COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Strasbourg, 30 septembre 2015

T-PD-BUR(2015)05

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

Rapport sur un projet d'avis sur les implications en matière de protection des personnes à l'égard de la transmission vers, et de leur traitement par des autorités publiques nationales ou étrangères, de données à caractère personnel relatives aux passagers aériens, contenues dans les listes des passagers dites API (Advanced Passenger Information» et dans leur dossier dit PNR (Passenger Name Record)

Le présent document contient un avant-projet d'avis élaboré par l'expert Mme Marie George. Il sera discuté lors de la 36e réunion du Bureau et sur la base des discussions une version révisée sera transmise au Bureau pour approbation.

Direction Générale Droits de l'homme et Etat de droit

Le Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (T-PD) a examiné, au regard des normes du Conseil de l'Europe en matière de protection des personnes à l'égard du traitement des données à caractère personnel, les questions soulevées de manière récurrente depuis les évènements du 11 septembre 2001, par les exigences des autorités publiques nationales et étrangères en matière de contrôles aux frontières réalisés sur la base de transmission de données relatives aux passagers (voyageurs), de leur exploitation et transmissions éventuelles ultérieures à d'autres autorités nationales ou étrangères, exigées des compagnies aériennes et des opérateurs de Système Informatisé de Réservation (SIR) aérien auxquels elles sont affiliées[1].Ces SIR assurent électroniquement sur le plan mondial la gestion des échanges d'information entre les compagnies et leurs partenaires, nécessaires à la gestion par chacun de la réalisation et du paiement des services qu'ils offrent et qui sont retenus par les passagers - agences de voyages, compagnies aériennes, banques et réseaux de cartes de crédit, loueurs de voitures et chaînes d'hôtels.

Le Comité est pleinement conscient des questions de sécurité des peuples qu'il incombe aux Etats de prendre en charge, liées aux personnes recherchées pour des motifs judiciaires ou de disparations de personnes, à la criminalité internationale du grand banditisme (narcotiques, armes, humains…), mais également à l'insécurité nationale et internationale aux conséquences dramatiques (morts de populations civiles, mouvements de populations cherchant refuge, émigrations massives), due à des attentats terroristes et conflits armés en extension tant en nombre que géographiquement, dont les origines tiennent à des radicalisations face aux inégalités économiques grandissantes et aux concurrences politico-économiques entre puissances, contexte dans lequel les pouvoirs des organisations régionales et internationales peinent à instaurer le développement équitable et la paix.

Le Comité estime que face à ces défis, des contrôles, en particulier aux frontières, doivent être facilités par le recours au (à des) traitement(s) automatisé(s) de données à caractère personnel relatives aux passagers, collectées de manière contraignante, en particulier auprès des compagnies aériennes qui les tiennent de leurs clients passagers aériens en fonction des services offerts et retenus pas les passagers. Ces transmissions et traitements par les autorités de contrôle aux frontières ne peuvent être légitimes que s'ils respectent, au risque d'aggraver la situation à court et moyen terme, les principes largement consacrés par la jurisprudence de la Cour européenne des droits de l'homme, fondée sur le droit international, la convention de sauvegarde des droits de l'homme et des libertés fondamentales, notamment son article 8 sur la protection de la vie privée et ses limitations, protection développée par deux textes en cours d'intégration et de modernisation, la convention no 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel et son protocole additionnel n° 181 de 2001 sur les transferts de données personnelles vers des pays tiers et sur les autorités de contrôle indépendantes.

Dans ce contexte et pour l'information et la réflexion de tous, le Comité estime nécessaire de préciser ce que l'on entend par la notion de « données des passagers » qui recouvre actuellement deux réalités différentes, parfois intégrées techniquement dans les Systèmes d'Information de Réservation (SIR). Il estime également nécessaire de tenir compte des enjeux pour l'Etat de droit liés au développement sans précédent de la numérisation massive de données dans la (es) société(s), et, pour les traiter y compris en matière de traitement des données des passagers, de certaines innovations mathématico technologiques mise en œuvre ou expérimentées, débouchant sur le profilage, y compris dynamiquement, des personnes concernées, selon leur niveau de risque présumé et des décisions étatiques qui peuvent en découler à leur encontre. Ces innovations suscitent d'ores et déjà des réflexions éthiques en particulier dans les milieux scientifiques.

[1] Systèmes Informatisés de Réservation (SIR) aérienne, en anglais « Computerized Reservation System (CRS) », qui préfèrent maintenant s'appeler "Global Distribution Systems (GDS)"),

I - Les données des passagers

I-1 *Les données dites « API- Advance Passenger Information »: forme, nature des informations, moment de leur collecte et par qui, finalités poursuivies par les autorités qui les exigent.*

Les catégories de données API ont été standardisées par l'Organisation de l'Aviation Civile Internationale (ICAO International Civil Aviation Organisation)[2] avec l' IATA (International Air Transport Association).

Les données sont collectées par les compagnies aériennes, au moment de l'enregistrement des passagers à l'aéroport.

Les listes de passager « API », comportent outre les n° de vol, lieux, dates et heures de départ et d'arrivée, les données suivantes provenant :

- des documents de voyage officiels présentés par les passagers (passeport, carte d'identité …) le cas échéant par lecture optique des deux lignes normalisées au bas du document dit « Machine Readable Zone (MRZ)» et comprennent : la nature et le numéro du document présenté, la nationalité, le nom, le ou les prénoms, la date de naissance de la personne, le pays de résidence, la date de validité du document ;
- du système d'information de la compagnie (ou de son SIR), l'indication automatique que les passagers prévus se sont présentés (show ; le passager non présenté sera automatiquement indiqué à la fermeture du vol comme « no show »), le numéro de sa place dans l'avion et les informations portées sur les étiquettes collées à leurs bagages,

Les listes de passagers ainsi constituées sont transmises aux autorités chargées du contrôle aux frontières au moment ou après fermeture du vol et en général avant le décollage de l'avion.

Selon IATA ; en 2015, 39 Etats requièrent les données API et 32 de plus le prévoit[3]

Dans l'Union européenne, à initiative de l'Espagne, suite à l'attentat de Madrid, le Conseil a adopté une directive en 2004[4] dont la transposition était exigée au plus tard le 5 septembre 2006

- rendant obligatoire, sous peine de sanction, la transmission aux autorités nationales de contrôle aux frontières extérieures, par les compagnies aériennes, de la liste de données correspondant à celle des données API des passagers entrant ou sortant de l'Union ;
- ayant pour finalité « d'améliorer le contrôle aux frontières extérieures et de combattre l'immigration illégale ».
- La modalité de transmission des données est celle du « pull » c'est à dire que ce sont les compagnies qui transmettent les données aux autorités, et non celle du « push » qui donnerait un accès direct aux autorités aux systèmes d'information de la compagnie.
- les Etats membres demeurent libres d'utiliser ces données à des fins répressives et sont libres d'appliquer ces obligations à d'autres transporteurs (maritimes, terrestres).
- Les autorités ne peuvent conserver les données que 30 jours sauf vis à vis des personnes soumises à des procédures répressives.

Le comité estime qu'en l'état de son information, et si les fichiers répressifs auxquels sont comparés les données API ont une base légale et sont mis en œuvre en conformité avec les textes du Conseil de l'Europe (y compris sa recommandation sur les fichiers de police), et qu'il en est de même dans l'Union européenne (notamment sur les fichiers Schengen sur les personnes recherchées et VIS sur les personnes ayant demandé un visa), les finalités poursuivies en Europe

[2] L'OACI fait partie du système de l'ONU. Elle a été créée en 1947 par la convention dite de Chicago. Elle comprend 191 Etats et développe avec les organisations des transporteurs aériens des normes et pratiques recommandées dont les Etats peuvent s'inspirer dans l'élaboration de leurs législations. Ces normes et pratiques font l'objet de formations et d'audits. http://www.icao.int/about-icao/Pages/FR/default_FR.aspx

[3] https://www.iata.org/whatwedo/security/facilitation/pages/index.aspx

[4] Directive 2004/82/CE du Conseil du 29 avril 2004 concernant l'obligation pour les transporteurs de communiquer les données relatives aux passagers Journal officiel n° L 261 du 06/08/2004

par le traitement des données API, sont légitimes, les données pertinentes et non excessives, les durées de conservations telles qu'indiquées dans le texte de l'UE, sont elles mêmes proportionnelles aux finalités poursuivies, sachant que les textes précités prévoient que les passagers sont informés et qu'ils peuvent exercer leurs droits, quelque soit leur nationalité ou leur lieu de résidence.

I – 2 Les données des dossiers des passagers dits « Passenger Name Record (PNR)

Les PNR sont collectées lors des réservations par les agences de voyages des compagnies aériennes ou accréditées par elles, transmises aux SIR, puis aux compagnies aériennes et à leur partenaires de location de voiture et hôtels à leurs propres fins.

Les catégories et sous catégories de données de réservation dans les dossiers des passagers PNR sont :
- standardisées de longue date et mise a jour par IATA (l'International Air Transportation Association), pour répondre aux demandes de réservations sur plusieurs vols de compagnies aériennes différentes ;
- utilisées de manière obligatoire (code et n° PNR, nom(s) et prénom(s), aéroport de départ et d'arrivée, dates et heures des vols et leur identification, information sur les paiements) ou selon les services offerts ou non par les compagnies et leurs partenaires;
- quelques catégories d'information sont à compléter en de texte libre.

Les données de réservations de vols sont indiquées par le passager (ou son représentant cf. cas notamment des groupes pour lesquels un seul code et n° PNR sera utilisé) en ligne ou à l'agence de voyages à laquelle il s'adresse (sur place ou par téléphone) qui les introduit dans le système informatisés de réservation auquel elle est affiliée, ce dernier les transmet aux autres SIR concernés. En effet dans le cas d'itinéraire de vols sur plusieurs compagnies recourant à des systèmes de réservations différents, les données qui les concernent sont transmises aux systèmes de réservation, accompagnées de la référence au code et numéro PNR attribué à l'origine.

Parmi les quatre plus grandes plateformes informatiques des plus importants SIR créés dans les années 80, seul celle d'Amadeus est localisée en Europe[5], les autres aux USA, Sabre, Galileo/Apollo, Worldspan. D'autres SIR sont apparus plus récemment en liaison avec la création les compagnies à bas coûts (low cost).

Les finalités de la collecte des données, de leurs transmissions et traitements par chacun des partenaires concernés, (agences, compagnies aériennes et partenaires au moyen des plateformes des SIR) sont :

- la confirmation (en ligne) de la(s) réservation(s) par l'agence avec indication du code et numéro du PNR ;
- la délivrance du ou des billets (en ligne, sur place ou par correspondance) par l'agence;
- la gestion des paiements des billets (en liquide, par remise de chèque et messageries ou réseaux interbancaires, par réseaux de cartes de crédit sur la base du n° de carte du passager), et des commissions aux agences.
- la mise à jour des dossiers PNR en cas de changements demandés par les passagers, et la mise à jour des comptes fidélité auprès de la compagnie concernée (n° de carte de fidélité)
- la communication automatique des réservations faites sur base du PNR d'origine aux éventuels autres compagnies/SIR concernés ;
- la transmission par les SIR et réseau, au moment opportun, des informations nécessaires aux partenaires pour la gestion de leurs services demandés, au système informatique de contrôle des compagnies aériennes pour la gestion des vols au départ et à l'arrivée et de leur logistique selon les services demandés ainsi que pour l'enregistrement des passagers.

[5] AMADEUS est le seul SIR possédé par des compagnies aériennes. Son siège est à Madrid, le service de recherche à Sophia Antipolis dans le sud de la France et la plateforme informatique à Munich). Amadeus est possédé et utilisé notamment par Air France, Iberia Airlines, Lufthansa. Scandinavian Airlines et plus de 60 autres compagnies de tous les continents y sont affiliés.

Le Comité constate que les données, collectées, dites PNR avant enregistrement des passagers à l'aéroport, sont de nature purement commerciales et paraissent sur le papier, strictement nécessaires à la mise en œuvre et aux paiements des services offerts et retenus par les passagers selon leurs seuls choix, par les compagnies aériennes et par leurs partenaires dans le cadre des déplacements des personnes (agences de voyages, location de voiture, hôtellerie).

Il estime, en l'absence de statistiques sur le sujet, que dans la très grande majorité des cas, les données à caractère personnel sont en nombre très limité. Mais ces données sont déjà intrusive et informative sur la vie des personnes/passagers concernés au regard de la liberté d'aller et venir, mais aussi de la vie privée s'agissant du moyen de paiement utilisé (liquide, chèque, n° de carte de crédit), des informations de contact (nom, téléphone fixe, mobile, e mail, adresse de facturation), de éventuel le numéro de carte de fidélité, du prix du billet, en plus des autres informations agence/ code agent, code et n° PNR, dates de réservation et de délivrance des billets, nom et prénom du passager, les vols aller ou aller et retour – code de la compagnie et n° de vol, dates et heures, aéroport de départ et d'arrivée -, n° de la place dans l'avion

Par ailleurs, le Comité estime que dans un nombre de cas vraisemblablement non négligeable, les données sont très intrusives à un titre ou un autre, ou cumulativement y compris concernant des données sensibles:

- en cas d'itinéraire complexe (plusieurs vols, sur les des compagnies différentes, sur plusieurs pays et continents différents), de mises à jour éventuelles (dont l'historique est conservé aux fins de régler d'éventuels réclamations),
- en cas de contraintes liées aux personnes et selon les services retenus indiqués dans le PNR sous les codes « Remarques générales », « OSI: Other service related information », « SSI: Special Services Information » et SSR: Special Service Requests » : handicapés en chaise roulante, aveugle ayant besoin d'aide, mineurs voyageant seuls, etc.)[6], choix alimentaires végétarien, hallal, casher, chambre de l'hôtel retenue et dates.
- ou encore en cas de réservations groupées sous un même PNR par commodité (noms et prénoms de personnes voyageant ensemble - en cas de voyage en famille, avec des collaborateurs de la même entreprise, ou en groupe, groupe touristique ou faisant référence, le cas échéant, au nom d'un syndicat ou d'un parti politique, d'une association à caractère politique ou religieux, le nom du groupe étant indiqué en texte libre, en particulier lorsqu'il a négocié des tarifs particuliers. Exemples d'une délégation d'un syndicat, d'un parti partant à un congrès, ou d'une association partant à la célébration d'une fête religieuse.

La durée de conservation des données dans les SIR, est dans AMADEUS de 3 mois après la fin de l'itinéraire réservé (pour répondre aux réclamations éventuelles), et paraît tout à fait raisonnable. Sur les autres plateformes le Comité ne dispose pas d'information. Dans les systèmes d'information interne aux compagnies, en Europe en fonction des standards de protection des données ces durées ne devraient pas dépasser le temps de la prescription pour la formation de recours commerciaux.

Le Comité, en l'état de son information, estime que les traitements de données à caractère personnel opérés par les partenaires à leurs seuls fins, ci dessus précisées, paraissent légitimes et proportionnés. Le Comité constate néanmoins que l'information des personnes et l'exercice de leurs droits d'accès, de rectification et de suppression et leur droit de recours, quelque soit leur nationalité et lieu de résidence, ne sont vraisemblablement garantis que vis à vis des traitements de données opérés par des compagnies, agences établis en Europe mais dont leur SIR est également établis en Europe, ou dans les pays tiers reconnus comme assurant un niveau de protection approprié.

[6] Autres sous codes standardisés, à la disposition des Compagnies aériennes, sous les codes Services Spéciaux Requis ou d'assistance dit SSR (Special Service Request) : chaise roulante normale (WCHR) ou y compris pour les escaliers (WCHS), confirmé à l'enregistrement (WCHC), déficient visuel, auditif, mental, usage d' un concentrateur d'oxygène (OXYG), siège supplémentaire EXST (personne obèse), allergies (NFCT pour Nut free Cabin Zone), ne parle pas la langue (LANG), service animaux en cabine (SRVA), enfant de moins de 12 ans, nom du tuteur au départ et à l'arrivée….

Dès lors, qu'il s'agisse des données en nombre limité, minimum mais déjà intrusives ou des données encore plus sensibles, le Comité estime qu'il est pertinent de se poser la question et d'interdire l'usage de ces données par un agent public, même sur ordre d'un supérieur hiérarchique, d'un Etat qui souhaiterait obtenir ces données aux fins de compléter les renseignements sur des personnes surveillées à des fins d'espionnage économique ou politique en particulier entre alliés (l'interdiction devrait être posée par la loi et la protection des lanceurs d'alerte assurée).

D'ores et déjà les Etats suivants exigent des données PNR : USA pour les vols internes et externes, en provenance de l'UE selon 4 accords successivement révisés de 2003 à 2012 qui prévoit en particulier le filtrage à l'arrivée et le masquage de données sensibles codifiées mais pas celles en texte libre, en provenance de l'UE vers le Canada et vers l'Australie selon deux accords qui prévoient en particulier la non transmission des données sensibles, la Nouvelle Zélande, la Corée du Sud, et en Europe le Royaume Uni, la France, le Danemark, la Belgique, la Suède ont adopté des législations nationales et procèdent à des mises en œuvre ou à des expérimentations…), la Russie l'a également prévu. En Amérique latine l'Argentine et le Mexique ont adopté des législations en ce sens. Selon IATA, en 2015 Le Brésil, le Japon et l'Arabie Saoudite seraient également concernés parmi les 30 Etats supplémentaires qui l'auraient prévu[7].

Au niveau de l'Union européenne une proposition de directive de la Commission de 2011[8] visant à imposer la communication de données du PNR pour tout vol à destination d'un pays tiers ou provenant d'un pays tiers à l'Union est à nouveau en négociation suite à l'attentat de Paris de janvier 2015, après une suspension due à un avis très négatif du point de vue de la nécessité et de la proportionnalité du Comité du Parlement européen, Liberté, sécurité, affaires intérieures. Sans attendre l'adoption de la directive, depuis 2012, 12 Etats membres ont bénéficié du financement européen pour la constitution de leur unité PNR prévu par la proposition de directive (Finlande, France, Estonie, Autriche, Lituanie, Suède, Pays bas, Roumanie, Portugal, Espagne, Slovénie, Hongrie)[9]. Sur l'état de la situation en 2015 (les initiatives et positions, institutionnelles, dont celles des autorités de protection des données, les pour les contre, la situation de certains Etats membres de l'UE, les analyses, il convient de consulter le site internet du service de recherche du parlement européen http://epthinktank.eu/2015/04/30/eu-pnr/.

II - L'analyse des données PNR au regard de leur transmission à des autorités publiques, et à l'usage qu'elles en font.

II-1 sur l'intrusion dans la vie privée de l'usage par des autorités publiques de données provenant des dossiers des passagers PNR

Dès lors, qu'un Etat demande à obtenir des données extraites des PNR des passagers allant ou quittant son territoire, qu'il s'agisse des données en nombre limité, minimum mais déjà intrusive ou des données encore plus sensibles, tel qu'indiqué au point I-2, et compte tenu des révélations depuis celles d'Edward Snowden en mai 2013 en matière d'espionnage par de multiples pays, le Comité estime qu'il est pertinent de se poser la question et d'interdire l'usage de ces données par un agent d'une autorité publique, même sur ordre d'un supérieur hiérarchique, à des fins d'espionnage économique ou politique, en particulier, entre alliés (interdiction devant être posée par la loi assortie de dispositions assurant la protection des lanceurs d'alerte).

II- 2 Sur les modalités de transmission des données

Les modalités de transmission aux Etats qui exigent des données du dossier passager PNR

[7] https://www.iata.org/whatwedo/security/facilitation/pages/index.aspx

[8] http://www.europarl.europa.eu/RegData/docs_autres_institutions/commission_europeenne/com/2011/0032/COM_COM(2011)0032_EN.pdf

[9] http://ec.europa.eu/dgs/home-affairs/financing/fundings/pdf/isec/isec-grants-awarded-2012_en.pdf#page=15

avant leur enregistrement à l'aéroport, ont ou ont eu recours, soit par la méthode du push (transmission par les SIR), soit la méthode du pull (accès des autorités directement à la plateforme du SIR.

A l'instar d'autres institutions européennes, le Comité estime que seule la méthode du pull est acceptable (elle est prévue par le dernier accord UE/US et dans la proposition de directive de 2011).

II- 3 Sur la relativité de l'amplitude et des révélations provenant d'un PNR au regard de la vie des personnes en situation problématique en cas de transmissions à des autorités publiques avant embarquement.

Le comité prenant en compte le fait que toutes les données PNR relèvent, bien normalement du strict choix du ou des passagers (itinéraire, choix alimentaire ou non etc.) souligne qu'une personne qui se sent dans une situation potentiellement problématique, par exemple vis à vis d'un acte passé ou futur de nature terroriste, adaptera ses choix et donc ses non - choix de manière à avoir un comportement le plus banal possible et protecteur de sa personne (réserver un aller et retour et non un aller simple à partir d'un pays différent de sa nationalité, faire des réservations pour plusieurs vols à partir de plusieurs agences, réserver ses vols non la veille du départ mais à l'avance, ne pas utiliser un moyen de paiement non liquide et habituel pour acheter des billets d'avion, ne pas demander une alimentation particulière etc.).

Une telle adaptation est également à prévoir en cas de départ et d'arrivée de plusieurs personnes qui sont en relation pour une même destination. Elles pourraient faire leurs réservations sous un même PNR, mais aussi préférer réserver leurs vols auprès de différentes agences, faire le voyage selon plusieurs itinéraires, à des dates distinctes.

Dès lors le Comité émet de sérieux doutes quant à la pertinence de données PNR qui seraient transmises à des Etats de manière systématique avant enregistrement pour détecter des personnes « à risque » et qui dépasseraient celles équivalentes prévues dans la liste des données API (à leur qualité « officielle » près).

II – 4 Sur les finalités poursuivies par les autorités publiques de contrôle selon les textes des accords bilatéraux et législation.

Les finalités telles qu'énoncées dans le 4ème accord entre l'UE et USA ou dans la proposition de directive européenne de 2011 paraissent raisonnables « la prévention et la détection d'infractions terroristes et d'infractions graves, ainsi que la réalisation d'enquêtes et de poursuites en la matière ou la prévention et la détection d'infractions terroristes et d'infractions transnationales graves (trafic d'humains, de drogue, d'armes), ainsi que la réalisation d'enquêtes et de poursuites en la matière ,[10]

Cependant des inquiétudes apparaissent lorsqu'il s'agit des usages autorisés pour identifiées des personnes dites « à risque », indépendamment des personnes identifiées préalablement comme liées au terrorisme, défini de manière très détaillée, ou à la criminalité internationale également définie tant dans le 4ème accord US/UE que dans la proposition de directive de 2011 mais comme pouvant être détectés par des traitements de données d'une autre nature.

Ainsi l'Article 4 du 4ème accord UE/USA prévoit que « 3. Les dossiers passagers peuvent être utilisés et traités parle DHS (Departement of Homeland Security) pour identifier les personnes qui feraient l'objet d'un interrogatoire ou d'un examen plus approfondis en arrivant aux États-Unis ou en quittant le pays, ou qui pourraient devoir faire l'objet d'un examen supplémentaire. Cette approche d'identification de personnes à rechercher, non par la connaissance préalable qu'en auraient les autorités, mais par des techniques de data mining et profilage, sur la base de critères ou sélecteurs fondés sur les cas passés, est prévue dans la proposition de directive de 2011. Il

peut d'agir aussi de processus dynamique (intelligence artificielle) ainsi que cela se pratique aux USA. La proposition de directive européenne prévoit à l'article 4.2.a) et d) que l'unité de renseignement passagers, indépendamment du croisement avec les fichiers Schengen et VIS prévu par ailleurs, peut effectuer des traitements pour « procéder à l'évaluation du risque représenté par les passagers avant leur arrivée prévue dans l'État membre ou leur départ prévu de celui-ci, afin d'identifier les personnes qui peuvent être impliquées dans une infraction terroriste ou une infraction transnationale grave "…. "analyser les données PNR aux fins de mettre à jour ou de définir de nouveaux critères pour la réalisation d'évaluations en vue d'identifier toute personne pouvant être impliquée dans une infraction terroriste ou une infraction transnationale grave conformément au point a)".

Le problème de l'usage de ces techniques pour cibler en pratique une partie très infime d'une population (le pourcentage des voyageurs terroristes ou criminelles est très faible au regard du nombre de voyageurs) est qu'il conduit, ce que les statisticiens et épidémiologistes savent bien, à identifier un fort tôt de "faux positifs" (personnes ne présentant pas de risques en pratiques) et à ne pas identifier un fort taux de "faux négatifs" (personnes présentant en pratique des risques). [11]

Dès lors, on imagine les difficultés majeures que les personnes interrogées à tord à l'aéroport ou surveillées à tord, aurons à prouver l'abus de pouvoir des autorités , malgré la décision humaine prise (et prévue dans ces textes) lorsque les critères évoluent manuellement ou en temps réel et dynamiquement. Dès lors est à souligner le caractère d'imprévisibilité probable de telles approches contraire à la jurisprudence de la CEDH.

Enfin le Comité, tout comme d'autres institutions européennes, est impressionné par l'absence d'informations rendues publiques démontrant l'efficacité dans le temps des techniques de profilage appliquées à des données PNR en indiquant par exemple le nombre de passagers contrôlés, le nombre des personnes ainsi suspectées, le nombre de celles interrogées à tord relevant de la catégorie des " faux positfs", le nombre de personnes suspectées ayant été ainsi arrêtées, le nombre de celles ayant été condamnées pour terrorisme ou activité criminelle internationale.

En conclusion sur les données PNR, le Comité considère au titre de la pertinance très relative des données des passagers PNR dès lors qu'ils se savent en situation de suspicion possible, et des résultats auxquels conduisent la recherche de personnes dangereuses potentiellement sur la base des techniques de profilage automatique, qu'au delà de la liste des données de type API contenues dans le PNR qui peut être transmise quelques heures avant le départ d'un avion, la transmission systématique aux autorités publiques d'autres données des PNR, même après retrait des données sensibles, est tout à la fois disproportionnée. . Il peut en découler l'inefficacité de la mesure. On ne peut en outre exclure un risque d'abus de pouvoir dans contexte d'imprévisiblité.

Conclusions

Le Comité est d'avis que

- La détection pro - active de personnes potentiellement suspectes par l'application aux données

[11] Sur les questions de faux positifs et de faux négatifs, consulter le "Security blog" de l'expert en sécurité Bruce Schneier Why Data Mining Won't Stop Terror, 3 September 2006, at: http://www.schneier.com/blog/.
- Douwe Korff, Technologies for the Use of Images: Automated Processes of Identification, Behavioural Analysis and Risk Detection Control at the Airports (2010), presented at Spanish Data Protection Agency Seminar, Madrid, Spain, 9-11 June 2010. Available at SSRN: http://ssrn.com/abstract=1977874
- Le rapport élaboré pour le comité de la convention 108 du Conseil de l'Europe " Passenger Name Records, data mining & data protection: the need for strong safeguards, by Douwe Korff, *Emeritus Professor of International Law*,London Metropolitan University Associate, Oxford Martin School, University of Oxford, with advice, comments and review by Marie Georges, *Council of Europe Expert, June 16, 2015*

PNR et API de techniques automatisées sur base de critères de suspicion, mis à jour régulièrement ou dynamiquement, par référence à des concomitances entre des données caractérisant les personnes ou leurs voyages, à celles de terroristes ou criminels avérés dans le passé, doit être considéré comme disproportionnée, inefficace dans le domaine considéré, contraire aux droits de l'homme par l'importance des faux positifs auxquels elle donne lieu et à son caractère d'imprévisibilité pour les personnes concernées, même avec l'assistance d'un avocat expert.

- En application des normes du Conseil de l'Europe en matière de dérogation ou limitation du droit à la protection de la vie privée et de la liberté d'aller et venir à une fin légitime, nécessaire et proportionnée dans une société démocratique, une telle dérogation ou limitation doit être établie par une législation claire, précise, prévisible et ne portant pas à l'essence du droit et de la liberté en cause en prévoyant au minimum les conditions suivantes :

  - Seule peut être transmise aux autorités de contrôle aux frontières avant enregistrement à l'aéroport, par les compagnies aérienne, en provenance de leur système interne de contrôle ou de leur SIR d'affiliation, la liste des passagers prévus pour un vol entrant ou sortant du territoire assortie de données extraites des dossiers PNR, comportant le code et numéro PNR, le code compagnie et numéro de vol, les dates et heures du vol au départ et à l'arrivée aux aéroports de départ et d'arrivée, l'identité des passagers prévus (noms et prénoms) ;
  - cette liste doit être complétée et mise à jour après enregistrement à l'aéroport par la liste des données officielles API des passagers extraites de leur document de voyage (personne enregistrée, n° de place dans l'avion, nature et n° du document, nationalité, nom et prénom, date de naissance), au mieux transmise par la compagnie concernée au moment de la fermeture du vol.

  - Les deux listes précitées doivent être transmises (méthode du push) par les compagnies à l'autorité de contrôle des frontières et de manière chiffrée.

  - Les données ne peuvent servir qu'à être comparées aux listes ou fichiers, tenus à jour très régulièrement, et créés en vertu, dans les Etats membres du Conseil de l'Europe, de la législation nationale ou de l'Union européenne, relatifs aux catégories de personnes suivantes : personnes interdites judiciairement de sortie de territoire ou d'entrée sur le territoire, personnes recherchées judiciairement, personnes déclarées disparues par leur famille, personnes faisant l'objet d'un suivi sur la base d'indices graves et concordant les rendant suspectes d'implication dans des activités de terrorisme, ou dans des activités de criminalité internationale grave.
  La liste des fichiers concernés doit être rendue publique, toutes les activités et actes criminels graves doivent être définies clairement et précisément ainsi que leurs conséquences pénales dans la législation concernée, les délits mineurs doivent être explicitement exclus.

  - Fin d'éviter la société de surveillance compte tenu du nombre grandissant de passagers aériens, après comparaison en temps réel et décisions humaines prises sur la base des résultats, les données doivent être supprimées dans un délai inférieur à un mois, sauf investigation ou de poursuite judiciaire, ou de suivi légalement autorisé par un juge ou une autorité indépendante.

  - En cas de suivi légalement autorisé, d'investigation ou de poursuite judiciaire, l'autorité de contrôle aux frontières doit détenir légalement le pouvoir d'obtenir, si nécessaire et demandée par l'autorité concernée, les autres données du dossier PNR concerné.

  - Les fichiers, transmissions et traitements, ci dessus visés, doivent faire l'objet pour la conception leur comparaison aux données de type API,
    - d'une coopération entre les différents services concernés adaptée aux finalités poursuivies et
    - d'une consultation préalable à leur création de ou des autorités indépendantes de contrôle de la protection des données compétentes, ainsi que de contrôles a postériori par celles ci dont les résultats sont rendus publics.

- Les fichiers doivent également faire l'objet de mise à jour très régulièrement, et, de même que ceux des acteurs du transport aérien impliqués,
    - de contrôles internes de la conformité et de sécurité relative à la disponibilité des données, à la confidentialité et l'intégrité des données en interne (chiffrement et consignation de tous les accès) et en transmission (chiffrement) ;
    - de la désignation d'un délégué chargée du contrôle de la protection de données et de la sécurité ;
    - et régulièrement d'audits.

- Les passagers doivent être informés au moment des réservations et de l'enregistrement à l'aéroport de l'existence de ces transmissions, fichiers et traitements, des autorités destinataires des données selon quelles circonstances, de leur durée de conservation et de l'existence de leurs droits.

- Les passagers concernés, doivent, quelque soit leur nationalité ou leur pays de résidence, disposer des droits garantis d'accès, de correction et de suppression des données conservées par chacune des autorités concernées, et de recours auprès de l'autorité indépendante de contrôle de la protection des données ainsi qu'auprès de la justice.

- L'autorité de contrôle aux frontières doit établir et rendre publique chaque année aux fins de transparence démocratique,
    - le nombre de voyages effectués en entrée et sortie du territoire,
    - le nombre de personnes interrogées à l'occasion du contrôle aux frontière du fait du résultat des comparaisons de listes et fichiers effectués, selon leur nationalité aux fins du contrôle de la non-discrimination, et des objets des interrogatoires,
    - le nombre de personnes dont des données PNR et API ont été conservées dans le cadre de suivis légalement autorisés, d'investigations et de poursuites judiciaires selon leurs objets et la nationalité des personnes concernées.

- En cas de transmission de données API et PNR vers des pays tiers, les accords internationaux bilatéraux ou multilatéraux doivent comporter l'ensemble des mesures ci dessus prévues et faire l'objet préalablement à leur adoption par les parlements concernés, de la consultation des autorités indépendantes de protection des données dont l'avis est rendu public. Ces mesures doivent viser les données relatives à tous les passagers, quelque soient leur nationalité et pays de résidence, en provenance ou à destination de leurs territoires quelque soit la localisation des données API et PNR.

- Les transmissions de données de PNR et API entre autorité nationale et autorités de pays tiers doivent faire l'objet d'autorisations d'un juge ou d'une autorité indépendante ainsi que de contrôle a posteriori et d'une transparence annuelle.

- La législation nationale et les accords internationaux précités, doivent prévoir l'interdiction pour les agents des services recevant des données de passagers, même sur ordre de leur supérieur, d'utiliser ou de transmettre des données à des fins d'espionnage économique ou politique entre pays alliés. La révélation de telles pratiques d'espionnage ne doit pas porter préjudice aux personnes qui les révèlent publiquement.