il est traditionnellement jugé légitime d'en permettre l'utilisation dans le contexte d'une enquête criminelle si l'information qu'elles apportent peut soit contribuer à résoudre l'enquête, soit aider à laver la personne concernée de tout soupçon.

Il est proposé de retenir la préconisation consistant en un filtrage des données sensibles par les transporteurs aériens, à charge pour eux de les conserver pendant une certaine durée afin de pouvoir répondre à une demande qui serait faite dans le cadre d'une procédure judiciaire.

En outre, comme le mentionne le rapport de la présidence française parmi les pistes explorées, tout traitement arbitraire ou discriminatoire devrait être explicitement exclu : aucun critère d'évaluation ne pourrait se fonder sur la race ou l'origine ethnique, les convictions religieuses, les opinions politiques, l'appartenance à un syndicat, la santé ou l'orientation sexuelle d'une personne ; ces éléments ne pourraient non plus servir de point de départ d'une enquête ou d'une quelconque recherche

4/ Les destinataires des données

Les États membres devront adopter une liste des autorités compétentes pour recevoir les données PNR et les traiter. Cette liste ne pourra comprendre que des autorités chargées de prévenir et de combattre les infractions terroristes et la criminalité organisée.

Mais ces autorités peuvent être dotées de compétences très diverses en fonction de la législation des États membres. Ces compétences peuvent inclure ou non le renseignement, la fiscalité, l'immigration ou les missions de police. La proposition devrait donc être beaucoup plus précise sur les compétences et les obligations légales de ces autorités et, aussi, des unités de renseignements passagers et des intermédiaires.

5/ La durée de conservation des données

Les données collectées pourront être conservées pendant cinq ans. Une période supplémentaire de huit ans est prévue mais avec des conditions particulières : pendant cette période, le traitement et l'utilisation des données PNR ne pourront se faire qu'avec le consentement de l'autorité compétente ; elle sera possible uniquement dans des circonstances exceptionnelles en réponse à une menace ou un risque spécifiques dans le cadre de la prévention d'infractions terroristes et de la criminalité organisée ou de la lutte contre ces phénomènes ; l'accès à ces données sera limitée au personnel des autorités compétentes spécifiquement habilitées à cet effet ; les données devront être effacées à l'issue de la période de huit ans.

On aboutirait ainsi à une durée globale de conservation de 13 ans qui apparaît manifestement disproportionnée par rapport aux objectifs poursuivis. Les réponses des États membres au questionnaire que leur avait adressé la Commission européenne met en évidence que la durée moyenne de conservation requise serait, en pratique, de trois ans et demi. Le rapport de la présidence française fait valoir que la durée de conservation des données pourrait être fixée autour de trois ans avec une durée supplémentaire de 3 à 7 ans, soit une durée totale de conservation de 6 à 10 ans. Le Sénat doit donc demander qu'un délai raisonnable soit retenu.

6/ Le régime de protection des données

La décision-cadre sur la protection des données dans le cadre du troisième pilier s'appliquera aux traitements de données à caractère personnel au titre du PNR européen.

Cependant, cette décision-cadre n'est applicable qu'aux relations entre États membres dans le contexte de la coopération policière et judiciaire en matière pénale. En revanche, les relations entre les transporteurs aériens, les intermédiaires éventuels et l'unité de renseignements passagers sont couvertes par la directive du 24 octobre 1995. Or la proposition n'indique pas à quelle étape la décision-cadre s'appliquera et pourrait même suggérer qu'elle aurait vocation à couvrir l'ensemble du processus. Il y a donc là une clarification à opérer sur le régime de protection des données, en privilégiant un haut niveau de protection par référence aux standards du Conseil de l'Europe.

7/ Le droit des personnes concernées

Un considérant de la proposition indique que le droit des personnes concernées, pour ce qui concerne le traitement des données, comme le droit à l'information, le droit d'accès, le droit de rectification, d'effacement, ainsi que les droits à réparation et aux recours juridictionnels, devraient être ceux prévus par la décision-cadre sur la protection des données dans le cadre du troisième pilier.

Outre la difficulté posée par le champ limité de cette décision-cadre, précédemment mentionnée, cette affirmation ne permet pas de déterminer qui sera le responsable du traitement chargé de donner suite à ces demandes. En conséquence, la proposition devrait être beaucoup plus précise sur le régime juridique applicable suivant l'étape du traitement des données et sur le responsable chargé de prendre en compte le droit à l'information, le droit d'accès ou de rectification.

8/ La transmission des données à des États tiers

La transmission des données ainsi collectées à d'autres États membres ne sera autorisée que dans les cas et dans la mesure où cette transmission est nécessaire pour prévenir et combattre les infractions terroristes et la criminalité organisée. La communication à des pays tiers ne sera permise qu'à la double condition que cette finalité soit bien respectée et que le pays tiers en question ne transmette pas les données à un autre pays tiers sans l'accord explicite de l'État membre. En outre, les conditions et garanties prévues par la décision-cadre sur la protection des données dans le cadre du troisième pilier seront applicables.

Cependant, cette décision-cadre ne vise que la protection des données reçues d'un autre État membre et pas les transferts directs de données d'un État membre vers un État tiers. En pratique, il sera probablement difficile de faire la part entre les données selon leur origine. En outre, il y a lieu de s'inquiéter de la réciprocité dont pourraient bénéficier des États tiers n'offrant pas les garanties nécessaires en matière de protection des données.

Il est donc nécessaire que la proposition précise expressément que l'État tiers devra assurer un niveau de protection adéquat de protection des données et que le transfert ne pourra s'opérer qu'au cas par cas et non par « masses » d'informations. Des garanties devraient être assurées dans la mise en oeuvre du principe de réciprocité.

Pour l'ensemble de ces motifs, la commission des affaires européennes a décidé de proposer au Sénat l'adoption de la proposition de résolution suivante :

PROPOSITION DE RÉSOLUTION

Le Sénat :

Vu l'article 88-4 de la Constitution ;

Vu la proposition de décision-cadre relative à l'utilisation des données des dossiers passagers (Passenger Name Record - PNR) à des fins répressives (E 3697) ;

- prenant acte que cette proposition de décision-cadre tend à promouvoir une approche harmonisée au sein de l'Union européenne de l'utilisation des données des dossiers passagers à des fins répressives et que des discussions sont en cours au sein du Conseil ;

- considère qu'une telle approche doit retenir parmi ses priorités d'assurer un respect effectif des droits fondamentaux, en particulier le droit au respect de la vie privée et à la protection des données à caractère personnel ;

- souligne que les finalités de la proposition doivent être précisément délimitées et concerner exclusivement la prévention, la détection, l'instruction, la poursuite et la répression du terrorisme et d'un ensemble d'infractions graves pour lesquelles l'utilisation de données des dossiers passagers s'avérerait pertinente ;

- estime que seule la méthode de transmission dite « PUSH » peut offrir les garanties nécessaires en permettant aux transporteurs aériens de garder le contrôle de la qualité des données transmises et des conditions de transmission ;

- juge nécessaire que des précisions et des garanties supplémentaires soient prévues sur la qualité des services qui seront chargés de l'unité de renseignements passagers et celle des autorités compétentes pour recevoir les données PNR et les traiter, ainsi que sur les conditions dans lesquelles des intermédiaires seraient susceptibles d'intervenir dans la collecte et la transmission des données ;

- demande que les autorités indépendantes sur la protection des données soient habilitées à effectuer des contrôles au sein de l'unité de renseignements passagers ;

- considère que la liste des données devant être transmises devrait faire l'objet d'un examen supplémentaire afin que l'utilité de leur collecte soit avérée au regard des finalités poursuivies ;

- demande que l'utilisation de données sensibles révélant la race ou l'origine ethnique, les convictions religieuses, les opinions politiques, l'appartenance à un syndicat, la santé ou l'orientation sexuelle d'une personne soit en principe exclue, que leur filtrage soit assuré directement par les transporteurs aériens et que, si leur conservation était envisagée aux seules fins de leur possible utilisation dans le cadre d'une enquête criminelle, des garanties spécifiques soient prévues ;

- juge manifestement disproportionnée la durée totale de treize ans prévue par la proposition pour la conservation des données et demande, en conséquence, que cette durée soit réduite à un délai raisonnable ;

- estime que le régime de protection des données applicable doit être clarifié, en privilégiant un haut niveau de protection par référence aux standards du Conseil de l'Europe ;

- demande que des garanties supplémentaires soient prévues dans le texte même de la proposition sur les droits des personnes concernées, en particulier pour l'exercice du droit à l'information, du droit d'accès, de rectification et d'effacement des données et que le responsable du traitement chargé de donner suite à leurs demandes soit précisément identifié ;

- considère que les conditions dans lesquelles les données seraient susceptibles d'être transmises à des États tiers n'offrent pas les garanties suffisantes ; demande, en conséquence, qu'un tel transfert ne soit possible qu'au cas par cas et sous réserve que l'État tiers assure un niveau de protection adéquat des données et que des garanties soient prévues dans la mise en oeuvre du principe de réciprocité.

Post-scriptum :

http://www.senat.fr/leg/ppr08-252.html