COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Strasbourg, le 19 août 2016

T-PD(2016)18rev

**COMITÉ CONSULTATIF DE LA CONVENTION
POUR LA PROTECTION DES PERSONNES À L'ÉGARD DU
TRAITEMENT AUTOMATISÉ DES DONNÉES À CARACTÈRE PERSONNEL
(T-PD)**

Avis sur

les implications en matière de protection des données du traitement des dossiers passagers

Direction générale droits de l'homme et Etat de droit

Table des matières

Le Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STCE n° 108, ci-après la « Convention 108 »),

Rappelant la Convention européenne des droits de l'homme (CEDH), en particulier ses articles 8 (droit au respect de la vie privée) et 13 (droit à un recours effectif), tels que développés plus avant par la jurisprudence de la Cour européenne des droits de l'homme, et l'article 2 (liberté de circulation) du Protocole n° 4,

Considérant la Convention 108 et les autres instruments pertinents du Conseil de l'Europe dans le domaine de la protection des données, notamment la Recommandation (87)15 visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police et la Recommandation (2010)13 sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage,

Notant l'expansion rapide, au niveau mondial, des systèmes informatiques et des législations ayant trait à la transmission par les transporteurs aériens des données à caractère personnel de leurs passagers aux autorités publiques pour assurer le respect de la loi, le maintien de l'ordre et la sécurité nationale,

Résolu à promouvoir le respect des droits de l'homme dans le contexte du traitement des données à caractère personnel des passagers aériens par les autorités publiques en charge de la prévention, de la détection, de l'instruction et de la poursuite des infractions de terrorisme et autres infractions pénales graves,

Adopte le présent avis :

1. Introduction

Face aux préoccupations grandissantes que suscitent les réactions aux récents attentats et menaces terroristes, il a été décidé, lors de la 32e réunion plénière (1-3 juillet 2015) du Comité consultatif de la Convention 108, de préparer le présent avis, en tenant notamment compte des aspects traités dans le rapport intitulé « Passenger Name Records (PNR), data mining and data protection: the need for strong safeguards » (Dossiers passagers (PNR), exploration et protection des données : nécessité de garanties solides – en anglais uniquement)[1].

Lors de ses 36ème (6-8 octobre 2015), 37ème (9-11 décembre 2015) et 38ème (22-24 mars 2016) réunions, le Bureau du Comité s'est employé à préparer l'avis, qui a été examiné à la 33e réunion plénière du Comité de la Convention 108 après consultation écrite des délégations et des parties intéressées.

Le Comité de la Convention 108 reconnaît que, dans le contexte récent de l'intensification des menaces d'attentats terroristes, la lutte contre le terrorisme doit être renforcée. Il souligne qu'il est important de le combattre de façon efficace et effective tout en veillant au respect des droits de l'homme, de l'état de droit et des valeurs communes défendues par le Conseil de l'Europe. Le Comité prend note de la volonté des gouvernements de mettre en place, au nombre des moyens de prévention du terrorisme et autres infractions pénales graves et dans le cadre des efforts qu'ils déploient pour garantir la sécurité de la population, des systèmes de filtrage des données à caractère personnel relatives aux passagers aériens. Dans ce contexte, le Comité juge nécessaire de rappeler les principes de protection

[1] Rapport préparé par M. D. Korff avec la contribution de Mme M. Georges: http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/T-PD(2015)11_PNR%20draft%20report%20Douwe%20Korff%20&%20Marie%20Georges_15%2006%202015.pdf

des données applicables à ces systèmes, en soulignant qu'une atteinte aux droits fondamentaux, et notamment à la protection de la vie privée et à la protection des données à caractère personnel, n'est acceptable que sous certaines conditions impératives.

L'article 8 de la CEDH et l'article 9 de la Convention 108 ont fixé les conditions qui doivent être respectées lorsqu'est envisagée une restriction des droits au respect de la vie privée et à la protection des données. Cette restriction doit être conforme à une loi clairement formulée ; elle doit en outre être nécessaire, dans une société démocratique, à la poursuite d'un but légitime (comme la sécurité nationale, la sûreté publique ou la prévention des infractions pénales).

2. Description des données PNR

Il existe plusieurs types de données relatives aux passagers ; aux fins du présent avis, le Comité concentrera son attention sur les dossiers passagers (PNR).

Les PNR sont des dossiers utilisés par les exploitants aériens aux fins commerciales et opérationnelles de la fourniture de services de transport aérien. Les PNR sont créés par les compagnies aériennes et les agences de voyages[2], en relation avec les réservations de voyage, afin de permettre un échange d'informations entre elles et en conformité avec les demandes des passagers. Ces dossiers sont saisis de plusieurs façons, étant donné[3] que les réservations peuvent être créées dans des systèmes mondiaux de distribution (GDS pour « Global Distribution Systems »), des systèmes informatisés de réservation (SIR) ou le système de réservation propre à la compagnie aérienne. Les données saisies dans le système de contrôle des départs (DCS pour « Departure Control System ») de la compagnie aérienne au moment de l'enregistrement du passager (c'est-à-dire, le numéro de siège et les informations relatives aux bagages) peuvent également être ajoutées automatiquement à un PNR existant lorsque le SIR et le DCS sont intégrés dans un même système.

Bien que les PNR aient été institués à l'origine pour le transport aérien, le SIR peut dorénavant aussi être utilisé pour les réservations d'hôtel, les locations de voiture ou les déplacements en bateau ou en train.

Compte tenu des besoins communs de multiples acteurs, le format et le contenu des PNR ont été progressivement harmonisés et normalisés par l'Association internationale du transport aérien (IATA), qui apporte son aide dans la conception de programmes relatifs aux données passagers.

Un PNR contient tout ou partie des informations suivantes fournies par les passagers :

- nom complet[4] ;
- adresse et autres coordonnées (numéro de téléphone, adresse électronique, adresse IP) ;

[2] A l'avenir, les « opérateurs économiques non transporteurs » (c'est-à-dire les agences de voyages et les tour-opérateurs) pourraient être tenus de communiquer les données PNR aux autorités nationales compétentes.

[3] Parmi les systèmes mondiaux de distribution traditionnels, Amadeus est le seul établi en Europe (siège en Espagne, centre de données en Allemagne et centre de recherche-développement en France). Il appartient notamment à Air France, Iberia, Lufthansa, British Airways et Scandinavian Airlines, qui l'utilisent ; plus de 60 autres transporteurs dans le monde y sont affiliés.

[4] Informations vérifiées sur la base des informations figurant sur le passeport présenté par le passager.

- type de document d'identité, numéro, pays de délivrance et date d'expiration[5] ;
- date et pays de naissance[6] ;
- nationalité[7] ;
- pays de résidence ;
- itinéraire (dates, lieu de départ et d'arrivée) ;
- adresse pour la première nuit passée dans le pays de destination ;
- méthode de paiement utilisée, avec adresse de facturation et informations sur la carte de crédit ;
- profil de client fidèle et avantages (billet gratuit ou surclassement sans frais) ;
- un champ ouvert avec des observations générales (« Demande de prestations spéciales », « Instructions relatives aux services optionnels » ou « Informations sur les autres services »), telles que l'ensemble des informations disponibles sur les mineurs non accompagnés, les demandes diététiques et médicales, les préférences de siège, les langues, les renseignements concernant un handicap et autres demandes similaires ;
- référence individuelle (code du dossier PNR) ;
- informations sur l'agence de voyage ou l'agent de voyage ;
- données du billet (numéro, date de réservation, date d'émission, aller simple) ;
- détail du prix et restrictions éventuellement applicables au tarif (et taxes) ;
- noms et nombre de passagers voyageant ensemble figurant dans le même PNR ;
- statut des passagers (confirmations, enregistrement, non-présentation ou passager de dernière minute sans réservation) ;
- numéro du siège et autres informations concernant le siège ;
- partage de code ;
- information scindée/divisée (lorsque les itinéraires de plusieurs passagers d'un PNR ne sont pas identiques et que des modifications doivent être apportées à la réservation d'un passager d'un PNR existant) ;
- bagages ;
- historique de toutes les modifications des données PNR susmentionnées.

Dans la pratique, le contenu des PNR varie sensiblement d'un cas à l'autre, étant donné que le nombre et le type des champs à compléter dépendent de l'itinéraire (par exemple, dans le cas d'un aller-retour couvrant plusieurs villes dans un même pays ou dans plusieurs pays), de l'offre de services des compagnies aériennes et du système de réservation utilisé (plus de 60 champs à renseigner dans certains cas).

Le fait que les informations recueillies soient fournies par les passagers, ou pour leur compte, et qu'elles ne soient pas systématiquement vérifiées (à l'exception par exemple des informations relatives au vol fournies par les compagnies aériennes et des informations figurant sur le passeport, lorsque celui-ci n'est pas un faux) doit aussi être pris en compte en relation avec le principe d'exactitude des données. Il existe un risque d'erreur puisqu'un PNR peut contenir des informations incorrectes sur une personne, qui pourraient, dans certaines circonstances, éveiller les soupçons.

Les compagnies aériennes peuvent avoir l'obligation légale de transférer tout ou partie des données PNR aux autorités publiques compétentes afin d'identifier des personnes soupçonnées de participation à des activités terroristes ou autres crimes graves.

[5] Informations vérifiées sur la base des informations figurant sur le passeport présenté par le passager.
[6] Informations vérifiées sur la base des informations figurant sur le passeport présenté par le passager.
[7] Informations vérifiées sur la base des informations figurant sur le passeport présenté par le passager.

3. Légalité

Si les PNR peuvent présenter un intérêt pour les autorités publiques compétentes dans la poursuite d'un but légitime, il faut qu'un certain nombre de conditions soient remplies pour que l'atteinte aux droits à la vie privée et à la protection des données qu'ils représentent puisse être permise.

Selon la jurisprudence de la Cour européenne des droits de l'homme relative à l'article 8 de la CEDH, une telle atteinte n'est permise que si elle est prévue par la loi et strictement nécessaire et proportionnée au but légitime visé.

Si la nécessité de l'atteinte et la proportionnalité des mesures envisagées doivent faire l'objet d'un examen approfondi en tenant compte de divers éléments, le Comité rappelle brièvement ce que recouvre, d'après la CEDH, la condition de légalité. L'exigence que toute atteinte soit « conforme à la loi » (ou « prévue par la loi » aux termes de l'article 9 de la Convention 108) implique que trois conditions soient remplies :

- la mesure doit être fondée en droit interne,
- la loi doit être suffisamment claire et précise pour être accessible à la personne concernée (elle doit à l'évidence être rendue publique), et
- la loi doit avoir des conséquences prévisibles (permettant à la personne, au besoin à l'aide de conseils appropriés, de régler son comportement et d'agir en conséquence)[8].

Dans le contexte du traitement des PNR par les services chargés du respect de la loi, le critère de la qualité de la loi implique une définition très précise et rigoureuse du but légitime visé.

4. Nécessité et proportionnalité

Vu l'atteinte aux droits des personnes concernées qui peut découler des mesures prescrites ou envisagées concernant le traitement des données PNR par les autorités publiques compétentes, il est indispensable de démontrer la nécessité et la proportionnalité de ces mesures. Le Comité demande l'examen des éléments objectifs qui permettent d'évaluer cette nécessité, la proportionnalité des mesures prescrites, ainsi que l'efficacité et l'effectivité du système (qui doivent pouvoir être démontrées lorsque de tels systèmes existent déjà).

Le traitement des données PNR – qui a l'avantage unique de permettre l'identification des personnes d' intérêt - est un filtrage général et non sélectif de tous les passagers, y compris de ceux qui ne sont pas soupçonnés d'avoir commis une quelconque infraction pénale, par différentes autorités compétentes, et il concerne des données collectées initialement à des fins commerciales par des entités privées. Eu égard à l'ampleur de l'atteinte aux droits à la vie privée et à la protection des données qui découlerait du traitement des données PNR, il doit être clairement établi que ledit traitement est une mesure nécessaire dans une société démocratique dans un but légitime ; il faut en outre que les garanties appropriées soient mises en place. Il est indispensable de démontrer expressément la nécessité de la collecte et de l'exploitation ultérieure des données PNR.

[8] Cour européenne des droits de l'homme : *Kennedy c. Royaume-Uni*, § 151 ; *Rotaru c. Roumanie*, 28341/95, §§ 50, 52 et 55 ; *Amann c. Suisse*, § 50 ; *Iordachi et autres c. Moldova* ; *Kruslin c. France*, § 27 ; *Huvig c. France*, § 26 ; *Association pour l'intégration européenne et les droits de l'homme et Ekimdzhiev c. Bulgarie*, § 71 ; *Liberty et autres c. Royaume-Uni*, § 59 ; etc.

La Cour européenne des droits de l'homme a souligné que « si l'adjectif "nécessaire" (…) n'est pas synonyme d'"indispensable" (…), il n'a pas non plus la souplesse de termes tels qu'"admissible", "normal" (…),"utile" (…),"raisonnable" (…) ou "opportun" »[9].

Disposant d'une marge d'appréciation dans le choix des moyens nécessaires pour atteindre son but légitime et nécessaire, l'Etat doit déterminer si les atteintes induites par ces mesures correspondent à un « besoin social impérieux »[10]. L'évaluation de la proportionnalité de la dérogation doit reposer sur l'examen d'un vaste ensemble d'éléments tels que la définition de buts clairs et limités, du champ d'application du système, de la nature des données concernées, de la nature du traitement, des modalités d'accès aux données et de leur conservation, etc.

Se prononçant sur la validité de la directive sur la conservation des données (en ce qui concerne la conservation des données de communication), la Cour de justice de l'Union européenne a souligné[11] que « les dérogations à la protection des données à caractère personnel et les limitations de celle-ci doivent s'opérer dans les limites du strict nécessaire ».

Dans le cas des systèmes existants de traitement des données PNR par les autorités publiques compétentes, une plus grande transparence sur l'évaluation de l'efficacité de ces systèmes doit être recherchée en vue de permettre une évaluation fondée et indépendante de la nécessité du système. Si cette transparence doit être détaillée, elle ne doit toutefois pas aller à l'encontre de l'objectif légitime. Par exemple, des informations objectives et quantifiables concernant les résultats atteints, comme le nombre de personnes arrêtées, les menaces terroristes qui pourraient être évitées, les autres effets dissuasifs, la modification des comportements des délinquants (par exemple, le renoncement à des actes criminels envisagés), la probabilité d'une augmentation importante du coût et de la difficulté de la perpétration d'infractions (tels que des attentats terroristes) permettraient d'éclairer l'évaluation de la nécessité d'un système de traitement des PNR.

Il convient de procéder à intervalles réguliers à un examen de la nécessité du système des PNR afin de déterminer s'il est toujours justifié.

5. Application des principes et garanties

(a) Limitation des finalités

Eu égard au degré d' atteinte aux droits à la vie privée et à la protection des données, induites par le traitement des données PNR par des autorités publiques compétentes, les buts doivent être définis par la loi de façon claire et précise sur la base de critères objectifs qui limitent la transmission de ces données uniquement aux autorités compétentes ainsi que le traitement ultérieur de ces données.

Les systèmes des PNR étant généralement justifiés par la prévention, la détection, l'instruction et la poursuite des infractions de terrorisme et autres infractions pénales graves (comme le trafic de drogues, la traite des êtres humains, la traite d'enfants, le blanchiment de capitaux) ou des crimes internationaux (comme les crimes contre l'humanité, les actes de torture ou le génocide), une délimitation claire de ces buts légitimes et notions correspondantes est nécessaire afin de circonscrire rigoureusement l'utilisation de ces systèmes.

---

[9] *Handyside c. Royaume-Uni*, 5493/72, §48.
[10] *Olsson c. Suède*, 10465/83.
[11] *Digital Rights Ireland*, C 293/12 du 8 avril 2014, § 52.

La définition des termes « terrorisme » et « actes de terrorisme » est particulièrement complexe (voir les conventions pertinentes des Nations Unies, la Convention du Conseil de l'Europe pour la prévention du terrorisme de 2005 et son Protocole additionnel de 2015) ; en l'absence d'une délimitation claire, ces termes doivent être interprétés de façon restrictive. Dans le cas contraire, la finalité du système de PNR resterait trop vague et le principe de proportionnalité ne serait pas respecté.

Dans des cas exceptionnels, la prévention de menaces graves au public (par exemple, pour la prévention de la propagation d'une maladie contagieuse dangereuse) pourrait aussi justifier l'utilisation des données PNR.

(b) Autorités compétentes

Afin de garantir le caractère proportionné des atteintes aux droits des personnes concernées, les autorités publiques recevant les données PNR doivent être les autorités responsables des buts légitimes précédemment définis.

Par ailleurs, l'établissement d'une unité de coordination spéciale (telle que l'« unité de renseignements passagers » dans le dispositif de l'UE) peut contribuer à empêcher une superposition entre les activités judiciaires et les activités de surveillance, mais les compétences d'une telle unité doivent être définies de façon rigoureuse et restrictive et rendues publiques.

La liste des autorités nationales compétentes qui sont habilitées par la loi à traiter les données PNR devrait être dressée et cette information devrait être rendue publique.

(c) Données personnelles des passagers

Les données transmises aux autorités publiques compétentes et traitées par ces dernières doivent être pertinentes, adéquates et proportionnées (article 5 de la Convention 108) par rapport aux finalités pour lesquelles elles sont traitées. Les données transmises doivent être clairement définies (la liste complète des éléments du PNR qui doivent être transmis doit être dressée), sur la base de critères objectifs, et des limites à leur utilisation ultérieure doivent aussi être établies.

Les PNR contiennent des informations visant à faciliter le voyage d'un passager, et peuvent comprendre un certain nombre de données sensibles (données pouvant servir à indiquer l'origine raciale, les opinions politiques, les convictions religieuses ou autres, l'état de santé ou l'orientation sexuelle d'une personne), non seulement sous certaines données «codées » mais aussi dans le champ ouvert contenant des observations générales (telles que les demandes diététiques et médicales, ou le fait qu'une association politique ou religieuse a bénéficié de billets à prix réduit pour le voyage de ses membres), ce qui pourrait conduire à une discrimination directe.

Même si les autorités compétentes recevant de telles données dans les PNR peuvent être autorisées à les traiter dans des circonstances exceptionnelles et rigoureusement justifiées (aucune évaluation ne peut être pratiquée sur la base de critères liés à des données sensibles, le Comité considère qu'une interdiction de l'utilisation systématique de telles données sensibles par les autorités publiques compétentes devrait être établie en tant que principe.

(d) Transmission des données

Il existe deux méthodes différentes de transmission des données, du secteur commercial aux autorités compétentes du secteur public :

- le mode « *pull* », par lequel les autorités publiques obtiennent un accès direct au système de réservation et en extraient une copie des données requises ;
- le mode « *push* », par lequel l'opérateur transfère les données PNR requises dans la base de données de l'autorité qui en fait la demande.

Le Comité considère que le mode « push », dans lequel l'opérateur assume l'entière responsabilité de la qualité des données et des conditions de transmission, doit être préféré, vu qu'il offre de plus grandes garanties de protection des données par rapport au mode « pull ».

(e) Mise en correspondance et exploration de données

Le traitement des données à caractère personnel peut concerner tous les passagers et pas seulement les individus ciblés soupçonnés d'être impliqués dans une infraction pénale ou de constituer une menace immédiate à la sécurité nationale ou à l'ordre public.

Les données PNR peuvent être comparées (« data matching ») à des bases de données[12] (à savoir, des bases sur les personnes condamnées pour infractions pénales graves, les personnes visées par une enquête pour soupçon d'activités terroristes, les passeports volés ou perdus) tenues par les autorités compétentes conformément à la loi afin d'identifier les suspects ou auteurs d'infractions ainsi que les personnes liées à ces suspects ou auteurs d'infractions potentiels (« graphe social »).

Les données PNR peuvent aussi être traitées dans le but d'identifier (par « data mining ») quiconque « pourrait » être impliqué ou s'engager dans les activités criminelles définies par la loi qui établit le partage des PNR avec les autorités compétentes comme, par exemple, les individus voyageant dans le but de devenir des combattants terroristes étrangers. Cela pourrait être obtenu par l'exploration de données selon des sélecteurs ou des algorithmes prédictifs.

L'évaluation des passagers par la mise en correspondance de données peut soulever la question de la prévisibilité, en particulier lorsqu'elle est effectuée sur la base d'algorithmes prédictifs utilisant des critères dynamiques susceptibles d'évoluer en permanence selon les capacités d'auto-apprentissage.

Le développement d'algorithmes d'exploration de données devrait se fonder sur les résultats d'évaluations régulières de l'impact probable du traitement de données sur les droits et libertés fondamentales des personnes concernées.

La structure de base des analyses devrait se fonder sur des indicateurs de risque prédéfinis ayant été clairement établis au préalable.

La pertinence des résultats individuels de ces évaluations automatiques devrait être examinée avec soin au cas par cas, par une personne et de façon non automatisée.

.

(f) Conservation des données

La durée de conservation des données PNR doit être clairement précisée et limitée au temps absolument nécessaire pour l'objectif prescrit dans la mesure où « la détermination de la durée de conservation doit être fondée sur des critères objectifs afin de garantir que celle-ci est limitée au strict nécessaire »[13]. Ces critères devraient être accessibles au public.

[12] Des bases de données créées, gérées et actualisées conformément à la loi.

[13] Digital Rights Ireland, C--293/12 du 8 avril 2014, § 64.

Masquer[14] certains éléments des données qui identifient le passager après une période prédéterminée, réduite au minimum, peut atténuer les risques induits par une période de conservation prolongée des données, comme par exemple un accès abusif, pour tous les passagers.

Il convient de rappeler que des données masquées permettent encore d'identifier les personnes et restent à ce titre des données à caractère personnel, et que leur conservation devrait aussi être limitée dans le temps pour prévenir une surveillance permanente généralisée.

(g) Droits d'information, d'accès, de rectification et d'effacement

Le Comité rappelle qu'aux termes de l'article 1 de la CEDH et de l'article 1 de la Convention 108, les droits à la vie privée et à la protection des données doivent être garantis à chaque personne relevant de la juridiction des parties contractantes, quels que soient sa nationalité ou son lieu de résidence.

La personne dont les données PNR sont transmises aux autorités compétentes a le droit de savoir comment elles sont traitées par ces autorités (nature des données, à quelles fins et comment, pour quelle durée), a un droit d'accès et a le droit de demander la rectification ou l'effacement des données à caractère personnel.

Même si la limitation de ces droits est soumise à des conditions restrictives mentionnées précédemment (à savoir que la limitation soit conforme à la loi et nécessaire pour atteindre un but légitime), le Comité recommande que les personnes qui ne sont pas soupçonnées d'avoir commis, ou d'envisager de commettre, un acte de terrorisme ou une autre infraction pénale grave jouissent du plein exercice des droits en question et que les personnes qui sont soupçonnées d'avoir commis, ou d'envisager de commettre, une telle infraction puissent au moins demander la correction de données inexactes et l'effacement de données illicites.

Toute limitation des droits considérés doit être portée à la connaissance des passagers au moment de la collecte de leurs données et pendant toute l'activité de traitement par les autorités publiques compétentes.

Lorsque des données relatives à un passager ont été recueillies à son insu, à moins qu'elles ne soient supprimées, la personne devrait être informée, si possible, que des informations sont conservées à son sujet dès que cela ne risque plus de desservir le but recherché par la collecte.

Les personnes concernées devraient être informées des modalités d'exercice de leurs droits et des voies de recours dont elles disposent.

(h) Sécurité

En application de l'article 7 de la Convention 108, des mesures de sécurité appropriées doivent être prises pour assurer la protection des données à caractère personnel. Cela suppose notamment que le système de PNR soit détenu dans un environnement physique sûr, doté de systèmes perfectionnés de protection contre l'intrusion et soumis à un strict contrôle d'accès (accès accordé à un nombre limité de personnes et basé, par exemple, sur une identification à niveaux multiples et la production d'un état d'audit des accès). En outre, la communication des données PNR aux autorités compétentes doit être protégée par des

[14] « Masquer » signifie rendre invisibles certains éléments de données permettant d'identifier une personne.

moyens techniques et procéduraux (par exemple, solide dispositif de cryptographie, procédures efficaces de gestion de clés, etc.).

(i) Flux transfrontières de données

Le Comité rappelle que tout transfert de données PNR aux Etats qui ne sont pas parties à la Convention 108 doit satisfaire aux conditions établies pour garantir la protection appropriée des personnes concernées dans ces Etats.

(j) Recours

Aux termes de la jurisprudence de la Cour européenne des droits de l'homme, il est essentiel que des « recours effectifs » contre les violations des droits fondamentaux existent et soient accessibles aux individus (et pas seulement aux ressortissants du pays particulier concerné). Si la Cour de justice de l'Union européenne mentionne expressément l'obligation de recours devant un tribunal, la Cour européenne des droits de l'homme a estimé[15] que l'absence de contrôle juridictionnel ne constituait pas nécessairement une violation des droits en jeu dès lors que la législation prévoit d'autres garanties fortes (par exemple, un contrôle indépendant par des autorités disposant de pouvoirs et de compétences suffisants pour exercer un contrôle effectif et continu).

L'article 10 de la Convention 108 impose aux parties d'établir « des sanctions et recours appropriés visant les violations aux dispositions du droit interne donnant effet aux principes de base pour la protection des données » énoncés dans la Convention.

Le Comité soutient la nécessité de prévoir une réparation effective pour les individus, qui couvrirait à la fois les recours judiciaires et administratifs. Le Comité souligne aussi qu'il est important, comme condition préalable à un recours effectif, que la personne concernée soit pleinement informée du traitement de ses données à caractère personnel, et insiste sur la difficulté de garantir un recours effectif contre des décisions fondées sur des algorithmes et de contester des atteintes fondées sur une analyse de données (faux positifs et autres mesures discriminatoires).

(k) Contrôle et transparence

Il ressort clairement de la jurisprudence de la Cour européenne des droits de l'homme que le contrôle des autorités chargées de la surveillance devrait être assuré par un organe externe indépendant.

Le Comité souligne le rôle des autorités compétentes chargées de la protection des données, qui doivent non seulement être consultées dans le cadre du processus normatif de l'adoption des lois et règlements pertinents, mais pourraient aussi évaluer la conformité d'un système de PNR avec les règles de protection des données sur la base des plaintes individuelles dont elles pourraient être saisies ou à leur propre initiative.

D'autres autorités indépendantes spécialisées (telles qu'une commission parlementaire) habilitées à surveiller les organes d'application de la loi et de renseignement peuvent également jouer un rôle s'agissant de contrôler le champ d'application et l'efficacité du système et d'effectuer des contrôles, au cas par cas, du bien-fondé de la conservation des données des passagers et de la durée de cette conservation.

Un contrôle assuré par des autorités indépendantes chargées de la protection des données et d'autorités indépendantes spécialisées chargées de surveiller les organes d'application de la loi et de renseignement ainsi que des évaluations indépendantes de l'efficacité mises en œuvre par les autorités compétentes elles-mêmes peuvent contribuer à une meilleure

[15] Klass et autres c. Allemagne, §§ 55 et 56 ; Kennedy c. Royaume-Uni, § 167.

transparence des pouvoirs et des compétences d'un système de PNR et à une plus grande responsabilisation.

En outre, il conviendrait de nommer des délégués à la protection des données au sein des instances chargées du traitement des données PNR, pour contrôler la conformité et la transparence du système (avec une évaluation régulière des risques en jeu et un audit systématique des PNR), le traitement et la communication des données, la mise à jour et la suppression des données, ainsi que les informations communiquées aux passagers. Les délégués à la protection des données pourraient également servir d'interlocuteurs en cas de plaintes ou autres demandes des personnes concernées. Ils sont encouragés à sensibiliser aux « bonnes pratiques ».

6. Conclusions

Compte tenu de l'atteinte particulière aux droits à la protection des données et à la vie privée que les mesures PNR peuvent représenter, la légalité, la proportionnalité et la nécessité d'un système PNR doivent être strictement respectées et démontrées, ce qui suppose notamment ce qui suit :

- une démonstration transparente et mesurable de la nécessité et de la proportionnalité du système au regard du but légitime poursuivi ;
- des définitions précises et strictes de l'objectif légitime poursuivi sont nécessaires et le traitement des données PNR ne doit être autorisé que pour des motifs limités et bien définis (prévention, détection, instruction et poursuite des infractions de terrorisme et autres infractions graves, ou dans des cas exceptionnels, prévention de menaces graves au public) ;

- une liste publique des autorités publiques compétentes (dans l'idéal, des unités de coordination spéciales) ;

- l'utilisation du « mode push » pour transmettre des données ainsi qu'une définition claire de la période de conservation initiale et des mesures de sécurité appropriées ;

- une interdiction de l'utilisation systématique des données sensibles ;

- une exploration des données limitée par des indicateurs de risque prédéfinis, avec un examen au cas par cas de la pertinence des résultats d'une manière non automatique ;

- des limitations uniquement nécessaires et prévues par la loi aux droits d'information, d'accès, de rectification et d'effacement dont jouissent les individus ;

- la compétence des autorités chargées de la protection des données (pouvant être consultées et habilitées à évaluer le système PNR et à traiter les plaintes individuelles) ;

- la disponibilité de voies de recours administratives et judiciaires effectives pour les personnes concernées ;

- un contrôle externe indépendant du système PNR ;

- un examen régulier du système PNR par les autorités compétentes.