



UNIVERSITÉ D'AIX-MARSEILLE
FACULTÉ DE DROIT ET DE SCIENCE POLITIQUE

PÔLE TRANSPORTS
INSTITUT DE FORMATION UNIVERSITAIRE ET DE RECHERCHE DU TRANSPORT
AÉRIEN (IFURTA)

L'IMPLÉMENTATION INTERNATIONALE DES UNITÉS
D'INFORMATION PASSAGERS

Mémoire pour l'obtention du
Master 2 Droit et Management du Transport Aérien

par

Niels THIMON

Sous la direction de Madame Le Professeur Julie LABORDE DIT BOURIAT

Année universitaire 2020-2021



UNIVERSITÉ D'AIX-MARSEILLE
FACULTÉ DE DROIT ET DE SCIENCE POLITIQUE

PÔLE TRANSPORTS
INSTITUT DE FORMATION UNIVERSITAIRE ET DE RECHERCHE DU TRANSPORT
AÉRIEN (IFURTA)

L'IMPLÉMENTATION INTERNATIONALE DES UNITÉS
D'INFORMATION PASSAGERS

Mémoire pour l'obtention du
Master 2 Droit et Management du Transport Aérien

par

Niels THIMON

Sous la direction de Madame Le Professeur Julie LABORDE DIT BOURIAT

Année universitaire 2020-2021

REMERCIEMENTS

Je souhaite avant tout remercier ma directrice de mémoire, Madame le Professeur Julie LABORDE DIT BOURIAT pour m'avoir fourni les outils nécessaires à la réussite de mon année universitaire ainsi que ma directrice d'alternance, Madame Fabienne CASTELLI-MAUDOUX pour sa confiance et son encadrement professionnel.

J'adresse ma reconnaissance aux professionnels de la BelPIU, d'AIRCOP et de l'UNODC ayant accepté de répondre à mes questions et de me transmettre leur expérience.

Je tiens à également à exprimer ma gratitude aux intervenants et au Secrétariat du Pôle Transports de l'Université Aix-Marseille et à la Direction des Affaires Juridiques d'Air France, grâce à laquelle j'ai pu m'épanouir professionnellement et humainement durant cette année.

À mes proches, pour leur soutien, leurs conseils et leur bienveillance.

SOMMAIRE

<i>Introduction</i>	8
<i>PARTIE 1- L'ÉMERGENCE ET L'ÉLABORATION DES UIP À L'INTERNATIONAL SUR LE MODÈLE EUROPÉEN</i>	15
SECTION 1- L'évolution du modèle de collecte des données passagers rendue nécessaire par le contexte international	15
I. Les premiers textes normatifs européens vers la création des UIP	15
II. La coopération au service de l'exportation du modèle européen à l'international.....	23
SECTION 2- Les défis structurels et légaux de l'implémentation du modèle des UIP au sein des États	32
I. Le manque de clarté des procédures de récupération des données passagers	32
II. Le manque de sécurité dans l'exploitation des données et leurs transferts	41
<i>PARTIE 2- L'ADAPTATION DU MODÈLE DES UIP À LA RECHERCHE D'UN SYSTÈME HARMONISÉ ET PERFORMANT</i>	47
SECTION 1- L'encadrement de la pratique des États et la prise en compte de leurs spécificités nationales	48
I. Le respect de la souveraineté des États en parallèle de la mise en place d'un modèle commun.....	48
II. L'importance de garanties et mesures pour le respect des bonnes pratiques des États	53
SECTION 2- L'harmonisation des pratiques au support d'un système d'UIP fiable et exportable	60
I. La composition de l'UIP comme variable importante dans la recherche d'une efficacité accrue	60
II. Les différentes opportunités d'application pratique d'un modèle fonctionnel d'UIP	65
<i>Conclusion</i>	72

TABLE DES ABRÉVIATIONS ET SIGLES UTILISÉS

§ : Paragraphe

AGNU : Assemblée Générale des Nations Unies

AIRCOP : Programme de coopération aéroportuaire

API : *Advanced Passenger Information*/Données passagers avancées

art. : Article

CEDH : Cour Européenne des Droits de l'Homme

cf. : *Conferatur*

chap. : Chapitre

Conv. : Convention

Conv. EDH : Convention Européenne des Droits de l'Homme

CSNU : Conseil de Sécurité des Nations Unies

CTITF : *Counter-Terrorism Implementation Task Force*/Équipe spéciale de lutte contre le terrorisme

Dir. : Directive

EES : *Entry/Exit System*/Système d'Entrée/Sortie

ETIAS : *European Travel Information and Authorization System*/Système européen d'information et d'autorisation de voyage

EUROPOL : Agence européenne de police criminelle

iAPI : *Interactive Advanced Passenger Information*/ Données passagers avancées interactives

IATA : *International Air Transport Association/ Association Internationale du Transport Aérien*

Ibid. : *Ibidem*

IMO : *International Maritime Organization/Organisation maritime internationale*

INTERPOL : Organisation internationale de police criminelle

OACI : Organisation de l'Aviation Civile Internationale

OICT : *Office of Information and Communications Technologies/Bureau des technologies d'information et de communication*

ONU : Organisation des Nations Unies

ONUCT/UNOCT : Bureau de lutte contre le terrorisme

ONUDD/UNODC : Office des Nations Unies contre la drogue et le crime

OSCE : Organisation pour la sécurité et la coopération en Europe

p. : Page

PAXLST : *Passenger list message/Message de liste passagers*

PDSW : *Passenger Data Single Window/Fenêtre Unique pour les données passagers*

PNR : *Passenger Name Record/Dossier au nom du passager*

pp. : Pages

Res. : Résolution

RGPD : Règlement Général sur la Protection des Données

SARP : *Standards and Recommended Practices/Standards et pratiques recommandées*

SIS : Système d'Information Schengen

TRIP : *Traveller Identification Programme*/Programme d'identification voyageur

TUE : Traité sur l'Union Européenne

UIP : Unité d'information Passagers

UNCCT/UNCTT : *United Nations Counter-Terrorism Centre*/Centre des Nations Unies pour la lutte contre le terrorisme

UNSCR : *United Nations Security Council Resolution*/Résolution du Conseil de Sécurité des Nations Unies

USAP : *Universal Security Audit Programme*/Programme universel d'audits de sûreté

VIS : *Visa Information System*/Système d'information sur les visas

WCO : *World Customs Organization*/Organisation mondiale des douanes

INTRODUCTION

“Le développement futur de l’Aviation Civile internationale peut grandement aider à créer et à préserver entre les nations et les peuples du monde l’amitié et la compréhension, alors que tout abus qui en serait fait peut devenir une menace pour la sécurité générale”¹

I. Le développement de l’aviation et des actes lui portant atteinte

1. La croissance rapide de l’aviation

L’Histoire fait remonter les sources de l’aviation moderne au début du 20^e siècle à la suite du tout premier vol motorisé réalisé le 17 Décembre 1903 par Orville et Wilbur Wright, autrement connus comme les Frères Wright. L’Histoire de l’aviation entendue comme la navigation aérienne par avion est donc récente. Le constat selon lequel entre 1903 et 2021, la société humaine passa de ses premiers individus sur un engin volant motorisé au transport de plusieurs millions d’individus quotidiennement à travers le monde démontre bien une évolution rapide et efficace du transport aérien. Cette évolution fut notamment accélérée par la Première Guerre Mondiale et la mise en place de ses troupes aéroportées qui représentaient un atout majeur lors des conflits. L’entre-deux guerres permit un fort essor du développement et de la recherche en matière aéronautique, qui se maintiendra durant la Seconde Guerre Mondiale, marquée par de constantes innovations en termes d’aéronefs.

2. L’exploitation des failles causées par cette croissance soudaine

C’est durant la Seconde Guerre Mondiale que s’observèrent les premiers comportements qui constitueront les infractions pénales et crimes sérieux aujourd’hui condamnés par les textes internationaux. Hors situation de guerre, la doctrine fait remonter les premières occurrences de détournements

¹ Conv. Chicago, Considérant 1 du préambule.

d'appareils aux années 1930. Alors encore rares, ces actions illicites connurent une démultiplication dans les années 70 avec les premières actions de plus grande létalité consistant en la prise d'otages et la destruction de ces appareils.

Les vols Swissair 330 et Aeroflot 109 respectivement du 21 Février 1970 et du 18 Mai 1973 en sont de graves exemples, des engins explosifs ayant été déclenchés d'un côté par le groupuscule FPLP², de l'autre par un individu isolé. Ces actes, précédés et succédés par d'autres, firent prendre conscience à la communauté internationale que le transport aérien était vulnérable au terrorisme et autres infractions sérieuses, notamment du fait de son rôle principal dans la mondialisation et le développement des échanges entre les États.

3. Les premières réponses internationales aux actes illicites contre l'aviation

Ce fut entre les années 1960 et 1970 que les premiers grands textes internationaux en la matière virent le jour. Ces actes illicites firent ainsi l'objet d'une réglementation en 1963 par la Convention de Tokyo³ concernant la capture illicite d'aéronefs civils en vol puis en 1970 par la Convention de la Haye⁴ et en 1971 par la Convention de Montréal⁵ ainsi que son protocole de 1988⁶ allant dans le sens d'un élargissement de sa portée et en réaffirmant l'importance.

Les organes internationaux chargés de la guidance des États et des politiques communes s'adaptèrent également aux nouvelles méthodes criminelles employées. Ainsi la Convention de Montréal de 1991⁷ vit elle le jour afin d'intensifier la capacité de détection de nouveaux types d'explosifs.

² Front Populaire de Libération de la Palestine.

³ Convention relative aux infractions et à certains autres actes survenant à bord des aéronefs, 14 Septembre 1963.

⁴ Convention pour la répression de la capture illicite d'aéronefs, 16 Décembre 1970.

⁵ Convention pour la répression d'actes illicites dirigés contre la sécurité de l'aviation civile, 23 Septembre 1971.

⁶ Protocole pour la répression des actes illicites de violence dans les aéroports servant à l'aviation civile internationale, 24 Février 1988.

⁷ Convention sur le marquage des explosifs plastiques et en feuilles aux fins de détection, 1^{er} Mars 1991.

II. Le déclencheur et l'accélération de la coopération internationale

1. Le 9/11 comme symbole de vulnérabilité du transport aérien

La communauté internationale s'organisait alors davantage selon une logique réactive de lutte contre le terrorisme et autres crimes sérieux en détaillant les régimes de sanction plutôt que selon une logique préventive. Les attaques coordonnées revendiquées par Al-Qaïda des tours jumelles du World Trade Center de New-York du 11 Septembre 2001 marquèrent un tournant dans l'histoire du terrorisme, de sa visibilité et de la prise de conscience de son imprévisibilité. Elles témoignèrent également de l'évolution de la menace par voie aérienne, les actions contre les aéronefs étant progressivement passées du stade de la prise d'otage et dégâts matériels à la dégradation en vol et à présent, à l'utilisation de l'aéronef comme une arme.

2. Le renforcement des formes de coopération entre États

Une telle désolation à l'aube de ce nouveau millénaire marqua les esprits et incita à davantage de coopération internationale pour lutter et éviter une recrudescence de ces tragédies. Les textes internationaux continuèrent d'être adoptés comme la Convention de Beijing⁸ de 2010 ainsi que son protocole⁹ la même année venant compléter les Convention précédemment établies et portant sur le même thème ou encore le protocole de Montréal¹⁰ de 2014. Des accords bilatéraux entre États commencèrent également à voir le jour en la matière.

⁸ Convention sur la répression des actes illicites dirigés contre l'aviation civile internationale, 10 Septembre 2010.

⁹ Protocole additionnel à la Convention de Beijing, 10 Septembre 2010.

¹⁰ Protocole portant amendement de la Convention relative aux infractions et à certains autres actes survenant à bord des aéronefs, 04 Avril 2014.

En parallèle de ces textes, des initiatives furent progressivement mis en place pour aller dans le sens de plus de sécurité et de sûreté du transport aérien vis-à-vis du terrorisme principalement, mais également des autres crimes et infractions pénales telles que les trafics en tout genre. Ces trafics concernent ainsi et de manière non exhaustive les drogues, êtres humains, organes, faune et flore protégées, armes ou encore biens culturels. La criminalité organisée profite du développement rapide du transport aérien et des flux importants entre États.

L'efficacité du droit international public repose sur la capacité des États à mettre en œuvre leur droit dans le respect de celui des autres États et sur leur capacité à poursuivre un objectif commun de manière harmonisée. Une initiative naquit en Europe de la volonté des États d'assurer une analyse en amont des données passagers reçues par les transporteurs aériens afin de pouvoir mieux appréhender des profils de voyageurs et tenter de déceler les infractions pénales avant qu'elles ne se déclarent.

III. L'étude d'un exemple du fruit de la coopération internationale contre le terrorisme et autres crimes sérieux

1. L'intérêt des Unités d'Information Passagers

Cette initiative, aujourd'hui connue sous le nom d'Unité d'Information Passager, s'est formée progressivement en Europe à travers divers textes de loi de différentes époques et les Organismes Internationaux tentent de l'ériger en standard à travers les États. Grâce à un Programme des Nations Unies, le nombre de ses États membres bénéficiant d'aide pour l'implémentation de ce système dans leur droit national s'élève à 42.

Les textes européens encouragent à ce que ces UIP soient le seul système en place au niveau national pour pouvoir recevoir les données des transporteurs aériens aux fins de conservation, analyse, traitement et transferts aux entités

habilitées à les recevoir. Elles travaillent conjointement avec les agences nationales de lutte contre la criminalité et autres entités internationales. Ce principe de canal unique fut pensé pour pallier à un système de récolte des données passagers encore très variable, peu réglementé et mal défini parmi les États.

Cette multiplication des schémas de système existant est un frein à une détection efficace des passagers posant un risque pour la sûreté et la sécurité de l'aviation civile.

Le fonctionnement de ces unités s'inscrit dans une logique de prévention de la criminalité par l'analyse des données API et PNR en amont du voyage. Les données API, Advanced Passenger Information, sont récoltées par lecture automatisée des documents de voyages ou par entrée manuelle de ces données par le passager ou le personnel aéroportuaire. Basées sur des documents officiels, elles sont considérées comme fiables.

Les données PNR, Passenger Name Record, sont quant à elle les données récoltées au moment de la réservation par le passager. Ce sont des informations supplémentaires qu'il transmet et qui peuvent entre autres renseigner le nombre de voyageur avec lui, les moyens de paiement utilisés, le parcours réalisé ou encore les demande de services particuliers à bord.

Par la vérification de ces deux types de données contre des listes de surveillance internationales ou par leur analyse en fonction de critères précis, les UIP seront en mesure de déceler des comportements à risque ou d'identifier des criminels suspectés ou avérés. Ces unités constituent l'objet d'étude de ce mémoire.

Afin qu'elles puissent fonctionner le plus correctement possible et tendre vers la finalité qui leur a été désignée, il est important d'étudier les faiblesses de leur régime pour en dégager des axes d'amélioration. De leur capacité à accomplir leur mission dépend la sécurité et la sûreté internationales.

2. La délimitation du cadre de la réflexion

Le cadre de la lutte contre le crime transnational est large et regroupe de nombreuses offenses à la loi. Selon les termes des textes les ayant institués, les UIP ont pour but de soutenir la lutte pour la prévention et la détection des infractions terroristes et des formes graves de criminalité ainsi que les enquêtes et poursuites en la matière.

Cette étude exclura l'analyse et la réflexion autour des actions prises par les autorités compétentes ayant reçues des données de la part des UIP. Le volet judiciaire relatif à l'appréhension de ceux ayant enfreint la loi et leur procès n'apparaîtra pas dans ce devoir. Les UIP récoltant des données passagers des transporteurs aériens, il ne sera donc pas fait mention des flux de fret/cargo.

3. Problématique et annonce de plan

La présente analyse proposera de mettre en lumière les défauts et blocages dans le réalisé des missions des UIP et d'apporter une réflexion sur les manières de fluidifier et rendre plus efficaces ces systèmes.

Cela en simplifierait l'implémentation dans les pays souhaitant en être bénéficiaires et tendrait vers une harmonisation et une standardisation bénéfique à la lutte contre les infractions terroristes et formes graves de criminalité.

Il existe toujours un amas de règles, normes, recommandations et pratiques relatif à la mise en place des UIP ou d'un système similaire de récolte de données passagers.

Ce manque de clarté mène à des interprétations et des transpositions dont le résultat varie selon les États. Les données passagers étant sensibles, et les structures d'accueil de ces données n'étant pas toujours bien définies, les transferts d'informations, nécessaires pour une coopération et une coordination interétatique optimale, peuvent être paralysés. Des mauvaises pratiques et des structures non adaptées à recevoir ces données peuvent même constituer des atteintes aux droits fondamentaux des personnes.

Un autre défi du modèle a attrait aux particularismes des États et à leur capacité à pouvoir travailler à la mise en place d'un standard international tout en étant en mesure de continuer à exercer leur souveraineté sur leur territoire. Certains États ayant déjà des politiques nationales de Défense définies pourraient décider de continuer ainsi par choix ou bien par obligation car ils ne peuvent pas adapter les recommandations internationales à leur modèle.

Ce document propose une réflexion sur les UIP par l'étude de l'équilibre entre l'harmonisation d'un nouveau standard et l'adaptation des régimes nationaux déjà en place.

Une première partie sera consacrée à l'analyse de l'émergence du modèle de l'UIP et de ses principaux défis en matière organisationnelle et réglementaire tandis qu'une seconde partie questionnera la nécessité d'une redéfinition du modèle pour le rendre plus adapté aux réalités internationales.

PARTIE 1- L'ÉMERGENCE ET L'ÉLABORATION DES UIP À L'INTERNATIONAL SUR LE MODÈLE EUROPÉEN

Les Unités d'information passagers sont nées du souhait de la communauté internationale de lutter contre la menace terroriste, alors en plein essor, ainsi que la survenance d'autres infractions sérieuses, de plus en plus fréquentes et variées, favorisées par la croissance du trafic aérien. Leur dénomination officielle et description de leur mode de fonctionnement est attribuable à l'Union européenne.

Ce modèle s'est ensuite progressivement exporté hors de l'Europe où il a continué à être développé et adapté par les États l'implémentant. Ces unités voient leur fonctionnement basé sur l'interprétation de textes normatifs de différentes époques. Du fait d'un manque de source normative unique et par l'évolution du contexte international de sécurité et sûreté, irrégularités et difficultés viennent entraver le bon déroulement de leur mission.

SECTION 1- L'évolution du modèle de collecte des données passagers rendue nécessaire par le contexte international

Le développement rapide des échanges et déplacements par voie aérienne ainsi que l'absence de garanties bien établies pour la sécurité et la sûreté de ce mode de transport permirent la ramification des réseaux de criminalité organisée sur ces nouveaux axes. La communauté internationale se saisit de la question et développa progressivement un ensemble de normes autour du trafic aérien, notamment passager. Les principes qui allaient constituer les UIP comme décrites aujourd'hui dans les textes internationaux se retrouvèrent rapidement dans le corpus juridique de l'Union européenne grâce à ce système de coopération étatique déjà bien en place.

I. Les premiers textes normatifs européens vers la création des UIP

Le Conseil et le Parlement européen sont les principaux organes à l'origine du corpus normatif de l'Union Européenne sur le sujet des UIP. Cette production légale s'est progressivement mise en place d'abord par le biais de la formulation de conseils aux États membres pour ensuite vêtir un caractère de plus en plus obligatoire à travers deux directives principales, la directive API et la directive PNR.

A. L'identification d'une nouvelle nécessité par les organes de l'Union européenne

Le corpus juridique ayant mené à la création des Unités d'Information Passagers telles qu'elles sont aujourd'hui fut développé en Europe par le Conseil de l'Union européenne, organe regroupant les chefs d'États ou de gouvernements des membres de l'Union Européenne, et le Parlement Européen.

La directive 95/46/CE « *relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données* »¹¹ du 24 Octobre 1995 est venue préciser et compléter les termes de la Convention « *pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel* » du 28 Janvier 1981¹². Cette directive de 1995 prévoyait déjà que le développement du marché intérieur allait « *nécessairement entraîner une augmentation sensible des flux transfrontaliers de données à caractère personnel entre tous les acteurs de la vie économique et sociale des États membres* »¹³. Le besoin d'encadrer le traitement de ces données s'est donc fait ressentir. Le contexte international de l'époque n'étant pas le même que celui de nos jours, la finalité de ces deux textes ne portait pas encore sur le traitement de données dans une optique de lutte contre les offenses criminelles. Il s'agissait même du contraire, la directive 95/46/CE excluant de son champ d'application les « *traitements ayant pour objet la sécurité publique, la défense, la sûreté de l'État* ». ¹⁴ L'un des

¹¹ Dir. 95/46/CE du Parlement européen et du Conseil, 24 Octobre 1995. Remplacée par le RGPD.

¹² Conv. du Conseil de l'Europe, 28 Janvier 1981.

¹³ Dir. 95/46/CE du Parlement européen et du Conseil, du 24 Octobre 1995, §5 p.1.

¹⁴ Ibid. art.3.2.

apports de ces textes fut l'importance à accorder au « rapprochement des législations »¹⁵ afin de permettre la bonne circulation de ces données et garantir un niveau de protection de leur traitement « équivalent dans tous les États membres »¹⁶.

Sans le nommer, la directive de 1995 évoque le « responsable du traitement » comme « une administration publique ou une autre personne soumise au droit public ou au droit privé »¹⁷. Ses attributions formèrent les contours du système que nous connaissons aujourd'hui sous le nom d'Unité d'Information Passagers.

Les 25 et 26 Mars 2011, le Conseil, par le biais de deux déclarations, a recentré le travail de l'Union sur la nécessité de coopération entre États et la lutte contre le terrorisme. Ces déclarations reprennent en les complétant les *Conclusions et plan d'action du Conseil Européen extraordinaire* du 21 Septembre 2001 présentés à la suite des attentats terroristes du 11 Septembre aux États-Unis.

La Déclaration du Conseil européen sur le terrorisme du 25 Mars 2004 fit suite aux attentats de Madrid du 11 mars 2004, les plus meurtriers d'Europe avec ceux de Lockerbie en Ecosse en 1988. Le Conseil Européen a ainsi appelé les États à prendre des mesures législatives en adoptant notamment les décisions-cadres relatives au mandat d'arrêt européen ou encore celle relative à « l'application de mesures spécifiques de coopération policière et judiciaire en matière de lutte contre le terrorisme ».¹⁸ et a « [chargé] le Conseil d'envisager des mesures dans [des] domaines [tels que la] (...) simplification de l'échange d'informations et de renseignements entre les services répressifs des États membres. ».¹⁹ Il a également appelé au renforcement des bases de données relatives à la criminalité organisée internationale, la cybercriminalité et au terrorisme telles qu'Europol²⁰.

¹⁵ Ibid. §8 p. 2.

¹⁶ Ibid. §8 p. 2.

¹⁷ Ibid. §32 p. 4.

¹⁸ Déclaration du Conseil européen sur le terrorisme, 25 Mars 2004, art. 5.

¹⁹ Ibid.

²⁰ Agence Européenne spécialisée dans la répression de la criminalité.

« La proposition de directive du Conseil concernant l'obligation pour les transporteurs de communiquer les données relatives aux personnes transportées, en vue de parvenir rapidement à un accord sur cette mesure »²¹ fut également mentionnée, tout comme la « proposition en vue de la définition d'une démarche commune de l'Union européenne concernant l'utilisation des données des passagers pour des impératifs de sécurité des frontières et de l'aviation et d'autres fins répressives. »²² qu'il a invité la Commission à présenter au plus tard en juin 2004. Ces propositions donneront suite aux directives API et PNR.

La Déclaration du 26 Mars 2004²³ appela quant à elle à une coordination entre les États plus efficace dans le respect du traité de Lisbonne²⁴ signé le 13 décembre 2007. Selon les termes du Conseil Européen, « il convient d'accélérer le rythme des réformes au niveau des États membres. Il y a lieu de renforcer le suivi des résultats obtenus au plan national, notamment par l'échange d'informations sur les meilleures pratiques. Il faut que les accords et les politiques définis au niveau de l'Union européenne soient plus rapidement traduits en mesures concrètes. »²⁵

B. Le caractère obligatoire de la collecte de données passagers par la directive 2004/82/CE

Le 29 avril 2004, le Conseil de l'Union européenne adopte la directive 2004/82/CE concernant l'obligation pour les transporteurs de communiquer les données relatives aux passagers, dite directive API. Cette directive fut exceptionnellement adoptée sans l'avis préalable du Parlement Européen et fut rédigée en des termes laissant aux États une marge de manœuvre importante

²¹ Déclaration du Conseil européen sur le terrorisme, 25 Mars 2004, art.6.

²² Ibid.

²³ Conclusions de la Présidence du Conseil Européen sur la poursuite des objectifs de l'UE en matière de croissance et d'emploi et sur les questions internationales, notamment le Proche-Orient, l'Irak et le Kosovo, 26 Mars 2004.

²⁴ Traité de Lisbonne modifiant le traité sur l'Union européenne, le traité instituant la Communauté européenne et certains actes connexes, 13 Décembre 2007.

²⁵ Conclusions de la Présidence du Conseil Européen (...), 26 Mars 2004, art. 10.

pour compléter et étendre les mesures mentionnées. Par exemple, le détail des données API requises est limité à quelques exemples cités à son article 3.

Le but recherché était « *[l'amélioration des] contrôles aux frontières et [la lutte] contre l'immigration clandestine, au moyen de la transmission préalable aux autorités nationales compétentes, par les transporteurs, de données relatives aux passagers.* »²⁶ Dans cette optique, le Conseil a invité les États de l'Union Européenne à se munir « *d'un dispositif fixant les obligations des transporteurs aériens qui acheminent des passagers sur le territoire des États membres.* »²⁷, faisant suite à la Convention d'application de l'Acquis de Schengen du 14 juin 1985²⁸ et à la directive 2001/51/CE²⁹ du 28 Juin 2001 qui la complète.

Dans la continuité de l'Acquis de Schengen, les mesures de la directive API visent à « *permettre d'intensifier les contrôles aux frontières et à prévoir suffisamment de temps pour que soit effectué un contrôle détaillé et approfondi de chacun des passagers, grâce à la transmission, aux autorités chargées d'effectuer ces contrôles, des données relatives aux personnes transportées.* »³⁰. Ces mesures doivent également respecter le but recherché sous peine de les rendre incompatibles avec les objectifs recherchés et de les faire aller à l'encontre des principes de la directive 95/46/CE.

Ainsi, les données API sont « *transmises aux autorités chargées d'effectuer le contrôle des personnes aux frontières extérieures par lesquelles le passager entrera sur le territoire d'un État membre* »³¹ puis comparées aux bases de données relatives à la migration.

²⁶ Dir. API du Conseil de l'UE, 29 Avril 2004, art. 1.

²⁷ Ibid.

²⁸ Convention d'application de l'Accord de Schengen du 14 juin 1985 entre les gouvernements des États de l'Union économique Benelux, de la République fédérale d'Allemagne et de la République française relatif à la suppression graduelle des contrôles aux frontières communes

²⁹ Directive 2001/51/CE du Conseil visant à compléter les dispositions de l'article 26 de la convention d'application de l'accord de Schengen du 14 juin 1985, 28 Juin 2001.

³⁰ Directive API du Conseil de l'UE, 29 Avril 2004, §11 p. 1.

³¹ Ibid. art.6.

En 2012, la Commission a opéré une première réévaluation de cette directive, complétée par une seconde³² dont elle a présenté les conclusions le 08 Septembre 2020 à Bruxelles. Il a notamment été souligné que la grande liberté laissée aux États à l'étape de la transposition a permis une implémentation très correcte des mesures de la directive API malgré une trop grande variété d'objectifs recherchés résultant d'interprétations différentes par les États (lutte contre l'immigration clandestine, amélioration des contrôles aux frontières, lutte contre les offenses à la loi, lutte contre le terrorisme).

Lors de la réévaluation de 2020, forte des apports de la directive 2016/821 étudiée ci-après, la Commission a rappelé l'importance des points focaux appelés Fenêtres Uniques (« *Single Window* ») ou Centres de Ciblage (« *Targeting Centres* ») dans la collecte et le traitement des données API entre autres. Ainsi un centre de ciblage était entendu par la Commission comme étant « *la capacité des pays (...) à conduire des évaluations automatisées des risques liés aux voyageurs sur la base des différents renseignements sur les voyages collectés (par exemple API, SIS³³, VIS³⁴, EES³⁵ etc.) qui peuvent être légalement utilisés pour la gestion des frontières et sur la base d'une analyse tactique des risques.* ».³⁶ Les « *autorités de gestion aux frontières, les Ministères de l'Intérieur et les autorités de protection des données* »³⁷ sont désignées comme « *principales autorités impliquées dans l'implémentation [de ces] systèmes API* »³⁸.

C. L'évocation du terme UIP et l'explication de son principe par la directive 2016/681

Le 27 avril 2016, le Parlement Européen et le Conseil adoptent la directive (UE) 2016/681 relative à l'utilisation des données des dossiers passagers (PNR) pour la

³² *Evaluation of the (...) API Directive* de la Commission Européenne, 08 Septembre 2020.

³³ Système d'information Schengen.

³⁴ Système d'information sur les visas.

³⁵ Système d'Entrée-Sortie.

³⁶ Traduit de l'anglais. *Evaluation of the (...) API Directive* de la Commission Européenne, 08 Septembre 2020, p. 17.

³⁷ Ibid.

³⁸ Ibid.

prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière, également appelée directive PNR. Elle fut adoptée dans la continuité du Programme de Stockholm³⁹ après l'échec d'une première proposition du Conseil le 6 Novembre 2007. Ce programme promouvait les droits des citoyens de l'Europe, la protection civile et l'espace de Liberté, Sécurité et Justice, entre autres.

La directive PNR, bien que son objectif diffère, complète la directive API. Plus précise que cette dernière quant au but recherché de la récolte du PNR des passagers, il y est expressément dit que « *la création et l'application de ces critères d'évaluation [du PNR] devraient être limitées aux infractions terroristes et aux formes graves de criminalité pour lesquelles l'utilisation de tels critères est pertinente.* ».⁴⁰ Toujours selon les termes de ladite directive, « *il est essentiel que tous les États membres adoptent des dispositions obligeant les transporteurs aériens qui assurent des vols extra-UE à transférer les données PNR qu'ils recueillent, y compris les données API. Les États membres devraient également avoir la possibilité d'étendre cette obligation aux transporteurs aériens qui assurent des vols intra-UE.* ».⁴¹

(UE) 2016/681 autorise la transmission de données API en plus des données PNR du fait de leur fiabilité globale car basées sur les documents des passagers (exclusion faite des procédures d'enregistrement automatiques ou « *self-check-in* » qui peuvent comprendre des erreurs). En sus, l'annexe 2⁴² de la directive est une énumération précise des catégories d'infractions entendues sous le terme de « formes graves de criminalité », démarche vouée à la nécessité de concision, de bonne délimitation de l'utilisation qui sera faite des données PNR et les raisons de leurs transferts.

C'est dans cette directive que le Parlement Européen et le Conseil mentionnent aux États Membres les Unités d'Information Passagers ainsi que leur rôle, leurs modalités de mise en place, leur fonctionnement et la nécessité qu'elles se

³⁹ Programme de Stockholm – une Europe ouverte et sûre qui sert et protège les citoyens, 04 Mai 2010.

⁴⁰ Dir. PNR du Parlement européen et du Conseil, 27 Avril 2016, §7 p. 2.

⁴¹ Dir. PNR du Parlement européen et du Conseil, 27 Avril 2016, §10 p. 2.

⁴² Liste des infractions visées à l'article 3, point 9).

conforment aux textes tels que la Charte⁴³, la CEDH⁴⁴, la Convention n°108⁴⁵ ou encore la décision-cadre 2008/977/JAI⁴⁶ du Conseil pour ce qui touche aux échanges d'informations. Ces UIP, idéalement une par pays, sont ainsi chargée de recevoir les données PNR des transporteurs aériens et une partie de leur API (méthode « *Push* ») et sont idéalement la seule entité à recevoir ces données, agissant de fait comme une PDSW, soit une « *Passenger Data Single Window* ». Les UIP, après analyse automatique de ces données et avec ou sans traitement manuel, transmettent d'une manière réglementée des informations spontanément ou sur demande de requérants ayant été désignés comme autorités compétentes selon l'article 7. Du fait du but recherché par les UIP, ces requérants nationaux sont la plupart du temps des agences veillant au respect de la loi, comme les douanes, la police, l'armée, les agences nationales du renseignement ou même Europol. Ces demandes de transmission de l'information se font également entre UIP de différents pays.

La directive PNR, en se basant sur la décision-cadre 2008/977/JAI, met à la charge des autorités de contrôle nationales la tâche de « *fournir des conseils sur l'application des dispositions adoptées par les États membres en vertu de la présente directive et de surveiller l'application de celles-ci* »⁴⁷. Selon le principe de subsidiarité consacré à l'article 5 du TUE⁴⁸, Le Parlement Européen et le Conseil donnent la capacité à l'Union de prendre des mesures en soutien desdites dispositions. En cas de projet d'acte d'exécution de la part de la Commission, l'avis du Comité⁴⁹ est requis, sans quoi le projet ne sera pas adopté.

⁴³ Charte des droits fondamentaux de l'UE.

⁴⁴ Convention Européenne des Droits de l'Homme.

⁴⁵ Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du Conseil de l'Europe, 28 Janvier 1981.

⁴⁶ Décision-cadre 2008/977/JAI du Conseil relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale, 27 Novembre 2008. Remplacée par 2016/680.

⁴⁷ Dir. PNR du Parlement européen et du Conseil, 27 Avril 2016, art. 4.

⁴⁸ Traité sur l'Union Européenne, 26 Octobre 2012.

⁴⁹ Règlement (UE) n°182/2011 du Parlement européen et du Conseil, 16 Février 2011, art. 7.

La Commission a ainsi invité les États à « [mettre] en vigueur les dispositions législatives, réglementaires et administratives nécessaires pour se conformer à la présente directive au plus tard le 25 mai 2018 »⁵⁰.

Comme prévu par l'article 19, la Commission a procédé au réexamen de la directive « sur la base des informations communiquées par les États membres » et a déterminé le 24 juillet 2020 dans son Rapport au Parlement Européen et au Conseil qu'elle « contribue positivement à son principal objectif de garantir la mise en place de systèmes PNR efficaces au sein des États membres, en tant qu'instrument de lutte contre le terrorisme et les formes graves de criminalité. »⁵¹ et « qu'aucune modification de la directive PNR ne devrait être proposée à ce stade. »⁵².

II. La coopération au service de l'exportation du modèle européen à l'international

Le développement de normes relatives au fonctionnement des UIP virent le jour à la même période en Europe et à l'international. Les textes européens furent cependant les précurseurs dans la mise en place de l'UIP en tant que système. L'intérêt d'un modèle commun s'étant fait ressentir, les Nations-Unies continuèrent de présenter à leurs membres des décisions relatives à la transmission des données passagers à certaines fins, décisions auxquelles les organes de l'Europe purent apporter leur concours et observations.

A. Le corpus normatif des institutions internationales et la participation de l'Union européenne

⁵⁰ Dir. PNR du Parlement européen et du Conseil, 27 Avril 2016, art. 18.

⁵¹ Rapport de la Commission au Parlement européen et au Conseil sur le réexamen de la directive (...) PNR, 24 Juillet 2020, chap. 4.

⁵² Ibid.

Le corpus juridique autour de l'importance des données API, PNR et leur usage s'est développé à la même période en Europe et dans le reste du monde. L'IATA⁵³ et la WCO⁵⁴ firent paraître en 1993 leurs lignes directrices relatives à l'API. Leur première révision eut lieu en 2003 avec la participation de l'OACI⁵⁵. Ces lignes directrices furent par la suite révisées à nouveau et complétées par ces trois organismes en 2010, 2013 et 2014. Le texte de 2014 ne faisait pas référence à l'importance de la mise en place d'une fenêtre unique nationale chargée de regrouper et traiter ces données. L'IATA évoquait par exemple la nécessité pour les transporteurs de les « [transmettre] une seule fois à tous ceux ayant l'autorité légale de demander et voir ces données ».⁵⁶

Cependant, l'usage de ces données dans le but de préserver la sécurité/ sûreté était déjà évoqué de manière conjointe par les trois Organisations à l'origine des lignes directrices. Ainsi lisait-on que les données API reçues des transporteurs « peuvent être le catalyseur pour un contact plus important entre ces agences [agences visant au respect de la loi] et le développement de programmes communs qui seront bénéfiques du point de vue de la conformité, la facilitation et la sûreté ».⁵⁷ Dans le même sens, les Organisations mentionnèrent un Plan devant notamment « décrire les demandes faites aux agences de contrôle aux frontières et transporteurs [sur des questions de développement] du trafic de stupéfiants ou d'immigration illégale et autres menaces similaires ».⁵⁸

L'OACI publia en 2010 la première édition de ses *Lignes Directrices sur les données PNR*⁵⁹ après avoir soulevé l'importance de la collecte de ces données dans sa recommandation B/5 adoptée dans le cadre de la 12^e Session de la Division Facilitation tenue au Caire en Égypte du 22 mars au 1^{er} Avril 2004.

⁵³ *International Air Transport Association/ Association Internationale du Transport Aérien*

⁵⁴ *World Customs Organization / Organisation Mondiale des Douanes*

⁵⁵ *Organisation de l'Aviation Civile Internationale*

⁵⁶ Traduit de l'anglais. *Guidelines on API* de WCO, IATA et ICAO, 2014, art. 4.2.9.

⁵⁷ *Ibid.* art. 10.3.

⁵⁸ *Ibid.* art. 7.6.2.

⁵⁹ Traduit de l'anglais « *Guidelines on Passenger Name Record (PNR) Data* ».

En sus du Plan Stratégique 2011-2016⁶⁰ déjà en place et du Programme de sûreté à son soutien, elle rédigea également en 2017 le Plan pour la sûreté de l'aviation dans le monde⁶¹ avec pour objectif de « *renforcer la sûreté de l'aviation dans le monde et d'aider les États à collaborer pour respecter les engagements exposés dans l'UNSCR 2309 (2016) et les Résolutions applicables de l'Assemblée de l'OACI.* ». ⁶² Ce Plan est basé sur les résolutions 2309 et 39-18 des Nations-Unies parues en 2016. Par la résolution 2309 du 22 Septembre 2016, le Conseil de Sécurité « *[demanda] à tous les États de s'employer dans le cadre de l'OACI à revoir et adapter ses normes de sûreté internationale afin de pouvoir répondre efficacement à la menace que le terrorisme fait peser sur l'aviation civile, renforcer et promouvoir la bonne application des normes et pratiques recommandées par l'OACI à l'annexe 17⁶³ [de la Convention de Chicago]* ». ⁶⁴ Par ailleurs, il « *[exigea] des compagnies aériennes opérant sur leur territoire qu'elles communiquent à l'avance aux autorités nationales compétentes des informations sur les passagers afin de détecter le départ de leur territoire, ou la tentative d'entrée sur leur territoire ou de transit par leur territoire, à bord d'appareils civils, de personnes désignées par le Comité* ». ⁶⁵ Cette succession de textes, avec la résolution 2178 du 24 Septembre 2014, posa la base internationale de la nécessité du transfert d'informations préalables tout en accordant une importance croissante à la lutte contre le terrorisme et autres crimes sérieux.

Ces différentes résolutions furent par la suite complétées par la 2396 du 21 Décembre 2017 puis la 2482 du 19 Juillet 2019. La 2396 réaffirma les précédentes et « *[demanda] également aux États Membres de contrôler les personnes dont ils ont des motifs raisonnables de penser qu'il s'agit de terroristes, notamment les personnes soupçonnées d'être des combattants terroristes étrangers et d'enquêter sur ces personnes (...) en recourant notamment à (...) la collecte et à l'analyse de données relatives aux voyages (...)* ». ⁶⁶ Le principe de la Fenêtre Unique n'apparaissait alors pas encore, la résolution « *[exhortant] les États Membres à (...) communiquer*

⁶⁰ Stratégie globale de sûreté de l'aviation (ICASS) – Plan d'action stratégique 2011-2016 de l'Assemblée de l'OACI, 26 Juin 2010.

⁶¹ Doc 10118, Plan pour la sûreté de l'aviation dans le monde de l'OACI, 1ere édition 2017.

⁶² Ibid. art. 2.1.1.

⁶³ Annexe 17 Sûreté, Convention de Chicago, 22 mars 1974.

⁶⁴ Rés. 2309 du Conseil de sécurité, 22 Septembre 2016, art. 5.

⁶⁵ Ibid. art. 6.g).

⁶⁶ Rés. 2396 du Conseil de sécurité, 21 Décembre 2017, art.4.

ces informations au niveau national, de manière appropriée, aux services de contrôle de première ligne que sont l'immigration, les douanes et la sécurité des frontières, et de les transmettre comme il convient aux autres États et organisations internationales compétentes concernés (...)». ⁶⁷ La résolution 2482 réaffirma quant à elle les propos de la 2396.

Afin de diffuser ces bonnes pratiques, les Nations-Unies demandèrent à l'OACI d'édicter des lignes directrices, ce qu'elle fit par le biais de son amendement à l'annexe 17 et sa révision du chapitre 9 de l'annexe 9⁶⁸ de la Convention de Chicago⁶⁹. Avant adoption, le Comité du Transport Aérien (ATC) de l'OACI avait mis en place des groupes de travail composés de représentants des États Membres de l'OACI et de l'Union Européenne en qualité d'observateurs.

L'Union Européenne a de ce fait pu apporter son soutien et proposer son avis à l'OACI dans la création de ses nouveaux Standards et Pratiques Recommandées de l'annexe 9 car elle avait déjà « *adopté des règles communes sur les données PNR sous la forme de la directive (UE) 2016/681 du Parlement européen et du Conseil, dont le champ d'application recoupe en grande partie la zone couverte par les nouvelles SARP [Standards et Pratiques Recommandées] envisagées.* »⁷⁰ C'est dans une décision (UE) 2019/2107⁷¹ du 28 Novembre 2019 que le Conseil de l'Union Européenne s'est exprimé sur la position à prendre vis-à-vis de la révision dudit chapitre 9, abordant entre autres le sujet des méthodes et protocoles de transmission des données ou encore leur utilisation et leur partage.

⁶⁷ Ibid. art. 8.

⁶⁸ Annexe 9 Facilitation, Convention de Chicago, 22 mars 1974.

⁶⁹ Convention relative à l'aviation civile internationale, 07 Décembre 1944.

⁷⁰ Council decision on the position to be taken on behalf of the European Union in the International Civil Aviation Organization as regards Amendment 28 to Annex 9 Section D to the Convention on International Civil Aviation, 12 Janvier 2021, &11.

⁷¹ Décision (UE) 2019/2107 du Conseil relative à la position à prendre, au nom de l'Union européenne, au sein du Conseil de l'Organisation de l'aviation civile internationale, en ce qui concerne la révision du chapitre 9 de l'annexe 9 (Facilitation) de la convention relative à l'aviation civile internationale en ce qui concerne les normes et pratiques recommandées en matière de données des dossiers passagers, 28 Novembre 2019.

Un 17^e amendement fut proposé pour l'annexe 17, prévoyant notamment « *des dispositions nouvelles ou révisées concernant les évaluations des vulnérabilités, le partage d'informations entre États et parties concernées (...)* »⁷² De la même manière, dans la décision (UE) 2019/2036 du 25 Novembre 2019, le Conseil de l'Union Européenne notifia que les pays de l'Union étaient « *favorables à la proposition relative à l'amendement (...)* ».⁷³

Plus récemment, le 12 Janvier 2021, sur la proposition par l'OACI d'un 28^e amendement à l'annexe 9 section D, le Conseil de l'Union Européenne s'est à nouveau exprimé en faveur des dispositions proposées. Rappelant dans un premier temps que « *les nouveaux standards et pratiques recommandées PNR énoncés dans l'amendement 28 (...) suivent largement des lignes de la position Européenne consacrées dans la décision 2019/2017* »⁷⁴ et que les « *règles communes en matière de PNR de la directive 2016/681 (...) [recoupaient] celles du champ couvert par les SARPs contenues dans l'amendement 28* »⁷⁵, le Conseil a ensuite exprimé que « *les exigences résultant du Droit de l'Union en matière de transfert et de traitement des données PNR sont plus strictes que les [SARPs] contenues dans l'amendement 28.* ».⁷⁶

B. Le soutien des entités internationales dans l'implémentation du modèle des UIP par les États

Dans un but d'élever la lutte contre le terrorisme comme l'un des piliers de la coopération internationale, l'Assemblée générale des Nations-Unies adopta le 8 Septembre 2006 dans une résolution 60/288⁷⁷ sa Stratégie antiterroriste

⁷² Décision (UE) 2019/2036 du Conseil relative à la position à prendre, au nom de l'Union européenne, au sein du Conseil de l'Organisation de l'aviation civile internationale en ce qui concerne l'amendement 17 de l'annexe 17 («Sûreté») de la convention relative à l'aviation civile internationale, 25 Novembre 2019, §4. p.1.

⁷³ Ibid. p.3.

⁷⁴ Traduit de l'anglais. *Council decision (...) as regards Amendment 28 to Annex 9 Section D art. 3.2.*

⁷⁵ Ibid. §11.

⁷⁶ Ibid. §18.

⁷⁷ Résolution 60/82 de l'Assemblée générale – La stratégie antiterroriste mondiale de l'Organisation des Nations Unies.

mondiale. Cette Stratégie, réexaminée tous les 2 ans, fut soutenue par le Centre des Nations Unies pour la lutte contre le terrorisme, créé en 2011 et opérationnel en 2012. Le Centre « apporte aux États Membres le soutien politique dont ils ont besoin et diffuse une connaissance approfondie de la Stratégie antiterroriste mondiale des Nations Unies ».⁷⁸ Au soutien de « la coordination et la cohérence de la lutte antiterroriste menée par les Nations Unies »⁷⁹ fut créée en 2005 l'Équipe spéciale de lutte contre le terrorisme.

Le 03 Avril 2017, le Secrétaire Général des Nations-Unies Antonio Guterres émit un rapport A/71/858 sur la *Capacité du système des Nations Unies d'aider les États Membres à appliquer la Stratégie antiterroriste mondiale des Nations Unies*, à la suite duquel fut adoptée le 15 Juin 2017 la résolution A/RES/71/291⁸⁰. Cette résolution amena à la création du Bureau de lutte contre le terrorisme. Ses 5 fonctions principales sont de « *diriger l'action menée au titre des divers mandats de lutte contre le terrorisme de l'Assemblée générale qui ont été confiés au Secrétaire général dans l'ensemble du système des Nations Unies; renforcer la coordination et la cohérence des activités des entités signataires du Pacte mondial de coordination contre le terrorisme pour assurer la mise en œuvre équilibrée des quatre piliers de la Stratégie antiterroriste mondiale des Nations Unies ; accroître l'aide que l'Organisation fournit aux États Membres pour renforcer leurs capacités de lutte contre le terrorisme ; promouvoir davantage les activités menées par l'ONU pour lutter contre le terrorisme, leur donner une plus grande visibilité et renforcer la mobilisation de ressources dans ce domaine ; veiller à ce que la priorité voulue soit accordée à la lutte contre le terrorisme dans l'ensemble du système des Nations Unies et à ce que les travaux importants menés s'agissant de la prévention de l'extrémisme violent soient fermement ancrés dans la Stratégie.* ».⁸¹

Le Bureau élaborera quant à lui le Pacte mondial de coordination contre le terrorisme des Nations-Unies. Regroupant 43 entités de l'Organisation, il sera signé le 23 Février 2018. Ce Pacte « *vise à renforcer une approche commune de*

⁷⁸ Site des Nations Unies – Page Bureau de lutte contre le terrorisme (cf. bibliographie).

⁷⁹ Site des Nations Unies – Page Équipe spéciale de lutte contre le terrorisme (cf. bibliographie).

⁸⁰ Résolution 71/291 de l'AGNU, Renforcer la capacité du système des Nations Unies d'aider les États membres à appliquer la Stratégie antiterroriste mondiale des Nations Unies, 15 Juin 2017.

⁸¹ Site des Nations Unies – Page Mandat de l'AG des NU (cf. bibliographie).

*l'action de l'ONU afin de soutenir les États Membres qui en font la demande dans la mise en œuvre équilibrée de la Stratégie antiterroriste mondiale des Nations Unies et d'autres résolutions et mandats pertinents de l'Organisation. ».*⁸²

Le Programme de lutte contre le terrorisme axé sur les déplacements fut officiellement lancé par le Bureau le 07 Mai 2019 et est lié à divers organismes tels que la Direction exécutive du Comité contre le terrorisme, l'Office des Nations Unies contre les Drogues et le Crime, l'OACI, le Bureau de l'informatique et des communications des Nations Unies, INTERPOL⁸³ ou encore AIRCOP⁸⁴.

Son but est « *[d'aider] les États Membres à renforcer leurs capacités de détection pour combattre les infractions terroristes et d'autres crimes graves en utilisant les renseignements préalables concernant les voyageurs, les dossiers passagers et d'autres données sur les passagers, conformément aux résolutions S/RES/2178(2014), S/RES/2396(2017) et S/RES/2482(2019) du Conseil de sécurité. ».*⁸⁵

Ce Programme est l'instrument principal de l'aide à l'implémentation des UIP à travers le monde. Ses 4 piliers sont « *l'assistance législative pour rédiger ou renforcer les cadres juridiques permettant de régler la collecte, la transmission, l'utilisation, la conservation et le partage des données relatives aux passagers (...); la mise en place [des UIP] (...); le soutien pour établir l'engagement et la connectivité des transporteurs et enfin l'assistance technique et une expertise pour le logiciel "goTravel", qui est une solution logicielle efficace permettant aux pays de collecter et de traiter les données relatives aux passagers. »*

C. L'importance du partage des bonnes pratiques pour une implémentation facilitée

⁸² Site des Nations Unies – Page Les 3 piliers des travaux de l'ONU (cf. bibliographie).

⁸³ Organisation internationale de police criminelle.

⁸⁴ Programme de coopération aéroportuaire.

⁸⁵ Site des Nations Unies – Page Renforcement des capacités de détection (cf. bibliographie).

L'implémentation et le développement des UIP comme standard à travers le monde est le but recherché par les différents organismes rattachés aux Nations-Unies et soutenant la Stratégie antiterroriste mondiale par la sécurisation du transport aérien.

Les Nations-Unies et l'Europe ont ainsi mis en place des Groupes de Travail Informels. Ces groupes « assurent un forum pour les UIP et les décideurs politiques impliqués dans la création de ces unités afin de soutenir la mise en œuvre des résolutions 2178, 2396 et 2482 (...). Ils favorisent la coopération et l'échange d'informations les plus larges possibles entre les UPI, sur la base de la réciprocité ou d'un accord mutuel et suivant des principes et des règles convenus en commun. (...) Le Programme de lutte contre le terrorisme axé sur les déplacements s'efforce de reproduire ce modèle dans toutes les régions du monde. ». ⁸⁶ Le modèle des UIP étant déjà largement diffusé en Europe du fait de la directive PNR, les groupes de travail informels européens ont été une aide pour la création de ceux des Nations-Unies. Ils peuvent être internationaux comme nationaux ou régionaux.

Le processus de communication des bonnes pratiques peut être aidé par les groupes informels mais il doit également être une démarche spontanée des États. Dans sa résolution 2396 de 2017, réaffirmant la 2178 de 2014, le Conseil de Sécurité « exhorte les États Membres à envisager (...) de déclasser à des fins administratives les données de renseignement (...) afin de (...) les transmettre comme il convient aux autres États et organisations internationales compétentes concernés, dans le respect des lois et politiques nationales et internationales, et de faire connaître leurs bonnes pratiques à cet égard ». ⁸⁷ Il demande également « aux États Membres, notamment par l'intermédiaire de leurs autorités centrales compétentes, ainsi qu'à l'Office des Nations Unies contre la drogue et le crime et aux autres entités compétentes des Nations Unies qui appuient le renforcement des capacités, de partager leurs meilleures pratiques et compétences techniques, par voie tant formelle qu'informelle, en vue d'améliorer la collecte, le traitement, la conservation et l'échange des

⁸⁶ Traduit de l'anglais. *Outcome document from the 4th OSCE-wide Seminar on Passenger Data Exchange*, 30 Octobre 2020, Session 5.

⁸⁷ Réso. 2396 du Conseil de sécurité, 21 Décembre 2017, art.8.

informations et éléments de preuve pertinents (...).».⁸⁸ Cette demande d'amélioration de la coopération internationale mais aussi régionale et sous-régionale concerne la lutte contre le terrorisme et autres formes graves de criminalité sous tous ses pans. La résolution 2482 de 2019 va également dans ce sens.

Ce partage de bonnes pratiques est un instrument venant s'ajouter à l'aide des entités des Nations Unies pour le développement des UIP à travers le monde, le terrorisme profitant de la fragilité des États à lutter contre sa détection.

En Europe par exemple, le Département des Menaces Transnationales de l'OSCE⁸⁹, plus grande organisation régionale de sécurité au monde, organise des « *ateliers de travail sur l'établissement d'un système d'échange de données passagers (...)* ».⁹⁰ Dernièrement, en Avril 2021, elle organisa, conjointement avec le Programme, le « *lancement virtuel du Groupe de Travail Informel régional de l'Europe de l'Est* »⁹¹ sur l'API et la PNR.

A l'international, le Programme de lutte contre le terrorisme axé sur les déplacements aide aussi les États Membres à créer des groupes de travail régionaux informels destinés à promouvoir l'échange d'informations et le partage des bonnes pratiques et d'enseignements, ce qui permet d'améliorer considérablement la mise en œuvre et les capacités nationales. La composante numérique du Programme, une plateforme interactive baptisée « *Cooperative Online Platform* »⁹², permet aux États Membres d'accéder à des informations partagées au niveau mondial et régional en permanence et de les rapprocher en ligne du Programme de lutte contre le terrorisme axé sur les déplacements.

⁸⁸ Ibid. art. 20.

⁸⁹ Organisation pour la Sécurité et la Coopération en Europe.

⁹⁰ Traduit de l'anglais. Outcome document (...), 30 Octobre 2020, chap. 3.

⁹¹ Traduit de l'anglais. Annexe 1 mémoire.

⁹² Annexe 2 mémoire.

La CTITF⁹³, entre autres entités, se voit également attribuer un rôle d'organisatrice de « groupes de travail et projets et activités liés au contre-terrorisme dans les domaines où la coopération parmi les acteurs du système des Nations-Unies peuvent apporter une valeur ajoutée pour l'implémentation de la Stratégie [mentionnée précédemment]. ».⁹⁴

SECTION 2- Les défis structurels et légaux de l'implémentation du modèle des UIP au sein des États

La coopération internationale suppose d'avoir à composer avec différents États dont les régimes juridiques peuvent être très différents les uns des autres. Les mesures proposées par les organes internationaux doivent être transposées au niveau national. Afin que l'adaptation de ces mesures puisse être mise en place par le plus grand nombre, les textes internationaux laissent aux États une part à l'interprétation et au choix des modalités d'application. Favorisant une implémentation internationale étendue, ces libertés entraînent aussi nécessairement des disparités dans les mises en place législatives et les régimes nationaux. Il en va ainsi pour certains aspects structurels et légaux des UIP, faisant émerger des obstacles nuisant à leur bon fonctionnement. C'est particulièrement le cas pour les transferts vers et depuis ces unités.

I. Le manque de clarté des procédures de récupération des données passagers

Ces obstacles mentionnés précédemment se forment notamment durant les phases de transfert vers l'UIP. La transmission des données par les transporteurs aériens est un volet nécessaire des UIP qui doivent les recueillir aux fins d'analyse, de traitement et de redistribution aux autorités et organismes compétents. Des procédures encadrent ces transferts par les

⁹³ Counter-Terrorism Implementation Task Force/Équipe spéciale de lutte contre le terrorisme.

⁹⁴ Traduit de l'anglais. Site des Nations Unies – Page Coordination and coherence of the counter-terrorism efforts of the United Nations (cf. bibliographie).

transporteurs mais la marge de manœuvre laissée aux États a permis la création et l'exploitation de façons de transférer trop variées ou mal définies. De plus, les particularismes nationaux relevant du domaine de la souveraineté des États, différents organismes ont parfois été créés pour recevoir les données passagers, ce qui peut prêter à confusion, surtout dans les cas de transferts de données d'un transporteur vers une UIP d'un autre État dont il ne connaît pas l'organisation.

A. Les disparités de qualité et quantité des données récoltées et transférées par les transporteurs aériens

Les organes de l'Union Européenne ont dressé à travers leurs directives des listes d'éléments demandés aux transporteurs en matière de données API et PNR.

Ainsi, la directive PNR de 2016 évoque qu'une « *liste des données PNR à transmettre à une UIP devrait être établie dans le but de [renforcer] la sécurité intérieure de l'Union et la protection des droits fondamentaux, notamment le respect de la vie privée et la protection des données à caractère personnel.* ». ⁹⁵ Cette liste est reprise dans l'annexe 1⁹⁶ à la directive. Toute autre donnée PNR devra être « *[effacée] immédiatement et de façon définitive dès leur réception.* ». ⁹⁷

Cependant, la directive API de 2004 dressait également une liste⁹⁸ non exhaustive des données à transmettre aux autorités compétentes. Ce manque de délimitation précise permettait donc aux autorités de demander un surplus de données aux transporteurs. Ces données étaient en partie les mêmes que celle de la liste de l'Annexe 1 de la directive PNR. Ainsi donc il est aujourd'hui possible d'être en conformité avec les exigences de la directive API en termes

⁹⁵ Dir. PNR du Parlement européen et du Conseil, 27 Avril 2016, §15 p. 2.

⁹⁶ Données des dossiers passagers telles qu'elles sont recueillies par les transporteurs aériens.

⁹⁷ Dir. PNR du Parlement européen et du Conseil, 27 Avril 2016, art. 6.

⁹⁸ Dir. API du Conseil de l'UE, 29 Avril 2004, art. 3.2.

de données à transmettre aux UIP tout en ne respectant pas les dispositions de la directive PNR sur le même point.

En plus de ne pas demander les mêmes données, la récolte de ces données par les États Membres ne se fait pas uniformément sur tous les vols. Par exemple, en date de Septembre 2020, « *la majorité des pays appliquant [la directive API] recevaient ou prévoyaient de recevoir les données API de tous les vols entrants extra UE/Schengen à destination de leur territoire tandis que 7 autres collectaient ou prévoyaient de collecter ces données uniquement sur des vols choisis* ». ⁹⁹ En effet, la directive API de 2004 ne précisait pas sur quel type de vol ces données devaient être collectées. Ainsi, les États Membres qui n'opèrent cette collecte que sur certains vols choisis le font « *sur la base d'une analyse des risques et/ou les priorités stratégiques* » ¹⁰⁰, ce qui peut être critique en cas de sous-évaluation de la menace. En sus, dans la majorité des États Membres, les données API « *ne sont pas collectées pour les vols charter et non réguliers* ». ¹⁰¹ La révision de la directive API de 2020 relève ainsi 3 tendances principales quant à la collecte des données API qui sont la collecte pour les vols provenant de l'extérieur de l'Union Européenne, la collecte pour ceux provenant de l'extérieur de l'espace Schengen et la collecte pour ceux provenant de l'extérieur de l'espace Schengen sauf pays Membres de l'Union Européenne.

Sur le point de la qualité des données, pour ce qui est de la capture des données API, elle peut se faire « *à travers les systèmes de réservation en ligne ou bien manuellement aux postes d'enregistrement* ». ¹⁰² La qualité des données n'est alors pas garantie du fait que ce sont les passagers ou le personnel de l'aéroport qui entrent les informations contenues sur les documents de voyage. Le manque de vérification peut entraîner des erreurs, remettant en cause la viabilité de données supposées être exactes.

⁹⁹ Traduit de l'anglais. Révision API 2020 p. 14.

¹⁰⁰ Ibid. p. 26.

¹⁰¹ Ibid. p.26.

¹⁰² Ibid. p. 56.

Il existe aujourd’hui des solutions technologiques « *pour vérifier les données API via le scan de la zone lisible par machine [des documents de voyage] ou même la lecture de données authentifiées par puce (...)* ». ¹⁰³ La redéfinition des listes de données à transmettre aux UIP ainsi que la récolte de ces données par les procédés technologiques fiables d’aujourd’hui participeraient de manière importante aux objectifs fixés d’identification de potentiels criminels voyageant par la voie aérienne.

B. La détermination complexe des structures habilitées à recevoir les données passagers

En 2016, le Parlement Européen et le Conseil notifièrent aux États Membres leur obligation de se conformer aux exigences de transposition de la directive PNR portant sur la création des UIP. Ainsi les États durent-ils « *[mettre] en vigueur les dispositions législatives, réglementaires et administratives nécessaires pour se conformer à la présente directive au plus tard le 25 mai 2018* ». ¹⁰⁴

Pour certains pays, ces modalités de transposition se firent plus aisément. La France, par exemple, avait déjà implanté par ses deux décrets n°2014-1095 du 26 septembre 2014 et n°2014-1566 du 22 décembre 2014 un système visant à recueillir les données API/PNR des transporteurs. Elle n’a ainsi eu qu’à « *mettre son système national en conformité avec les nouveaux standards européen en la matière* ». ¹⁰⁵

Il en va de même pour la Belgique qui s’était muni au préalable d’un système de récolte et de traitement des données PNR dès 2016. Son Arrêté Royal du 18 Juillet 2017 et celui du 21 Décembre 2017 vinrent finir d’organiser l’unité Belge BelPIU comme elle est aujourd’hui.

¹⁰³ Ibid. p. 56.

¹⁰⁴ Dir. PNR du Parlement européen et du Conseil, 27 Avril 2016, art. 18.

¹⁰⁵ Site PNR.gouv – Page Transposition par la France de la directive Européenne PNR (cf. bibliographie).

Cependant cette transposition ne s'est pas faite à l'identique parmi tous les pays Européens. Le Danemark par exemple n'était pas lié à la directive PNR du fait qu'il « *[disposait] d'une clause générale de non-participation à la législation de l'UE dans le domaine de la justice et des affaires intérieures (JAI), sauf lorsqu'elle se fonde sur l'acquis de Schengen.* ».¹⁰⁶ Ainsi son système PNR était différent car les douanes récupéraient les données des transporteurs avant transmission au Service danois de sécurité et de renseignement et celui de renseignement et de la défense (respectivement PET et DDIS). Depuis 2018, le Danemark a finalement travaillé sur la mise en conformité de son système PNR avec la directive européenne sur le sujet.

Selon le rapport d'évaluation de la Commission Européenne du 08/09/2020 sur la directive API, « *près de la moitié des pays de mise en œuvre [de la directive] rapportèrent traiter les données API en même temps que les données PNR* »¹⁰⁷ selon le principe de la Fenêtre Unique. Certains pays procèdent différemment. Dans le cadre des Pays-Bas par exemple, « *les données API sont traitées par les autorités aux frontières répondant du Ministère de la Défense, les données PNR sont traitées par l'UIP (Pi-NL), une unité indépendante rattachée au Ministère de la Défense mais sous la responsabilité du Coordinateur National pour la sûreté et le contre-terrorisme.* ».¹⁰⁸ Cette organisation bicéphale pour le traitement des données API et PNR est présente dans la majorité des États Membres.

Une homogénéisation de la notion de Fenêtre Unique, idéalement incarnée par les UIP, pour la réception et le transfert des données passagers est un axe de travail qu'il est important de continuer à développer. Cette multitude de structures habilitées à recevoir cette information crée de la confusion empêchant une coopération optimale dans le domaine de la lutte contre le terrorisme, crimes sérieux et autres offenses à la loi, et n'est pas sécurisé. Par ses rapports, la Commission devrait continuer à légiférer en faveur de l'UIP comme structure centrale pour la réception des données API/iAPI et PNR. Un ajustement des textes européens, notamment de la directive PNR sur les

¹⁰⁶ Traduit de l'anglais. Jesper Lund, « *Denmark prepares for passenger data exchange with the EU* », 19 Décembre 2018 (cf. bibliographie).

¹⁰⁷ Traduit de l'anglais. Révision API 2020 p. 17.

¹⁰⁸ Ibid. p. 18.

données API que l'UIP serait habilitée à recevoir serait un pas dans cette direction.

La directive PNR est de 2018 tandis que la directive API date de 2004. Les systèmes API mis en place par les États pour se conformer à cette dernière sont donc beaucoup plus anciens et il est normal que l'adaptation législative et organisationnelle des Pays Membres au nouveau système de la directive PNR prenne du temps.

C. La multiplicité des formats de messages et protocoles de transfert des données passagers

Sur recommandation des Nations-Unies, le transfert des données des transporteurs à l'UIP ou autre système national chargé de la réception et du traitement de ces données doit se faire à travers un système de schéma de message reconnu et lisible par toutes les parties concernées appelé PAXLST EDIFACT/ONU pour les données API (pour les États ne fonctionnant pas avec une UIP comme Fenêtre Unique) et PNRGOV pour les données PNR (et les États incluant l'API dans le transfert de la PNR).

Ces messages sont ensuite transférés par les transporteurs via des protocoles de transfert choisis par eux. En Europe, la directive API, du fait de sa grande marge de manœuvre laissée aux États, a mené à la mise en place de nombreux schémas de messages et protocoles de transfert.

Le Parlement Européen et le Conseil voulurent être plus précis dans la directive PNR en disant que « *ces lignes directrices [des Nations-Unies] devraient (...) servir de base pour l'adoption des formats de données reconnus pour les transferts des données PNR par les transporteurs aériens aux États membres.* ».¹⁰⁹ en reconnaissant que « *les compagnies charter, les exploitants de taxis aériens et les transporteurs aériens d'affaires fonctionnent selon un modèle commercial différent et peuvent ne pas disposer de l'infrastructure technique nécessaire pour transmettre les*

¹⁰⁹ Dir. PNR du Parlement européen et du Conseil, 27 Avril 2016, §17 p. 3.

données [sous ce format]. ».¹¹⁰ Ces transferts devaient se faire « *par voie électronique (...) ou tout autre moyen approprié garantissant un niveau de sécurité des données approprié (...).* ».¹¹¹ , à charge pour les transporteurs aériens de « *choisir et de préciser à l'UIP le protocole commun et le format de données qu'ils ont l'intention d'utiliser pour leurs transferts* ».¹¹² À la suite de la directive PNR, conscient de cette trop grande variété de formats, la Commission proposa une décision d'exécution (UE) 2017/759¹¹³ du 28 avril 2017 dans laquelle elle précisa les protocoles communs et formats à utiliser tout en invitant ceux ne pouvant pas adopter ce modèle à discuter avec leur État pour convenir d'un moyen électronique de transfert au niveau de sécurité satisfaisant.

Furent ainsi reconnus comme viables les protocoles de transfert IBM MQ et IATA Type B déjà majoritairement utilisés. La Commission demanda aux États de se conformer aux types de messages mis en avant par les Nations-Unies.

Il existe en outre un particularisme Européen dans la récolte et le transfert des données vis-à-vis des systèmes ETIAS¹¹⁴ et EES/VIS. Les données récoltées par les transporteurs passent ensuite par ces systèmes qui analyseront les informations relatives aux passagers européens et rejetteront celles des nationaux d'États tiers. Les données passagers recueillies dans un premier temps sont ensuite envoyées de manière non différenciée aux États de destination. Ce système de double envoi n'est pas en la faveur d'une facilitation et uniformisation des procédures.

Il conviendrait que la Commission, lors du réexamen de sa décision d'exécution 2017/759 prévu en 2021, uniformise les protocoles de transfert comme elle souhaitait le faire par le développement de son protocole AS4 afin

¹¹⁰ Traduit de l'anglais. Révision API 2020 pp. 26-27.

¹¹¹ Dir. PNR du Parlement européen et du Conseil, 27 Avril 2016, art. 8.3.

¹¹² Ibid. art. 16.2.

¹¹³ Décision d'exécution (UE) 2017/759 sur les protocoles communs et formats de données devant être utilisés par les transporteurs aériens lors d'un transfert de données PNR aux unités d'information passagers, 28 Avril 2017.

¹¹⁴ *European Travel Information and Authorization System*/Système européen d'information et d'autorisation de voyage.

de permettre un unique transfert. Concernant les messages, l'idéal resterait de maintenir uniquement le format PNRGOV mais cela impliquerait pour les États Membres de l'Union Européenne de fonctionner avec leur UIP comme Fenêtre Unique pour la réception et le traitement des données API et PNR. La Commission devrait continuer à interdire le transfert de données par tout format autre qu'informatique (format papier, appels téléphoniques et autres) et continuer à s'exprimer en faveur de plus de sécurité quant aux transferts convenus entre les transporteurs particuliers et leur État.

II. Le manque de sécurité dans l'exploitation des données et leurs transferts

Un autre obstacle majeur au fonctionnement fluide des UIP et à leur normalisation touche à l'absence d'un standard dans l'exploitation et la sécurisation des données passagers. Ces données, lorsque transmises par les transporteurs aériens, sont généralement isolées à partir d'une liste ou de critères précis. Ces garanties sont nécessaires pour le respect de la vie privée des passagers et la conformité de l'utilisation des données pour la lutte contre le terrorisme et autres infractions sérieuses. Du fait des sources internationales multiples, des incompatibilités dans l'application de normes peuvent avoir lieu, ce qui peut paralyser les échanges d'informations ou générer des atteintes à la vie privée des personnes disproportionnées par rapport au but recherché par les UIP.

A. La fluctuation des champs et critères requis de collecte et d'utilisation des données passagers

Dès le moment où les UIP reçoivent les données passagers de la part des transporteurs aériens, elles procèdent à leur analyse et à leur transmission aux entités habilitées à les recevoir. Ces transferts ne doivent se faire qu'afin que les données « *fassent l'objet d'un traitement dans des cas spécifiques, aux fins de la prévention et de la détection d'infractions terroristes ou de formes graves de*

criminalité, ainsi qu'aux fins d'enquêtes et de poursuites en la matière ». ¹¹⁵ Ils se font principalement entre les UIP des différents États qui les redistribueront ensuite à leurs autorités compétentes nationales. Selon l'article 9.3 de la directive PNR, en cas d'urgence, les autorités nationales peuvent demander certaines données directement à l'UIP d'un autre pays à condition que la demande soit motivée. Cette transmission ne se fera qu'au cas par cas et après une procédure de réexamen individuel s'il y a eu correspondance informatique dans un premier temps. Cette procédure est décrite à l'article 6.6 de la directive PNR. Europol peut également « *demander aux UIP des États membres [de l'Union Européenne] des données PNR ou le résultat du traitement de ces données dans les limites de ses compétences [en vertu de la décision-cadre 2009/371/JAI¹¹⁶] et pour l'accomplissement de ses missions* ». ¹¹⁷

Malgré ces précautions mises en place, la nécessaire protection entourant les transferts de tout type est remise en cause par certaines pratiques. Un État peut ainsi décider de modifier les critères d'évaluation de la menace terroriste ou infractions graves requis pour procéder au traitement des données des passagers ou bien décider d'un allongement de la liste des données que les passagers devront envoyer à l'UIP.

La directive PNR indique que les critères préétablis servant à l'évaluation des passagers doivent être « *réexaminés à intervalles réguliers par les UIP en coopération avec les autorités compétentes* ». ¹¹⁸ Ce réexamen pourrait être entendu comme la possibilité de modifier ces critères.

Le manque de définition précise du but de la collecte des données peut également constituer une problématique au regard de la sécurité des données car cela pourrait mener à une confusion dans les demandes aux UIP et les données à transférer. Le réexamen de la directive API par la Commission Européenne a mis ce point en avant. « *La directive [ayant été] rédigée dans l'esprit*

¹¹⁵ Dir. PNR du Parlement européen et du Conseil, 27 Avril 2016, art. 6.2.b).

¹¹⁶ Décision du Conseil portant création de l'Office européen de police (Europol), 06 Avril 2009.

¹¹⁷ Dir. PNR du Parlement européen et du Conseil, 27 Avril 2016, art. 10.1.

¹¹⁸ Ibid. art. 6.4

*d'“harmonisation minimale”, elle laisse donc à chaque État membre la possibilité d'étendre les obligations prévues par la directive par le biais du droit national ».*¹¹⁹ Ainsi les États ont-ils collecté les données passagers pour plusieurs buts différents comme l'amélioration des contrôles aux frontières ou la lutte contre l'immigration illégale. Cela remet en cause les principes de proportionnalité et de nécessité mis en avant par la législation du Parlement Européen et du Conseil dans le cadre de la lutte contre le terrorisme et autres infractions sérieuses.

Concernant les données API en elles-mêmes, le réexamen de la directive montre que « *la liste [des données API de l'article 3.2 de la directive] n'est pas exhaustive et les pays Membres peuvent demander des éléments de données additionnels en accord avec leur législation nationale* ». ¹²⁰ Toujours selon le réexamen de la Commission, « *la directive API n'est pas entièrement cohérente avec le cadre réglementaire international sur les informations relatives aux passagers dans la mesure où les champs de données sur les vols et les passagers (...) ne correspondent pas (...)* ». ¹²¹

En effet, l'équipe de l'OACI chargée de réviser l'annexe 9 et d'y ajouter de nouveaux SARPs a proposé pour standard 9.34 de laisser aux États contractants la possibilité de « *[conserver] la possibilité d'introduire ou de maintenir des niveaux de protection plus élevés des données PNR, selon leur cadre juridique et administratif* ». ¹²²

Toutes ces exceptions et différences de procédures remettent en cause la sécurisation des transferts de données passagers. Les Organisations Internationales devraient continuer à travailler à l'édiction de nouveaux standards internationaux afin de mieux encadrer et définir les éléments de données voués à être traités et transférés.

¹¹⁹ Traduit de l'anglais. Révision API 2020 p.8.

¹²⁰ Ibid. p. 16.

¹²¹ Ibid. p. 42.

¹²² Traduit de l'anglais. *Facilitation Panel 11th meeting, Recommendations for PNR SARPs*, 13 au 16 Janvier 2020, nouveau standard 9.34.b).

B. Les risques d'atteintes aux droits des passagers par la volonté de garantir la Sécurité et la Sûreté

Des failles dans la sécurisation des données passagers, sensibles et personnelles, peuvent constituer une atteinte à la vie privée des personnes. Les données transmises par les UIP sont régies par des dispositions relatives à leur conservation et leur dépersonnalisation. Ces transferts ne devraient être autorisés qu'en cas d'un niveau suffisant de protection du médium de communication et de la structure qui recevra les données. Les textes européens comme internationaux précisent ainsi que les traitements ne pourront pas porter sur des données pouvant être discriminatoires pour le passager. Est ainsi condamnée l'utilisation par les UIP de données telles que « *l'origine raciale ou ethnique, opinions politiques, religion ou convictions philosophiques, appartenance à un syndicat, état de santé, vie sexuelle ou orientation sexuelle.* ».¹²³ Selon l'article 6.1 de la directive PNR, les données recueillies, si différentes de celles listées à l'Annexe 1, devront être définitivement effacée dès leur réception par l'UIP.

Les passagers ont également certains droits sur leurs informations tels que les « *droits d'accès, de rectification, d'effacement et de limitation, et droits à réparation et à un recours juridictionnel prévus dans le droit de l'Union et le droit national (...).* ».¹²⁴ ainsi que celui « *d'être informés du traitement des données à caractère personnel les concernant* »¹²⁵. Ces informations devront être « *précises, aisément accessibles et facilement compréhensibles* ».¹²⁶ De plus, « *Lorsqu'une atteinte aux données à caractère personnel est susceptible d'entraîner un risque élevé pour la protection des données à caractère personnel ou d'affecter négativement la vie privée de la personne concernée, les États membres veillent à ce que l'UIP fasse part de cette atteinte à la personne concernée et à l'autorité de contrôle national sans retard injustifié.* ».¹²⁷

¹²³ Dir. PNR du Parlement européen et du Conseil, 27 Avril 2016, art. 13.4.

¹²⁴ Ibid. art. 13.1.

¹²⁵ Ibid. §29 p. 4.

¹²⁶ Ibid.

¹²⁷ Ibid. art. 13.8.

Les transferts des États membres de l'Union Européenne vers les États tiers sont autorisés s'ils remplissent « *les conditions prévues à l'article 13 de la décision-cadre 2008/977/JAI* »¹²⁸ et s'ils répondent « *aux principes de nécessité et de proportionnalité et au niveau de protection élevé conféré par la Charte et la CEDH.* ».¹²⁹

En Europe, tous les échanges entre les États membres entre eux et des États membres aux États tiers doivent respecter le même degré de confidentialité. Aux textes cités précédemment s'ajoutent pour ce type d'échanges le nécessaire respect d'instruments additionnels tels que le RGPD ou encore la convention n° 108.

Sur le point de la période de conservation des données, « *Les États membres veillent à ce que les données PNR fournies par les transporteurs aériens à l'UIP y soient conservées dans une base de données pendant une période de cinq ans (...)* ».¹³⁰ Parallèlement, il y est précisé que dans « *le cas où des données PNR spécifiques ont été transférées à une autorité compétente (...), la conservation de ces données par l'autorité compétente est régie par le droit national.* ».¹³¹

Il n'est pas précisé clairement dans ce cas de figure que les autorités compétentes destinataires des données ont l'obligation de supprimer ces données après 5 ans maximum de conservation. La directive reprecise que dans de pareils cas, « *leur durée de conservation par cette autorité devrait être fixée par le droit national, indépendamment des périodes de conservation de données prévues par la présente directive.* ».¹³² Selon le professionnel rattaché à AIRCOP, ces données normalement dépersonnalisées « *à l'expiration d'une période de 6 mois* »¹³³ suivant leur réception par l'UIP peuvent rester conservées et personnalisées plus de 25 ans dans les bases de données d'autorités nationales dès lors qu'elles sont utilisées dans une affaire liée au terrorisme ou à une enquête ou opération en cours.

¹²⁸ Ibid. art. 11.1.a).

¹²⁹ Ibid. §31 p. 4.

¹³⁰ Ibid. art. 12.1.

¹³¹ Ibid. Art 12.4.

¹³² Ibid. §26 p. 4.

¹³³ Ibid. art. 12.2.

Une autre zone grise mise en avant par la Commission lors de son réexamen de la directive API concerne l'obligation de supprimer les données API des passagers 24h après réception par l'UIP. Certains États membres ne respectent pas cette limite de 24h et se basent sur les dispositions de la directive PNR. En outre, « les États membres ont généralement fait usage de la possibilité incluse dans la directive API de stocker les données API pendant plus de 24 heures lorsque cela est nécessaire pour l'exercice de "fonctions statutaires". La plupart des pays d'application n'ont pas défini de limite de temps dans ce cas."¹³⁴

L'équipe de travail de l'OACI a également relevé que selon certains participants, « il était difficile d'établir une période de conservation fixe car les États peuvent avoir des lois différentes qui exigent une période de conservation plus longue ».¹³⁵

Il incombe aux Nations-Unies de veiller à ce que la lutte contre le terrorisme et autres infractions sérieuses n'engendre pas des atteintes aux données passagers sur le motif que cette lutte représente un intérêt général supérieur.

À l'international, les travaux de l'OACI et du Conseil de Sécurité s'inscrivent dans la volonté d'être plus protecteurs de ces données et d'arriver à un standard en la matière qui soit reconnu et appliqué par tous les États à travers le monde.

Cela s'observe par exemple dans le nouveau standard 9.25 paragraphes c) et d) proposé par l'équipe de travail de l'OACI relatif à l'information des passagers quant à la collecte de leurs données ainsi que l'ouverture et la transparence des États contractants quant à la collecte, l'utilisation, le traitement et la protection de ces données. Cette volonté d'uniformisation est aussi reprise par la résolution 2396 et la 2482 après elle.

¹³⁴ Traduit de l'anglais. Révi. API 2020 p. 20.

¹³⁵ Traduit de l'anglais. Facilitation Panel (...) §2.2.4. p.3.

C. Le manque de coopération spontanée entre UIP comme conséquence des lacunes du modèle

Les textes européens comme internationaux rappellent aux États l'importance d'échanger entre eux, y compris de manière spontanée. Le Parlement Européen et le Conseil rappellent que les « *États membres devraient échanger entre eux (...) les données PNR qu'ils reçoivent, lorsque cela est jugé nécessaire aux fins de la prévention et de la détection des infractions terroristes et des formes graves de criminalité, ainsi que des enquêtes et des poursuites en la matière. Les UIP devraient, le cas échéant, transmettre sans tarder le résultat du traitement des données PNR aux UIP des autres États membres en vue d'un complément d'enquête.* ».¹³⁶ Plus généralement, « *les États membres [doivent veiller] à ce que (...) toutes les données PNR pertinentes et nécessaires ou le résultat du traitement de ces données soient transmis par ladite UIP aux UIP correspondantes des autres États membres.* ».¹³⁷

C'est soutenu par la résolution 2396 du Conseil de Sécurité des Nations-Unies qui « *demande également aux États Membres, lorsqu'ils ont des informations sur le voyage, l'arrivée ou l'expulsion d'individus capturés ou détenus dont ils ont des motifs raisonnables de penser qu'il s'agit de terroristes, y compris les personnes soupçonnées d'être des combattants terroristes étrangers, de les communiquer, en temps voulu, notamment au pays d'origine, au pays de destination et, le cas échéant, aux pays de transit et à tous les pays dont les voyageurs en question ont la nationalité, et de leur communiquer toute autre information pertinente concernant ces personnes, et demande en outre aux États Membres de coopérer et de prendre au plus vite les mesures opportunes, dans le respect du droit international applicable, et de partager ces informations avec INTERPOL, selon qu'il convient ; (...)* ».¹³⁸

Cependant, la Commission européenne observe que « *le transfert de données PNR à la propre initiative de l'unité d'informations passagers est bien moins répandu.* »¹³⁹, l'expliquant par le fait que « *la formulation large et assez vague de la*

¹³⁶ Dir. PNR du Parlement européen et du Conseil, 27 Avril 2016, §23 p. 3.

¹³⁷ Ibid. art. 9

¹³⁸ Rés. 2396 du Conseil de sécurité, 21 Décembre 2017, p.6.

¹³⁹ Réexamen directive PNR 2020 p.10.

*disposition de la directive portant sur les transferts spontanés a suscité une certaine réticence lors son application. ».*¹⁴⁰

En sus de cette formulation large et assez vague, les problématiques soulevées précédemment relatives à la sécurisation des données passagers et des différentes exceptions aux procédures de transferts entre États sont autant de freins à cette spontanéité de communication entre UIP.

Par exemple, à la suite d'un transfert de données d'un État membre de l'Union Européenne à un État tiers, des « *transferts de données PNR [d'un État tiers à un autre État tiers] sans l'accord préalable de l'État membre dont les données ont été obtenues* »¹⁴¹ peuvent s'opérer. Les organes de l'Union Européenne n'imposent pas explicitement les mêmes niveaux de protection pour ces cas particuliers que pour le reste des échanges. Le Parlement Européen et le Conseil précisent uniquement que ces transferts devront respecter l'article 13§2 de la décision-cadre 2008/977/JAI qu'ils doivent être essentiels et ne peuvent être opérés que dans une situation où l'accord préalable n'a pas pu être donné à temps par l'État membre.

Autre exemple, les autorités compétentes peuvent formuler une demande d'informations directement auprès d'une UIP. En Europe, dans le cadre de ces demandes directes « *L'échange d'informations (...) peut avoir lieu par l'intermédiaire de n'importe quel canal de coopération existant (...)* ».¹⁴² Cette disposition manque de précision quant au niveau de sécurité requis de ces canaux. Il pourrait même s'agir de canaux non numériques, pourtant largement déconseillés par la Commission européenne.

Pour rappel, l'un des nouveaux standards proposés par l'équipe de travail de l'OACI laisse aux États contractants « *la possibilité d'introduire ou de maintenir des niveaux de protection plus élevés des données PNR, selon leur cadre juridique et*

¹⁴⁰ Ibid.

¹⁴¹ Dir. PNR du Parlement européen et du Conseil, 27 Avril 2016, art. 11.2.

¹⁴² Ibid. art. 9.5.

administratif » ainsi que la « *capacité de négocier des arrangements supplémentaires avec d'autres États contractants (...) pour (...) assurer un niveau supérieur de protection des données PNR* ». ¹⁴³ Ce manque d'uniformisation dans les garanties de protection, conservation et traitement des données entre les États n'encouragent pas les transferts. De trop hauts niveaux de protection risqueraient ainsi de paralyser les transferts avec les États destinataires n'ayant pas en place les structures d'accueil de ces données jugées nécessaires par l'État expéditeur.

PARTIE 2- L'ADAPTATION DU MODÈLE DES UIP À LA RECHERCHE D'UN SYSTÈME HARMONISÉ ET PERFORMANT

Le principal défi empêchant d'ériger l'UIP comme standard international repose sur la multiplicité des modèles qui ont été mis en place par les États. Les États, ayant à charge de transposer des résolutions et autres textes des entités internationales ayant une portée commune, doivent nécessairement apporter des modifications lors de l'adaptation en droit national. Certaines de ces adaptations de modèle peuvent se montrer inefficaces, d'autres peuvent mener à des atteintes dans la façon dont les procédures sont mises en œuvre. Le principe de l'UIP reposant sur la coopération nationale et internationale, son bon fonctionnement suppose l'assurance du respect par tous de ses principaux mécanismes prévus pour atteindre son objectif, d'autant plus que les données exploitées sont privées et sensibles. Ce respect doit pouvoir être contrôlé et assuré. Afin de permettre une adaptation au plus grand nombre, une réflexion sur la structure organisationnelle de l'UIP permettrait de déterminer le modèle le plus pertinent à adopter. La somme d'une structure adaptée et de processus de traitements optimisés et harmonisés permettrait de maximiser l'efficacité du modèle des UIP et de l'adapter en fonction des besoins.

¹⁴³ Traduit de l'anglais. *Facilitation Panel (...) Standard 9.34.b) et c).*

SECTION 1- L'encadrement de la pratique des États et la prise en compte de leurs spécificités nationales

Cet encadrement des pratiques Étatiques est nécessaire pour assurer la bonne cohésion et la bonne application du droit, mais il doit se faire dans le respect de la souveraineté de chaque État. Les spécificités nationales ne permettant de toutes les façons pas l'application mondiale d'un modèle exactement similaire à travers tous les pays, il est important de prendre en compte les modes de fonctionnement et les adaptations nationales afin de pouvoir permettre la meilleure application possible des normes internationales en fonction de chacun. Un encadrement efficace passe également par la nécessité de mise en œuvre de sanctions à titre dissuasif venant condamner les mauvaises pratiques.

I. Le respect de la souveraineté des États en parallèle de la mise en place d'un modèle commun

S'ils sont tenus par les normes internationales en vertu du principe de primauté, les États doivent tout de même être en capacité de pouvoir notifier un désaccord ou un différend relatif à l'application de certaines mesures. Certaines normes peuvent en effet entrer en conflit avec les systèmes déjà en place. Refuser le système des UIP en faveur d'un principe déjà en place est un choix qu'un État peut faire, tout comme celui de rajouter des mesures plus protectrices allant dans le sens du texte transposé.

A. Les observations formulées par les États quant aux résolutions des Nations-Unies

Lors de l'adoption de textes normatifs par le Conseil de Sécurité des Nations-Unies, l'OACI ou encore par le Parlement Européen et le Conseil, la possibilité est laissée aux États de pouvoir notifier leur désaccord ou leurs observations sur tout ou partie du texte. Ce mécanisme est en place car la coopération internationale doit composer avec la nécessaire reconnaissance de la

souveraineté des États sur leurs territoires. Lors de l'adoption de la directive 2016/681, le Royaume-Uni et l'Irlande ont par exemple notifié leur souhait d'application du texte malgré le protocole n°21¹⁴⁴ déjà en place. Le Danemark a quant à lui notifié sa volonté de ne pas participer à l'adoption de la directive ni d'être lié par celle-ci du fait du protocole n°22¹⁴⁵.

Les États de l'Union Européenne ont également la possibilité de formuler des demandes de décision préjudicielles ou de saisir la Cour de justice d'un renvoi préjudiciel pour s'assurer de la bonne conformité des directives avec d'autres textes tels que la Charte et le Traité. Ce fut le cas de la Belgique¹⁴⁶ et de l'Allemagne¹⁴⁷.

Les textes internationaux de l'OACI prévoient également des procédures afin de permettre aux États de notifier une différence ou un désaccord, notamment en se référant à la Convention de Chicago. Selon la Convention, « *Tout État qui estime ne pouvoir se conformer en tous points à l'une quelconque de ces normes ou procédures internationales, ou mettre ses propres règlements ou pratiques en complet accord avec une norme ou procédure internationale amendée, ou qui juge nécessaire d'adopter des règles ou des pratiques différant sur un point quelconque de celles qui sont établies par une norme internationale, notifie immédiatement à l'Organisation de l'aviation civile internationale les différences entre ses propres pratiques et celles qui sont établies par la norme internationale.* ».¹⁴⁸ Il en va de même pour les amendements qui, s'ils ne sont pas pris en considération et adaptés par l'État ou si adaptés différemment, devront être notifiés par l'État au Conseil qui notifiera telles différences aux autres États. Si cela n'est pas fait, alors l'État sera considéré comme étant en situation de non-conformité.

L'Union Européenne a ainsi mis en action cette notification de différence concernant les nouveaux standards et pratiques recommandées proposées par

¹⁴⁴ Protocole n°21 du TFUE sur la position du Royaume-Uni et de l'Irlande à l'égard de l'espace de liberté, de sécurité et de justice, 26 Octobre 2012.

¹⁴⁵ Protocole n°22 du TFUE sur la position du Danemark, 09 Mai 2008.

¹⁴⁶ Réexamen directive PNR 2020 p. 4.

¹⁴⁷ Ibid.

¹⁴⁸ Conv. Chicago art. 38.

l'équipe de travail de l'OACI. Tandis que cette équipe, à travers son standard 9.34.b) et c) proposait de reconnaître aux États la possibilité d'introduire de plus hauts niveaux de protection des données PNR et celle de négocier des arrangements supplémentaires entre eux, le Conseil de l'Union Européenne considéra que ses directives sont plus précises, notamment concernant la nécessité de se conformer au RGPD et à la Charte.

L'État devra alors remplir un Dépôt Électronique des Différences¹⁴⁹. Ce procédé se confronte cependant à deux principales limites. D'une part, les États ne notifient parfois pas ou incorrectement les différences entre leur système et les lignes directrices internationales. Notifier correctement une différence ou un désaccord par rapport à une norme internationale implique de saisir convenablement le sens et la portée de cette dernière. Les textes internationaux relatifs à l'implémentation d'un système unique de collecte de données API et PNR étant intentionnellement généraux et permissifs, identifier la manière selon laquelle un système national diffère de ce qui est attendu peut être complexe. S'ajoute à cela des difficultés pouvant être liées à la multiplicité de amendements apportés aux textes internationaux et aux délais à respecter pour la mise en conformité, souvent courts. D'autre part, la prise en compte de ces dépôts électroniques par la communauté internationale n'est pas immédiate et des pratiques non conformes ou non adaptées peuvent subsister et compromettre les interactions entre les États.

Ces notifications sont importantes afin de permettre une compréhension claire des pratiques générales, ce qui est fondamental dans des domaines comme la sécurité et la sûreté. La révision de cette procédure de notification doit être envisagée en ce qu'elle est une composante nécessaire du souhait d'établir un standard international.

B. La nécessité de composer avec les particularismes nationaux

¹⁴⁹ Traduit de l'anglais. *Electronic Filing Of Differences* (EFOD).

Le projet de développement des UIP à travers les États de la communauté internationale doit se faire en composant avec les particularités de chacun. Les organismes désignés par les Nations-Unies pour implémenter le Programme de lutte contre le terrorisme axé sur les déplacements doivent ainsi adapter la mise en place en fonction des structures déjà existantes et des contraintes des États bénéficiaires.

Le Programme ne doit pas tendre immédiatement vers un modèle unique d'UIP mais vers l'amélioration des systèmes déjà précédemment mis en place par les États, certains d'entre eux n'ayant parfois aucune base en matière de récupération de données passagers dans le but de la lutte contre le terrorisme et autres infractions sérieuses. Selon le professionnel rattaché à AIRCOP, la Gambie voit le programme des Nations Unies adapté à ses structures déjà en place, à savoir leur contrôles aux frontières et leur Centre de traitement pour les données API. Le Programme travaille donc à implémenter une collecte systématisée des données API et PNR des transporteurs.

Le Programme s'appuie sur le logiciel TRIP¹⁵⁰, rebaptisé goTravel. Ce logiciel permettant la collecte, l'analyse, la conservation et le partage des données passagers est offert à l'État bénéficiaire pour une durée de deux ans. Il n'est cependant pas obligatoire et la possibilité est laissée aux États de continuer à utiliser leur propre système, à condition qu'il respecte les obligations prévues par le droit international.

Au-delà des problématiques liées à la sécurité des transferts et de l'utilisation des données mentionnées précédemment, l'UNOCT reconnaît que « *La mise en place d'un système efficace et sûr est très complexe et onéreuse. Les États Membres risquent d'acquérir un système coûteux qui ne sera pas adapté à leur objectif ou de faire porter leurs efforts sur des domaines de la gestion des données personnelles présentant un intérêt marginal, sans commune mesure avec leurs besoins ou trop mal définis en termes opérationnels et juridiques par rapport à leur contexte national.* ».¹⁵¹

¹⁵⁰ Traveller Identification Programme/Programme d'identification voyageur

¹⁵¹ Programme de lutte contre le terrorisme axé sur les déplacements du BLT, p.2. (Cf. bibliographie).

C. La marge de manœuvre laissée aux États dans la transposition des textes internationaux

Les obligations internationales tendant vers l'uniformisation d'un modèle d'UIP à travers le monde doivent être mises en parallèle avec le nécessaire respect de la souveraineté des États sur leur territoire et le droit qui y est applicable. D'importantes variations dans la mise en place de dispositions internationales par les États peuvent ainsi être observées du fait de la transposition et l'adaptation dans le système législatif national qui en sont faites.

En Europe, la directive API ayant été rédigée dans le but de laisser aux États une grande marge de manœuvre « *la liste [de données API nécessaire] est non-exhaustive et les pays d'application peuvent demander des éléments de données supplémentaires conformément à la législation nationale que ceux listés à l'article 3(2) (...)* ». ¹⁵² Un autre manque de clarté de la directive porte sur sa finalité, ce qui mena les États à demander ces données pour atteindre des objectifs différents de la lutte contre le terrorisme comme celui de la lutte contre l'immigration illégale.

En sus des problématiques liées à la fixation arbitraire de la période de conservation des données, la directive PNR laisse aux États la possibilité de réexaminer ¹⁵³ les critères d'évaluation des passagers et ce, à intervalle régulier, permettant ainsi des différences de pratiques en fonction des critères retenus. De plus, il revient à chaque État membre d'arrêter « *une liste des autorités compétentes habilitées à demander aux UIP ou à recevoir de celles-ci des données PNR ou le résultat du traitement de telles données (...)* » ¹⁵⁴

¹⁵² Traduit de l'anglais. Révision API 2020 p.16.

¹⁵³ Dir. PNR du Parlement européen et du Conseil, 27 Avril 2016 art. 6.4.

¹⁵⁴ Ibid. art. 7.

Pour respecter le principe de souveraineté, aucune limite de désignation n'a été imposée par le Parlement Européen ou le Conseil. Elles doivent simplement être considérées comme compétentes dans le domaine du but recherché. Cependant, comme mentionné précédemment, ce but est susceptible de varier selon les États. Selon le professionnel de la BelPIU, l'UIP ne peut contester la désignation faite par son État de nationalité de ces autorités compétentes.

En plus d'autoriser un niveau plus élevé de protection et de permettre des arrangements supplémentaires entre États, l'équipe de travail auprès de l'OACI choisissait en 2020 de faire tendre ses standards vers la possibilité pour les États membres de « [mettre] en place un programme PNR [spécifique] ou [d'apporter] des changements importants à un programme déjà en place [et conforme] (...) »¹⁵⁵, à condition d'en informer les autres États. Ce programme devra être conforme aux normes et pratiques recommandées de l'OACI, permettant pourtant des différences de résultats dans leur application.

La nécessité de composer avec la souveraineté des États laisse la porte ouverte à autant de particularités qui doivent être surveillées afin de ne pas s'éloigner de la recherche d'un régime commun et de la finalité souhaitée.

II. L'importance de garanties et mesures pour le respect des bonnes pratiques des États

La souveraineté des États se traduit notamment par la possibilité qu'ils ont d'appliquer le droit qu'ils souhaitent sur leur territoire. Cette possibilité n'est cependant pas absolue et c'est particulièrement vrai dans le cas des UIP dont le modèle est basé sur la coopération internationale. Les États étant amenés à entretenir des relations pour le bon déroulement des procédures, et un État n'ayant pas autorité sur les pratiques ou le territoire d'un autre État, il est important que soient établies des garanties permettant la bonne application des dispositions relatives au respect des données passagers.

¹⁵⁵ Traduit de l'anglais. *Facilitation Panel (...) Standard 9.35.*

A. Les schémas de contrôle et de remontée de l'information à l'échelle de l'UIP pour la protection des données passagers

Il n'existe pas encore un modèle uniformisé d'UIP à travers le monde. Les États intègrent les dispositions internationales dans leur corpus juridique national, ce qui même à des niveaux différents de conformité. Ces UIP gèrent des données passagers sensibles telles que des informations de cartes bancaires ou encore des données médicales. Ainsi, il est important que soient prévus à leur échelle des mécanismes de contrôle afin de faire respecter les principes de confidentialité aux étapes de leur gestion, transferts, conservation ou encore de leur récolte.

La directive PNR charge ainsi les UIP de nommer « *un délégué à la protection des données chargé de contrôler le traitement des données PNR et de mettre en œuvre les garanties pertinentes* ». ¹⁵⁶ Ces délégués devront notamment être indépendants et représenter pour le passager le « *point de contact unique pour toutes les questions relatives au traitement des données PNR [le] concernant (...)* ». ¹⁵⁷ En plus de la vérification du traitement des données par l'UIP, le délégué sera prévenu en cas de transfert d'un État membre à un État tiers puis en cas de second transfert de ces données entre deux États tiers. ¹⁵⁸ Europol devra également le prévenir si elle procède à une demande auprès d'une UIP. ¹⁵⁹ Enfin, le délégué vérifiera *ex post* les transferts intégraux de données PNR de l'article 12.3 de la directive, ou encore les transferts opérés en urgence sans l'accord préalable de l'État de l'UIP à laquelle il se rattache.

Ayant « *accès à toutes les données traitées par l'UIP* », il pourra « *renvoyer l'affaire à l'autorité de contrôle nationale* » s'il « *estime que le traitement de certaines données n'était pas licite* ». ¹⁶⁰

¹⁵⁶ Dir. PNR du Parlement européen et du Conseil, 27 Avril 2016 art. 5.

¹⁵⁷ Ibid.

¹⁵⁸ Ibid. art. 11.4.

¹⁵⁹ Ibid. art. 10.3.

¹⁶⁰ Ibid. art. 6.7.

Cette autorité de contrôle nationale joue également un rôle important dans la vérification des bonnes pratiques de l'UIP. Ainsi, elle se verra mettre à disposition les registres de l'UIP, contenant des informations au moins sur « *la collecte, la consultation, la communication et l'effacement* ». ¹⁶¹ Elle se verra également notifiée « *lorsqu'une atteinte aux données à caractère personnel est susceptible d'entraîner un risque élevé pour la protection des données à caractère personnel ou d'affecter négativement la vie privée (...)* » d'un passager.¹⁶² Le reste de ses missions de surveillance et de conseil est prévu à l'article 15 de la directive PNR. Elle est également pourvue de pouvoirs effectifs d'intervention, peut saisir les institutions politiques, ester en justice, porter les violations à l'autorité judiciaire et ses réclamations pourront faire l'objet d'un recours juridictionnel.¹⁶³

Suivant le modèle de la directive PNR, l'équipe de travail de l'OACI enjoignit en 2020 dans ses SARPs les États contractants à désigner « *une ou plusieurs autorités nationales compétentes* »¹⁶⁴ afin d'occuper les mêmes fonctions que celles énoncées dans la directive.

Ce fonctionnement de ce modèle est en théorie efficace lorsqu'appliqué à un État récupérant les données PNR et API des transporteurs à travers une Fenêtre Unique. Cependant, certains États fonctionnent encore sur un modèle bicéphale avec les données API envoyées à un centre de ciblage (ou équivalent) détaché de l'UIP qui elle, se verra envoyer uniquement les données PNR.

Ces informations envoyées et conservées par ces centres de ciblage ne sont pas couvertes par les mêmes protections que les UIP. Du fait de la nature de ces données API qui ne demandent pas de traitement et leur délai de conservation normalement fixé à 24h, aucun délégué au sens de celui désigné par la directive PNR n'est mentionné. Cela est susceptible de créer des failles de sécurité car

¹⁶¹ Ibid. art. 13.6.

¹⁶² Ibid. art. 13.8.

¹⁶³ Décision-cadre 2008/977/JAI du Conseil, 27 Novembre 2008 art. 25.

¹⁶⁴ Traduit de l'anglais. *Facilitation Panel (...)* Standard 9.28.

alors aucun mécanisme de surveillance, de report et donc aucun recours n'est prévu.

B. Les pouvoirs de sanction des entités à l'échelle internationale pour l'exploitation appropriée des données passagers

À l'échelle internationale, l'application de sanctions est moins évidente du fait que les organes tels que le Conseil de Sécurité des Nations-Unies ou l'OACI sont des organes de guidance dans leur essence. L'OACI peut ainsi procéder à des audits afin de superviser les pratiques des États. C'est ce qu'elle fait notamment par le biais de l'USAP, le Programme universel d'audits de sûreté. Par le biais de ses SARPs, elle proposera aux États les bonnes pratiques qu'il conviendrait d'adopter.

Le Conseil va pour sa part pouvoir rendre des avis et statuer sur des « désaccords entre deux ou plusieurs États contractants à propos de l'interprétation ou de l'application de la [Convention de Chicago] et de ses Annexes (...) »¹⁶⁵ à condition que ce désaccord ne puisse être réglé par voie de négociation. La Cour permanente de Justice internationale ou le tribunal d'arbitrage *ad hoc* pourront également intervenir dans le cas où appel serait fait de la décision du Conseil.

Cependant ces procédures se font après saisine de la part des États. Le Conseil de Sécurité, s'il n'en est pas notifié, ne pourra ainsi pas se prononcer spontanément en cas de mauvaises pratiques telles que l'utilisation frauduleuses de données obtenues sans accord préalable, l'extension du temps de conservation des données API et PNR, la modification des critères d'évaluation pour le traitement de ces données ou encore la nomination par un État d'une autorité nationale non compétente à recevoir des données passagers au vu du but recherché.

¹⁶⁵ Conv. Chicago art. 84 et 54 j) et n).

La directive PNR autorise l'Union Européenne à « *prendre des mesures conformément au principe de subsidiarité consacré à l'article 5 du traité sur l'Union européenne* » et ce, conformément au principe de proportionnalité et sans excéder « *ce qui est nécessaire pour atteindre [les] objectifs.* ». ¹⁶⁶ En outre, la Cour de Justice de l'Union Européenne pourra sanctionner au terme d'une action en dommages et intérêts mais seulement si elle est saisie.

Les procédures les plus efficaces pour sanctionner une pratique non-conforme avec les textes internationaux restent appliquées au niveau national. Selon la directive PNR, « *Les États membres déterminent le régime des sanctions applicables aux violations des dispositions nationales adoptées en vertu de la présente directive et prennent toutes les mesures nécessaires pour assurer la mise en œuvre de ces sanctions.* ». ¹⁶⁷ En Europe s'est ainsi répandue une coopération entre les délégués à la protection des données et les autorités nationales compétentes dans le but de surveiller le bon respect des garanties de sécurité liées aux données passagers et d'en sanctionner les abus. En supplément, la Commission européenne devrait être en mesure de pouvoir user de son pouvoir d'engager des procédures d'infractions à l'encontre des États membres ne respectant pas les obligations contenues dans ses directives. Les États devant respecter la souveraineté des autres États, ce sont aux organes internationaux tels que la Commission ou l'ONU que reviendra la mission de faire respecter le droit en cas de violation par leurs membres.

C. Les différends entre les États et leurs transporteurs aériens quant aux exigences de leur mise en conformité

La multiplication des spécificités nationales et des différences de standards entre États a des retombées négatives sur les transporteurs aériens. La directive API de 2004 était déjà très peu protectrice des transporteurs en ce qu'elle prévoyait en son article 4 un régime de sanctions financières en cas de mauvais

¹⁶⁶ Dir. PNR du Parlement européen et du Conseil, 27 Avril 2016 §38 p. 5.

¹⁶⁷ Ibid. art. 14.

ou d'absence de transfert de leurs données sans prévoir de clause de modération dans la mise en place de ces sanctions. Le développement des textes relatifs aux données passagers, à leur protection, leur transfert et à leur traitement dans un contexte de développement de la menace terroriste et autres infractions graves par voie aérienne a mis les transporteurs dans une position difficile. La directive API, alors rédigée dans des termes permettant une bonne marge de manœuvre aux États, a entraîné la mise en place de multiples systèmes et structures de réception des données ainsi que différents standards de communication de ces données en fonction des pays. La Commission Européenne, lors de sa révision de ladite directive, a constaté que cette multitude de structures créait « *un fardeau pour les transporteurs en ce qu'il leur faut comprendre chaque modèle d'organisation national afin de transmettre les données API aux autorités nationales, et parfois régionales, pertinentes (...)* ». ¹⁶⁸

La multiplication des structures habilitées à recevoir les données ainsi que la trop grande variété de schémas de messages et de protocoles de transferts sont autant d'écueils dans lesquels peuvent tomber les transporteurs.

Ces derniers font également parfois face à des situations dans lesquelles ils sont juridiquement contraints par le pays de destination à révéler des informations relatives aux passagers alors que la législation du pays de départ leur interdit de les communiquer. L'équipe de travail de l'OACI a, à ce sujet, proposé une pratique recommandée selon laquelle « *les États membres ne [devraient pas pénaliser] les exploitants d'aéronefs pendant qu'ils essaient de résoudre les différends relatifs au transfert de données PNR.* ». ¹⁶⁹

Il existe certains cas particuliers dans l'aviation d'Affaires concernant les « *petits opérateurs [qui] n'utilisent pas de systèmes de réservation, les vols [étant] souvent réservés au tout dernier moment et l'itinéraire pouvant même changer après*

¹⁶⁸ Traduit de l'anglais. Révision dir. API 2020 p. 55.

¹⁶⁹ Standard 9.36.

le décollage »¹⁷⁰. Il leur est ainsi très difficile de pouvoir se conformer et éviter les sanctions.

Ainsi, face à la récurrence de ces problématiques, les deux approches principales consistent en « *l'engagement avec les transporteurs sans recourir aux sanctions et aux mesures d'exécution, et une approche plus directe de l'exécution agressive sanctionnant la non-conformité.* ».¹⁷¹

En cas d'application de sanctions pour non-respect de leurs obligations en matière de transfert de données PNR, l'Europe précise pour ses États qu'elles devront être « *effectives proportionnées et dissuasives, y compris [les] sanctions financières (...)* ».¹⁷² De la même manière, « *les États membres déterminent le régime des sanctions, y compris des sanctions financières, à l'encontre des transporteurs aériens qui ne transmettent pas de données comme le prévoit l'article 8, ou ne les transmettent pas dans le format requis.* ».¹⁷³ Ces sanctions devront également être effectives, proportionnées et dissuasives.

Les textes prévoient comme circonstance exonératoire « *les erreurs causées par une "défaillance des systèmes" dans la transmission des données API aux autorités.* ».¹⁷⁴ Cette position est reprise par l'équipe de travail de l'OACI lorsqu'elle propose comme standards que « *les États contractants n'imposeront pas d'amendes ou de sanctions aux exploitants d'aéronefs pour toute erreur inévitable causée par une panne des systèmes qui peut avoir empêché la transmission de données PNR ou entraîné la transmission de données PNR corrompues* ».¹⁷⁵

¹⁷⁰ Traduit de l'anglais. Révi. PNR 2020 art. 6.2.

¹⁷¹ Ibid. p. 18.

¹⁷² Dir. PNR du Parlement européen et du Conseil, 27 Avril 2016 §18 p. 3.

¹⁷³ Ibid. art. 14.

¹⁷⁴ Traduit de l'anglais. Révi. API 2020 p. 19.

¹⁷⁵ Traduit de l'anglais. *Facilitation Panel (...)* Standard 9.33 c).

L'équipe a également proposé comme nouveau standard que les États contractants « *chercheront, autant que possible, à limiter les contraintes opérationnelles et administratives pesant sur les exploitants d'aéronefs (...).* »¹⁷⁶

SECTION 2- L'harmonisation des pratiques au support d'un système d'UIP fiable et exportable

En matière de transmission et traitement de données passagers, les États n'ont pas arrêté de modèle unique mais ont parfois plusieurs structures différentes chargées de regrouper les données de transporteurs. Les Nations-Unies comme l'Union Européenne règlementent en faveur d'une centralisation de ces informations relatives aux passagers. L'UIP serait idéalement cette entité centralisant ces données afin de permettre une clarté dans les échanges internationaux, une structure de modèle comprise de tous. Telle réalisation permettrait d'améliorer le système déjà existant et d'étendre les limites des UIP à la fois vis-à-vis des acteurs du transport chargés de transmettre mais également par rapport à l'utilisation qui pourrait être faite de ces données, autre que la lutte contre le terrorisme et autres infractions sérieuses.

I. La composition de l'UIP comme variable importante dans la recherche d'une efficacité accrue

En matière de données passagers, le standard aujourd'hui mis en avant sur la scène internationale et poussé par les différents organes des Nations-Unies est celui d'une Fenêtre Unique, idéalement l'UIP, chargée de centraliser toutes les informations envoyées par les transporteurs aériens. Ces données seraient ensuite réparties spontanément ou sur demande des autorités compétentes. La réflexion sur la composition de l'UIP se rattache notamment au questionnement de sa légitimité à analyser et affirmer ou infirmer qu'il existe

¹⁷⁶ Ibid. standard 9.33.b.

une motivation suffisante pour obtenir certaines données alors qu'une mauvaise interprétation pourrait avoir de graves conséquences.

A. L'UIP comme Fenêtre Unique face aux nombreuses demandes formulées devant elle

Les États fonctionnant avec un système bicéphale ou pluricéphale de capture des données passagers peuvent être confrontés aux limites apportées par la multiplicité des procédures et aux difficultés que cette multiplicité pose vis-à-vis des transferts. La Fenêtre Unique est le modèle que les organes internationaux souhaitent ériger comme un standard afin de permettre une simplification des procédures, un système compréhensif et donc une mise en œuvre efficace. Les autorités compétentes s'adresseraient ainsi à une entité unique. Si cette façon de fonctionner est privilégiée, elle doit cependant composer avec le risque que les demandes ne se superposent pas.

Les autorités compétentes tendant à un objectif commun, elles peuvent être amenées à travailler sur un même cas et il peut arriver que certaines d'entre elles adressent à l'UIP une demande similaire. Au-delà de l'inconvénient d'avoir à traiter puis transférer plusieurs fois les mêmes données, cela peut également compromettre les procédures d'enquêtes du fait que deux autorités travaillent sur un même dossier sans s'en être mutuellement informées. Les UIP devraient vérifier si deux demandes similaires n'ont pas été introduites auprès d'elle et éventuellement mettre en relation les autorités qui ont formulé ces demandes similaires.

Différentes entités peuvent formuler des demandes, principalement les UIP d'autres États et les autorités compétentes de l'État de l'UIP ou d'un autre. Il est donc nécessaire d'éviter que cela mène à des doublons de demandes qui ralentiraient les recherches en matière de terrorisme et autres infractions sérieuses. Afin d'éviter cela, un axe de développement à envisager serait le renforcement de la coordination nationale ou internationale entre les autorités compétentes. Un système y ressemblant est mis en œuvre en Belgique, permettant aux autorités de lutte contre le crime de coopérer avec d'autres

autorités tendant au même but à travers l'Europe. C'est le système NAPL-2. Cette coordination éviterait cette multiplication de transferts de mêmes données.

Sur un plan opérationnel, une meilleure coopération éviterait que deux autorités se gênent dans leur travail en menant une investigation ou une opération similaire. Cela permettrait également une efficacité accrue dans le travail de ces autorités qui seraient amenées à communiquer entre elles.

B. La légitimité des UIP dans leur mission de contrôle des demandes adressées à elles

L'Europe, les Nations-Unies et l'OACI, à travers leurs textes, décrivent l'importance de la mise en place d'une Fenêtre Unique pour le traitement des données passagers, d'un système centralisé par lequel la totalité des demandes des autorités compétentes relatives aux données passagers passerait.

Ces demandes, nationales ou internationales, doivent être spécifiques, motivées ou encore nécessaires. Il reviendra ensuite à ce système centralisé, idéalement l'UIP, de faire droit à cette demande ou pas. Bien que les autorités requérant ces données tendent à un but commun qui est celui de la lutte contre le terrorisme et autres infractions sérieuses, chacune possède des méthodes de travail, procédures spécifiques et outils qui leurs sont propres.

Les UIP doivent ainsi juger de la motivation et de la nécessité de transmettre des données ou le résultat du traitement de ces données à ces différentes autorités. Cette analyse et ce jugement n'est pas évident car les UIP doivent déterminer ce qui est nécessaire aux autorités pour accomplir leurs missions. Déjà complexe à l'échelle nationale, cela peut se montrer d'autant plus délicat dès lors que les données ou le traitement de celles-ci sont demandés par des UIP d'États tiers ou directement par des autorités internationales dans le cadre des demandes urgentes par exemple. Un refus formulé par une UIP peut avoir de dramatiques conséquences sur la sûreté des États.

Cette problématique se présente également dans le cas des transferts spontanés de la part de l'UIP selon lesquels « *Les États membres s'assurent que toute concordance positive obtenue à la suite du traitement automatisé des données PNR (...) est réexaminée individuellement par des moyens non automatisés, afin de vérifier si l'autorité compétente (...) doit prendre des mesures en vertu du droit national.* ».¹⁷⁷

Encore une fois, l'UIP est un filtre qui doit déterminer la nécessité de transmettre des données aux autorités compétentes. Là encore, une mauvaise interprétation pourrait constituer une lourde atteinte à la sûreté.

Un autre nœud dans la procédure concerne les justifications invoquées par les requérants. Cette justification, ou motivation aux fins d'obtenir certaines informations passagers peut être formulée sans qu'aucun contrôle de sa véracité ne soit mis en place. Les UIP n'ayant qu'une perception partielle des enquêtes menées par les autorités compétentes, perception nourrie par les éléments fournis par lesdites autorités, elles ne sont pas toujours en mesure de pouvoir mener une analyse en profondeur et peuvent ainsi être amenées à transmettre les informations demandées sans saisir la portée de l'utilisation qui en sera faite.

Il existe également des situations dans lesquelles les UIP peuvent ne pas être habilitées à refuser des demandes qui lui sont présentées. Cela peut être le cas d'une demande formulée directement par l'État national de l'UIP.

C. L'adaptation structurelle du modèle de l'UIP au service d'une plus grande efficacité

Cette problématique de la légitimité des UIP à juger de la nécessité d'une demande par une autorité compétente nécessite une réflexion sur la structure de l'UIP en elle-même et sur ses capacités à comprendre, analyser et interpréter le travail qui va être fait par les autorités compétentes grâce aux données

¹⁷⁷ Dir. PNR du Parlement européen et du Conseil, 27 Avril 2016 art. 6.5.

qu'elles pourraient leur transmettre. De plus, le développement du système de réseau entre autorités compétentes décrit précédemment serait bénéfique mais il requerrait tout de même plusieurs requêtes, une à l'UIP puis une ou plusieurs autres aux autres autorités nationales compétentes si d'autres informations sont nécessaires, comme des informations fiscales ou autres.

Une première manière de pallier à ces faiblesses serait de permettre le regroupement d'experts indépendants détachés des différentes autorités nationales au sein d'une même UIP. Chacun agirait comme un point focal pour l'autorité dont il connaît le fonctionnement. Il existe une autre manière de faire que certains États appliquent déjà.

Le modèle Belge, appelé BelPIU, fait ainsi travailler en coopération la Police Fédérale, la Sûreté de l'État, le Service général du Renseignement et de la Sécurité et enfin l'Administration générale des Douanes et Accises. Elles ne travaillent pas directement dans l'UIP mais s'organisent comme un Hub avec l'UIP au centre.

Dans le modèle Finlandais, les demandes formulées auprès de l'UIP passent également par ces autorités et la coopération entre elles leur permet de déterminer la pertinence de faire suivre les informations aux demandeurs. Ce transfert se fera par l'autorité la plus compétente en la matière après concertation avec les autres autorités pour éviter les doublons. Pareillement, les données reçues des transporteurs sont directement accessibles à ces autorités qui n'auront pas besoin de présenter des demandes aux UIP pour pouvoir les exploiter.

Cette structure nucléaire s'appelle un *Fusion Center*, ou Centre de fusionnement en français. Il en existe également un au Botswana appelé "*Counter-Terrorism Analysis Fusion Agency*", et un autre en Sierra Leone tandis que l'UNOCT a en place un projet appelé "*Fusion Cell Project*"

De cette façon, tous les contrôles dans différentes bases de données sont directement opérés en même temps sans qu'il soit besoin de formuler une requête à l'UIP qui vérifiera dans sa base de données puis demandera la

vérification d'une autre information par le biais de la base de données d'une autre autorité. Cette vérification est faite sur des bases de données aussi bien nationales qu'internationales et l'information est également soumise aux listes de surveillances en vigueur comme celle d'INTERPOL.

Au niveau supranational, une autre possibilité serait de travailler à la formation d'UIP communes entre plusieurs États. Ce cas de figure est déjà prévu par la directive PNR¹⁷⁸. Qu'elle regroupe ou pas les autres autorités nationales, cette façon de fonctionner permettrait une amélioration de la coopération entre les États du fait de la facilitation des transferts d'informations entre eux et encouragerait le développement des transferts spontanés entre UIP encore trop peu répandu.

Il sera par la suite important de prévenir les autres États du fonctionnement du système national en place tant qu'il n'y aura pas d'uniformité de modèle. Les demandes pourront ainsi être formulées auprès des bons acteurs et cela évitera la confusion et le ralentissement des procédures, ce qui serait une atteinte au but final recherché.

II. Les différentes opportunités d'application pratique d'un modèle fonctionnel d'UIP

L'élaboration d'un modèle commun et fonctionnel d'UIP à l'international permettrait de pouvoir étendre le rayon d'action de ces unités par l'élargissement du rayon de captation d'informations passagers qu'elles seraient habilitées à recueillir. Ainsi les UIP pourraient-elle recueillir des données passagers d'autres acteurs du transport aérien mais également des transporteurs maritimes, ferroviaires ou encore routiers. Cela permettrait un meilleur suivi des personnes suspectées d'être liées à la criminalité organisée.

¹⁷⁸ Ibid. §13 p. 2.

Un modèle fonctionnel de gestion et d'analyse des données passagers pourrait également avoir d'autres applications utiles, si tant est que le cadre juridique de ces nouveaux buts soit bien défini.

A. La multiplication des accords bilatéraux et multilatéraux entre États

Les « *accords et arrangements bilatéraux ou multilatéraux* »¹⁷⁹ entre États sont permis par les textes internationaux qui leur laissent la possibilité d'introduire ou de maintenir des niveaux de protection plus élevés. Ils peuvent par exemple être conclus pour assurer une meilleure sécurisation d'une route jugée sensible et vulnérable aux flux criminels entre deux États, ou bien afin d'assurer une meilleure sécurité dans le transfert des données passagers.

Cependant la possibilité de passer de tels accords et arrangements reste aujourd'hui bridée et peut être limitée par certaines dispositions nationales prises par les États lors de la transposition des textes relatifs à la mise en place de systèmes comme celui des UIP. Ainsi, la France et le Canada envisagèrent-ils de conclure un accord entre eux qu'ils signèrent le 25 Juin 2014. La Cour de Justice de l'Union Européenne rendit un avis le 26 Juillet 2017 appelé Avis 1/15 de la Cour (grande chambre) dans lequel elle exprima que cet accord était partiellement en désaccord avec certains articles de la Charte des droits fondamentaux de l'Union européenne relatifs au transfert, à l'utilisation et la conservation de données sensibles.

Ces accords entre États sont encore très peu nombreux, particulièrement lorsque ces États ne font pas partie d'une structure politique ou d'un groupement commun. L'Europe par exemple n'en a conclu que trois.¹⁸⁰ Celui avec les États-Unis fut approuvé par le Parlement européen en avril 2012 et « [entra] en vigueur le 1^{er} Juillet 2012, remplaçant l'accord précédent qui datait de

¹⁷⁹ Ibid. art. 21.

¹⁸⁰ <https://www.europarl.europa.eu/news/fr/press-room/20150123BKG12902/directive-sur-les-donnees-des-dossiers-passagers-de-l-ue-donnees-pnr-apercu/10/accords-pnr-avec-des-pays-tiers>

2007 ». Celui avec l’Australie fut approuvé en octobre 2011. Malgré le refus de l’accord de 2014 avec le Canada, un autre de 2006 est toujours en vigueur.

Des autorisations de négociations ont été accordées par le Conseil de l’Union européenne avec le Japon, le Mexique et un nouveau avec le Canada. Ces accords peuvent ainsi permettre un plus haut niveau de coopération entre les États pour une lutte plus efficace contre le terrorisme et autres infractions sérieuses.

Harmoniser les prérequis et les dispositions nationales sur la conservation, le transfert et la conservation des données, entre autres mesures, serait un terrain favorable pour le développement de nouvelles coopérations internationales.

B. L’extension de la récolte des données passagers à d’autres acteurs du transport

Un autre point qui permettrait une lutte plus efficace contre le terrorisme et autres infractions sérieuses serait d’étendre la possibilité pour les UIP de réunir des données passagers supplémentaires à celles transmises par les transporteurs aériens. Les UIP pourraient par exemple bénéficier de données passagers des domaines maritimes, ferrés et routiers. Certains États en prévoient déjà la récolte par leur UIP. En date de 2020, « dix États européens [collectaient] ces données des transporteurs maritimes, quatre [du ferroviaire] et un des bus et cars ».¹⁸¹

Le professionnel de la BelPIU expliquait que cette dernière travaillait déjà sur la collecte des données du transport par trains à grande vitesse mais également bus internationaux et par la voie maritime ainsi que sur les données recueillies par les agences de voyages. Ces procédés seront prochainement officialisés par décrets royaux. Cette extension est prévue par la directive PNR.¹⁸²

¹⁸¹ Traduit de l’anglais. Révi. API 2020 p. 15.

¹⁸² Dir. PNR du Parlement européen et du Conseil, 27 Avril 2016 §33 p. 4.

Concernant les données passagers récoltées auprès des acteurs de l'aérien en Europe, certains opérateurs économiques ne sont pas concernés par cette obligation de transmettre leurs données. C'est le cas des agences de voyages et autres entreprises privées par exemple. Une extension de l'obligation de transmission de données à ces entités permettrait de développer la capacité de détection et d'analyse des UIP en accroissant les données par la suite exploitables par les agences visant à faire respecter la loi.

Cette extension ne pourrait être décidée qu'après une analyse de sa nécessité et de ses conséquences sur les acteurs concernés. En effet, le fait de mettre en place de tels mécanismes représente un investissement en termes de coût et demande une restructuration des systèmes en place.

La Commission, lors de son réexamen de 2012 puis 2020 de la directive API et après avoir sollicité les États membres sur la question, avait présenté la position des compagnies aériennes quant aux avantages pour elles de mettre en place un système de récolte de données passagers comme prévu par la directive. Ces transporteurs considèrent qu'il n'y avait « *pas de différence significative en termes d'impacts observés ou perçus* ». ¹⁸³ Cependant, les impacts positifs relevés par les autorités nationales et les résultats enregistrés dans la lutte contre le crime transnational montrent que malgré ce manque de nécessité relevé par les transporteurs, tel fonctionnement est très bénéfique à l'autre bout de la chaîne. Ainsi l'extension à d'autres acteurs de l'aérien de ces obligations relatives aux données passagers pourrait s'avérer très utile dans le but poursuivi par les UIP.

Sur le point de la variété des données capturées, la transmission de certaines informations supplémentaires pourrait être pertinente telles que « *les informations sur les places et les données relatives aux bagages, que la plupart des transporteurs récoltent* ». ¹⁸⁴ Pour permettre un élargissement des données récoltées, il faudrait justifier de la nécessité et de la proportionnalité de cette collecte afin d'être en accord avec le RGPD.

¹⁸³ Traduit de l'anglais. Révi. API 2020 p. 30.

¹⁸⁴ Ibid. p. 29.

A l'internationale, cette extension aux domaines autres que l'aérien est progressivement réglementée. Ainsi, au cours de sa 103^e session, le Comité de la Sécurité Maritime de l'Organisation Maritime Internationale approuvait les « *mesures pour l'amélioration de la sécurité maritime à travers l'API et la PNR pour les navires de croisière et les autres modes de transport maritime.* ». ¹⁸⁵

La collecte de ces données serait donc un véritable apport à la mission de l'UIP de garantir plus de sûreté des divers types de trafic, à condition que les UIP sachent analyser et transmettre convenablement ces données venant d'autres modes de transport que l'aérien. Les déplacements des criminels s'en retrouveraient davantage entravés et leur suivi pourrait se poursuivre à l'intérieur des territoires et aux points d'entrée ou de liaisons nationales autres qu'aériens.

C. La plus grande variété des finalités de l'utilisation des données par les UIP

Un modèle fonctionnel d'UIP, en plus de permettre une facilitation du partage d'informations aux niveaux national et international ainsi qu'une récolte de données élargie à d'autres modes de transport, autoriserait potentiellement l'utilisation de ces données pour tendre vers des finalités autres que celle de la lutte contre le terrorisme et autres infractions sérieuses.

La récolte des données passagers est un outil puissant permis par la coopération des États. Le but recherché par son biais doit être clairement défini pour réduire les risques d'utilisation frauduleuse ou de dérives. Principalement exploitées à des fins sécuritaires du fait du contexte international troublé par l'émergence d'un nouveau type de menace, ces données et les systèmes mis en place pour les traiter pourraient avoir une application pratique liée à un autre domaine.

¹⁸⁵ Traduit de l'anglais. Annexe 1 mémoire.

Lors de la révision de la directive PNR en 2020, « *plusieurs États membres ont également souligné que l'utilisation des données PNR pourrait constituer un outil précieux pour protéger la santé publique et prévenir la propagation de maladies infectieuses, par exemple en facilitant le traçage des personnes qui ont été assises près d'un passager infecté.* »¹⁸⁶ La Lettonie par exemple a mis en place la collecte des données PNR pour des raisons médicales car la pandémie a été érigée comme une menace nationale.

La pratique de la récolte de données dans le but du traçage de personnes à risque d'infection eut cours lors de l'émergence de la Covid-19 afin de déterminer les voyageurs en provenance de la Chine suite à un vol direct ou avec escale. Ces nouvelles mesures prises en urgence et à une échelle sans précédent ont pu entraîner des atteintes à la nécessaire confidentialité des données personnelles du fait d'une absence de réglementation. Le but justifiant la récolte, le traitement et le transfert de ces données n'était plus correctement défini et les pratiques furent très disparates.

Ainsi, afin qu'une extension des objectifs recherchés puisse être envisagée, il sera important d'établir avec précision un cadre venant délimiter le but de la collecte des données afin d'éviter les mauvaises pratiques que l'on retrouve déjà dans la lutte contre le terrorisme et autres infractions sérieuses. Cette délimitation précise permettrait d'établir rapidement un standard qui soit efficace.

En matière de santé, le cadre devra également fixer une limite en termes de durée de mise en œuvre des procédures car le but recherché, c'est-à-dire le traçage de personnes directement ou indirectement concernées par une infection, n'est pas un but permanent. Il est conjoncturel en fonction de la situation sanitaire et ne suit pas une logique de prévention mais, au contraire, de réaction vis-à-vis d'une épidémie. Il s'agirait donc d'en déclencher l'application, à l'inverse du domaine de la lutte contre le crime qui doit suivre une logique préventive.

¹⁸⁶ Révi. PNR 2020 art. 3.3.

Cette réflexion pourrait être abordée lors du Symposium mondial de l'OACI sur la sûreté de l'Aviation qui se tiendra de manière virtuelle du 08 au 10 Septembre 2021. Il s'intitulera « *Business NOT as usual* »¹⁸⁷ et abordera les questions de l'impact et des conséquences de la Covid-19 sur le transport aérien.

¹⁸⁷ Traduction française : Les affaires PAS comme d'habitude.

CONCLUSION

Depuis le développement des Unités d'Informations Passagers, les États reportent une amélioration dans le nombre de crimes et de tentatives d'attentats déjoués. Par exemple, trois mois après la mise en place de la BelPIU, la Belgique avait déjà recensé 834 correspondances avec les bases de données de police. Ces correspondances correspondaient à des profils liés à des crimes graves.¹⁸⁸

La coopération internationale est un outil efficace de lutte contre ces crimes et le terrorisme, un type de criminalité particulier qui n'a aucune base légale et est imprévisible.

La sûreté aérienne, déjà perfectionnée de par les initiatives des États en la matière et le regard de la communauté internationale sur ces questions, continue encore à se renforcer. Cela s'observe par exemple par l'extension à venir de la compétence des UIP, que ce soit par la captation de données passagers provenant d'acteurs plus variés de l'aérien ou par la récolte de ces données provenant d'autres modes de transports.

Ce renforcement est nécessaire car la menace terroriste est toujours d'actualité et s'adapte aux évolutions des législations et actions la visant.

Ce mécanisme des UIP comporte toujours des défauts et faiblesses que cette étude tente de mettre en lumière tout proposant un début de réflexion sur l'amélioration du système.

Le travail à l'échelle nationale a son importance mais la coopération internationale par un système commun reste plus efficace encore car elle permet une vision générale au-delà des frontières des États et la possibilité de

¹⁸⁸ <https://centredecrise.be/fr/news/securite-au-quotidien/interet-europeen-pour-la-nouvelle-direction-belpiu-du-centre-de-crise>

grouper les forces et capacités afin d'anticiper le terrorisme et autres crimes sérieux.

L'enjeu fondamental d'une coopération efficace est la sûreté et sécurité internationale. Cet enjeu dépend de l'efficacité des procédures en place concernant les transports aériens, maritimes et terrestres qui sont les points d'entrée dans les États et dont la surveillance étroite permettra de réduire les potentielles menaces sur le reste des territoires.

BIBLIOGRAPHIE

I. Traités (dont internationaux) et manuels

Annexe 9 de 2017.

http://www.icscc.org.cn/upload/file/20200508/20200508100922_97215.pdf

Conseil de l'Union Européenne - Décision (UE) 2019/2036 du Conseil, « relative à la position à prendre, au nom de l'Union européenne, au sein du Conseil de l'Organisation de l'aviation civile internationale en ce qui concerne l'amendement 17 de l'annexe 17 («Sûreté») de la convention relative à l'aviation civile internationale », 25 novembre 2019.

<https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32019D2036&from=EN>

Conseil de l'Union européenne - Directive 2001/51/CE du Conseil, visant à compléter les dispositions de l'article 26 de la convention d'application de l'accord de Schengen du 14 juin 1985, 28 juin 2001.

<https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32001L0051&from=FR>

Convention de Chicago, Protection de l'Aviation Civile Internationale contre les actes d'intervention illicite - Annexe 17, Décembre 1992.

https://www.senat.fr/rap/195-016/195-016_annexe1.pdf

OACI - Convention relative à l'aviation civile internationale, neuvième édition, 2006.

https://www.wipo.int/edocs/lexdocs/treaties/en/icao-ca/trt_icao_ca_002en.pdf

OACI - Normes et pratiques recommandées internationales, Annexe 9 à la Convention relative à l'aviation civile internationale, Octobre 2017.

https://www.icao.int/WACAF/Documents/Meetings/2018/FAL-IMPLEMENTATION/an09_cons_fr.pdf

Union européenne - Acquis de Schengen - Convention d'application de l'Accord de Schengen du 14 juin 1985 entre les gouvernements des États de l'Union économique Benelux, de la République fédérale d'Allemagne et de la République française relatif à la suppression graduelle des contrôles aux frontières communes, 22 septembre 2000.

[https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:42000A0922\(02\):fr:HTML](https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:42000A0922(02):fr:HTML)

Union européenne - Acquis de Schengen - Décision du Comité exécutif concernant l'introduction et l'application du régime Schengen dans les aéroports et les aérodromes [SCH/Com-ex (94) 17, rev. 4], 22 décembre 1994.

<https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:41994D0017&from=EN>

Union européenne - Programme de Stockholm, 2010.

<https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=LEGISSUM:jl0034&from=FR>

Union Européenne - Protocole (N°21) sur la position du Royaume-Uni et de l'Irlande à l'égard de l'espace de liberté, de sécurité et de justice, 26 octobre 2012.

<https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A12012E%2FPRO%2F21>

Union Européenne - Protocole (N°22) sur la position du Danemark ,9 mai 2008.

<https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A12008E%2FPRO%2F22>

Union européenne - Traité de Lisbonne modifiant le traité sur l'Union européenne, le traité instituant la Communauté européenne et certains actes connexes, 13 décembre 2007.

<https://www.assemblee-nationale.fr/13/projets/PL%20690%20Traite.pdf>

Union européenne - Traité sur l'Union européenne (version consolidée), 26 octobre 2012.

https://eur-lex.europa.eu/resource.html?uri=cellar:2bf140bf-a3f8-4ab2-b506-fd71826e6da6.0002.02/DOC_1&format=PDF

II. Articles physiques et en ligne

API-PNR France - Transposition par la France de la directive Européenne PNR 2016/681, 27 avril 2016.

<https://pnr.gouv.fr/Actualites/Transposition-par-la-France-de-la-directive-Europeenne-PNR-2016-681-du-27-avril-2016>

European Digital Rights (EDRi) - Denmark prepares for passenger data exchange with the EU, 19 Decembre 2018.

<https://edri.org/our-work/denmark-prepares-for-passenger-data-exchange-with-the-eu/>

Nations Unies, Bureau de lutte contre le terrorisme - Programme de lutte contre le terrorisme axé sur les déplacements.

https://www.un.org/cttravel/sites/www.un.org.cttravel/files/general/french_ct_travel_programme_summary_0.pdf

Nations Unies, Bureau de lutte contre le terrorisme - Renforcement des capacités de détection.

<https://www.un.org/counterterrorism/fr/countering-terrorist-travel>

Nations Unies - *Coordination and coherence of the counter-terrorism efforts of the United Nations.*

<https://www.un.org/counterterrorism/ctitf/>

Nations Unies - *goTravel Technical Introduction.*

<https://www.un.org/cttravel/fr/goTravel>

Nations Unies - Mandat de l'Assemblée générale des Nations Unies sur la création du Bureau de lutte contre le terrorisme, 15 juin 2017.

<https://www.un.org/counterterrorism/fr/about>

Nations Unies - Piliers de la Stratégie antiterroriste mondiale des Nations Unies.

<https://www.un.org/counterterrorism/fr/un-global-counter-terrorism-strategy>

Nations Unies - *United Nations Countering Terrorist Travel Programme, goTravel Brochure.*

https://www.un.org/cttravel/sites/www.un.org.cttravel/files/ctt_brochure_web.pdf

OACI - *Facilitation Programmes*.

<https://www.icao.int/Security/FAL/Pages/default.aspx>

OACI - *ICAO TRIP (Traveller Identification Programme)*.

<https://www.icao.int/security/FAL/TRIP/Pages/default.aspx>

OACI - La mise en œuvre de normes relatives à l'échange de données sur les passagers est essentielle au contre-terrorisme et à la prévention de crimes graves, 31 mai 2021.

<https://www.icao.int/Newsroom/Pages/FR/Implementation-of-passenger-data-exchange-standards-crucial-to-counter-terrorism-and-prevention-of-serious-crime.aspx>

OACI - Le Programme universel d'audits de sûreté (USAP) et son objectif.

https://www.icao.int/Security/USAP/Pages/FR/default_FR.aspx

OACI - Nouvel amendement des normes sur les données PNR pour renforcer les efforts mondiaux de lutte contre le terrorisme, 3 juillet 2020.

<https://www.icao.int/Newsroom/Pages/FR/New-PNR-Data-Standards-amendment-to-improve-global-counterterrorism-efforts.aspx>

Parlement européen - Accords PNR avec des pays tiers, 1er juin 2016.

<https://www.europarl.europa.eu/news/fr/press-room/20150123BKG12902/directive-sur-les-donnees-des-dossiers-passagers-de-l-ue-donnees-pnr-aperçu/10/accords-pnr-avec-des-pays-tiers>

Représentation permanente de la France auprès de l'OACI - Dossier : L'OACI et la Sûreté mondiale de l'aviation, 14 avril 2021.

<https://oaci.delegfrance.org/Dossier-L-OACI-et-la-Surete-mondiale-de-l-aviation>

United Kingdom Parliament - Passenger Name Record (PNR) data: updating international standards and negotiating an EU/Japan PNR Agreement, 23 avril 2020.

<https://publications.parliament.uk/pa/cm5801/cmselect/cmeuleg/229-xiii/22908.htm>

III. Rapports publics

Ademola Oladele, RO AVSEC/FAL, ICAO, *“Implementing Biometrics and Advanced Passenger Information (API)”*, 19 au 21 mars 2019.

<http://www.worldsecurity-index.com/shareDir/documents/15537969400.pdf>

AGNU - Résolution 72/284 « Examen de la Stratégie antiterroriste mondiale des Nations Unies », 26 Juin 2018.

<https://documents-dds-ny.un.org/doc/UNDOC/GEN/N18/198/81/PDF/N1819881.pdf?OpenElement>

Commission Européenne - Conclusions de la Présidence Conseil Européen de Bruxelles, 25 et 26 mars 2004.

https://ec.europa.eu/commission/presscorner/detail/fr/DOC_04_1

Commission Européenne - Décision d'exécution (UE) 2017/759 de la Commission, « sur les protocoles communs et formats de données devant être utilisés par les transporteurs aériens lors d'un transfert de données PNR aux unités d'information passagers. Schémas de messages à utiliser en Europe pour transferts », 28 avril 2017.

<https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32017D0759&from=EN>

Commission européenne - Rapport au Parlement européen et au Conseil « sur le réexamen de la directive 2016/681 relative à l'utilisation des données des dossiers passagers (PNR) pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière », 24 juillet 2020.

<https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:52020DC0305&from=FR>

Conseil de l'Europe - Convention 108 +, Convention du Conseil de l'Europe, « pour la protection des personnes à l'égard du traitement des données à caractère personnel », 18 mai 2018.

<https://rm.coe.int/convention-108-convention-pour-la-protection-des-personnes-a-l-egard-d/16808b3726>

Conseil de l'Europe - Convention du Conseil de l'Europe, « pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel », 28 janvier 1981.

<https://rm.coe.int/1680078b39>

Conseil de l'Europe - Décision 2005/671/JAI du Conseil, « relative à l'échange d'informations et à la coopération concernant les infractions terroristes », 20 septembre 2005.

<https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32005D0671&from=SL>

Conseil de l'UE - Décision (UE) 2019/2107 « relative à la position à prendre, au nom de l'Union européenne, au sein du Conseil de l'Organisation de l'aviation civile internationale, en ce qui concerne la révision du chapitre 9 de l'annexe 9 (Facilitation) de la convention relative à l'aviation civile internationale en ce qui concerne les normes et pratiques recommandées en matière de données des dossiers passagers », 28 novembre 2019.

<https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32019D2107&from=EN>

Conseil de l'Union Européenne - Décision-cadre 2006/960/JAI du Conseil, « relative à la simplification de l'échange d'informations et de renseignements entre les services répressifs des États membres de l'Union européenne », du 18 décembre 2006.

<https://eur-lex.europa.eu/legal-content/fr/TXT/?uri=CELEX:32006F0960>

Conseil de l'Union Européenne - Décision-cadre 2008/977/JAI du Conseil, « relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale », 27 novembre 2008.

<https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32008F0977>

Conseil de l'Union Européenne - Décision du Conseil, « autorisant l'ouverture de négociations avec le Japon en vue d'un accord entre l'Union européenne et le Japon sur le transfert et l'utilisation de données des dossiers passagers (PNR) afin de prévenir et de combattre le terrorisme et les formes graves de criminalité transnationale », 4 février 2020.
<https://data.consilium.europa.eu/doc/document/ST-5378-2020-INIT/fr/pdf>

Conseil de l'Union Européenne - Directive 2004 / 82 / CE du Conseil, « concernant l'obligation pour les transporteurs de communiquer les données relatives aux passagers », 29 avril 2004.
<https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32004L0082&from=EN>

Conseil Européen - Conclusions de la Présidence du Conseil Européen, « sur la poursuite des objectifs de l'UE en matière de croissance et d'emploi et sur les questions internationales, notamment le Proche-Orient, l'Irak et le Kosovo », 26 mars 2004.
<https://www.vie-publique.fr/discours/149012-conclusions-de-la-presidence-du-conseil-europeen-sur-la-poursuite-des-ob>

Conseil Européen - Conclusions et Plan d'action du Conseil Européen extraordinaire, 21 septembre 2001.
https://www.senat.fr/fileadmin/Fichiers/Images/commission/affaires_europeennes/Conclusions_CE/bruxelles_sept2001.pdf

Conseil Européen - Déclaration du Conseil européen, « sur le terrorisme (avec l'annexe 1 "Objectifs stratégiques de l'Union européenne dans la lutte contre le terrorisme" et la déclaration sur la solidarité contre le terrorisme) », 25 mars 2004.
<https://www.vie-publique.fr/discours/148171-declaration-du-conseil-europeen-sur-le-terrorisme-avec-lannexe-1-obje>

CVRIA - Avis 1/15 de la Cour (grande chambre), 26 juillet 2017.
[https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:62015CV0001\(01\)&from=EN](https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:62015CV0001(01)&from=EN)

European Commission - Evaluation of the « Council Directive 2004/82/EC on the obligation of carriers to communicate passenger data (API Directive) », 08 septembre 2020.
<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=SWD:2020:174:FIN&rid=10>

European Commission - Evaluation of the European Commission, « on the implementation and functioning of the obligation of carriers to communicate passenger data set up by Directive 2004/82 », 17 septembre 2012.
https://ec.europa.eu/home-affairs/sites/default/files/e-library/documents/policies/irregular-migration-return/return-readmission/docs/evaluation_of_the_api_directive_en.pdf

European Commission - Proposal for a Council decision “on the position to be taken on behalf of the European Union in the International Civil Aviation Organization as regards Amendment 28 to Annex 9 Section D to the Convention on International Civil Aviation”, 12 janvier 2021.
<https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021PC0016&rid=6>

European Commission - Study on Advance Passenger Information (API), Evaluation of Council Directive 2004/82/EC, « on the obligation of carriers to communicate passenger data », Février 2020.

<https://op.europa.eu/en/publication-detail/-/publication/3ef3a394-5dcb-11ea-b735-01aa75ed71a1/language-en/format-PDF>

ICAO - A40-10: *Addressing Cybersecurity in Civil Aviation*.
<https://www.icao.int/cybersecurity/Documents/A40-10.pdf>

ICAO - Document 9944, « *Guidelines on Passenger Name Record (PNR) Data* », 1st edition 2010.
https://www.icao.int/Security/FAL/ANNEX9/Documents/9944_cons_en.pdf

ICAO EUR - NAT Office -Paris, « *Annex 9 -Facilitation, Amendements 27 and 28 to Annex 9* », 2020.
<https://www.icao.int/EURNAT/Other%20Meetings%20Seminars%20and%20Workshops/2021%20FAL%20Seminar/2021%20FAL%20Sem%20PPT02.pdf>

ICAO - *Guidelines on Advance Passenger Information (API)*, 2010
<https://www.icao.int/Security/FAL/Documents/2010%20API%20Guidelines%20Final%20Version.ICAO.2011%20full%20x2.pdf>

ICAO - *Guidelines on Advance Passenger Information (API)*, 2014
https://www.iata.org/contentassets/18a5fdb2dc144d619a8c10dc1472ae80/api-guidelines-main-text_2014.pdf

ICAO/Interpol, *Passenger Data Exchange Forum - Building Capacity of Member States in API/PNR Implementation*, 27 - 28 mai 2021.
<https://www.icao.int/Meetings/TRIP-Symposium-2021/PublishingImages/Pages/Presentations/Global%20Programs%20and%20Solutions%20for%20APIPNR.pdf>

ICAO - *Report of the FALP PNR-TF, on “Recommendations for PNR SARPs”*, 13-16 janvier 2020.
<https://www.icao.int/Meetings/FALP/Documents/FALP11-2020/FALP11.IP1.PNRTF%20Report.pdf>

Jitu Thaker, *Technical Officer ICAO - Electronic Filing Of Differences (EFOD) System : Background and Introduction*, 12 mars 2018.
<https://www.icao.int/MID/Documents/2018/Regional%20FAL%20Seminar/PPT5.pdf>

Nations Unies - *Rapport de la conférence de haut niveau des Nations Unies sur la lutte contre le terrorisme*, 28-29 juin 2018.
<https://www.un.org/counterterrorism/ctitf/sites/www.un.org.counterterrorism.ctitf/files/18-14992-F-Report-Counter-Terrorism-FR.pdf>

Nations Unies - *Résolution adoptée par l'Assemblée générale, « Renforcer la capacité du système des Nations Unies d'aider les Etats Membres à appliquer la stratégie antiterroriste mondiale des Nations Unies*, 15 juin 2021.
<https://documents-dds-ny.un.org/doc/UNDOC/GEN/N17/172/59/PDF/N1717259.pdf?OpenElement>

Nations Unies - Rapport du Secrétaire général, « Capacité du système des Nations Unies d'aider les États Membres à appliquer la Stratégie antiterroriste mondiale des Nations Unies », 3 avril 2017.

<https://documents-dds-ny.un.org/doc/UNDOC/GEN/N17/088/94/PDF/N1708894.pdf?OpenElement>

Nations Unies - Résolution 2178 (2014) adoptée par le Conseil de sécurité à sa 7272e séance, 24 septembre 2014.

<https://documents-dds-ny.un.org/doc/UNDOC/GEN/N14/547/99/PDF/N1454799.pdf?OpenElement>

Nations Unies - Résolution 2309 (2016) adoptée par le Conseil de sécurité à sa 7775e séance, 22 septembre 2016.

<https://documents-dds-ny.un.org/doc/UNDOC/GEN/N16/295/79/PDF/N1629579.pdf?OpenElement>

Nations Unies - Résolution 2396 (2017) adoptée par le Conseil de sécurité à sa 8148e séance, 21 décembre 2017.

<https://documents-dds-ny.un.org/doc/UNDOC/GEN/N17/460/26/PDF/N1746026.pdf?OpenElement>

Nations Unies - Résolution 2482 (2019) adoptée par le Conseil de sécurité à sa 8582e séance - 19 juillet 2019.

<https://documents-dds-ny.un.org/doc/UNDOC/GEN/N19/224/99/PDF/N1922499.pdf?OpenElement>

Nations Unies - Résolution adoptée par l'Assemblée générale, « Septième examen de la Stratégie antiterroriste mondiale de l'Organisation des Nations Unies », 30 juin 2021.

<https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/175/71/PDF/N2117571.pdf?OpenElement>

OACI - Plan pour la sécurité de l'aviation dans le monde, édition 2020-2022, 2020.

https://www.icao.int/publications/Documents/10004_fr.pdf

OACI - Plan pour la sûreté de l'aviation dans le monde, première édition, 2017.

<https://www.icao.int/Security/Documents/GLOBAL%20AVIATION%20SECURITY%20PLAN%20FR.pdf>

OACI - Résolutions adoptées par l'Assemblée à sa 39e session, 06 octobre 2016.

https://www.icao.int/Meetings/a39/Documents/Resolutions/a39_res_prov_en.pdf

OACI - Soutien de la mise en œuvre et du développement (ISD), Programme de sûreté (ISD - SÛRETE), 2 novembre 2010.

https://www.icao.int/ESAF/Documents/meetings/2010/esaf_dgca4/docs/wp09_fr.pdf

OACI - Stratégie globale OACI de sûreté de l'aviation (ICASS), Plan d'action stratégique 2011-2016, 28 juin 2010.

https://www.icao.int/Meetings/AMC/Assembly37/Working%20Papers%20by%20Number/wp018_fr.pdf

OSCE - Décision No 6/16, « Renforcement de l'utilisation des renseignements préalables concernant les voyageurs », 9 décembre 2016.

<https://www.osce.org/files/f/documents/1/d/290566.pdf>

OSCE - Outcome Document from the 4th OSCE-wide Seminar on Passenger Data Exchange Organised Jointly by the Organization for Security and Co-operation in Europe and the United Nations Office of Counter-Terrorism, 30 octobre 2020.

<https://www.osce.org/files/f/documents/a/b/472794.pdf>

Parlement Européen et Conseil - Directive (UE) 2016/680 du Parlement européen et du Conseil, « relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil », 27 avril 2016.

<https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=celex%3A32016L0680>

Parlement européen et Conseil - Directive 2016/681 « relative à l'utilisation des données des dossiers passagers (PNR) pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière », 27 avril 2016.

<https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016L0681&from=FR>

Parlement et Conseil de l'Union Européenne - Règlement (UE) 2017/458 du Parlement Européen et du Conseil, « modifiant le règlement (UE) 2016/399 en ce qui concerne le renforcement des vérifications dans les bases de données pertinentes aux frontières extérieures », 15 mars 2017.

<https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32017R0458&from=EN>

Parlement européen et Conseil - Directive 95/46/CE du Parlement européen et du Conseil, « relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données », 24 octobre 1995.

<https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:31995L0046&from=FR>

Parlement européen et Conseil - Règlement (UE) 2017/2226 « portant création d'un système d'entrée/de sortie (EES) pour enregistrer les données relatives aux entrées, aux sorties et aux refus d'entrée concernant les ressortissants de pays tiers qui franchissent les frontières extérieures des États membres et portant détermination des conditions d'accès à l'EES à des fins répressives, et modifiant la convention d'application de l'accord de Schengen et les règlements (CE) no 767/2008 et (UE) no 1077/2011 », 30 novembre 2017.

<https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32017R2226&from=EN>

Parlement européen et Conseil - Règlement (UE) 2018/1240 « portant création d'un système européen d'information et d'autorisation concernant les voyages (ETIAS) et modifiant les

règlements (UE) no 1077/2011, (UE) no 515/2014, (UE) 2016/399, (UE) 2016/1624 et (UE) 2017/2226 », 12 septembre 2018.

<https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32018R1240&from=EN>

WCO and ICAO - Appendix III: Instruments of the WCO and ICAO on API, Recommendation of the customs co-operation Council, « concerning adherence to standards in relation to data requirements for advance passenger information (API) », 6 Juillet 1993.

<http://www.wcoomd.org/~media/wco/public/global/pdf/topics/facilitation/instruments-and-tools/tools/api-guidelines-and-pnr-doc/api-guidelines-2013-appendix-iii-instruments-of-wco-icao-on-apie.pdf?db=web>

IV. Sites internet :

Site de l'Union Européenne : La Cour de Justice de l'Union Européenne (CJUE)

https://europa.eu/european-union/about-eu/institutions-bodies/court-justice_fr#que-fait-la-cour-de-justice

Site d'Europol : Secure Information Exchange Network Application (SIENA).

<https://www.europol.europa.eu/activities-services/services-support/information-exchange/secure-information-exchange-network-application-siena>

Site de l'OACI : ICAO Global Aviation Security Symposium 2021 (AVSEC2021).

<https://www.icao.int/Meetings/AVSEC2021/Pages/default.aspx>

Site de l'OACI : Sécurité et facilitation de l'aviation - Aviation Security and Facilitation News

<https://www.icao.int/Security/Pages/default.aspx?p=13>

Site des Nations Unies : Bureau de lutte contre le terrorisme - UNCCT : Programmes et projets.

<https://www.un.org/counterterrorism/fr/cct/programme-projects>

Site des Nations Unies : Conseil de Sécurité des Nations Unies - Résolutions.

<https://www.un.org/securitycouncil/fr/content/resolutions>

Site des Nations Unies : Office on Drugs and Crime - Our work.

https://www.unodc.org/unodc/en/terrorism/UNODC_Role.html

Site des Nations Unies : Programme de Lutte contre le terrorisme axé sur les déplacements.

<https://www.un.org/cttravel/fr>

Site des Nations Unies : Programme de Lutte contre le terrorisme axé sur les déplacements - Synthèse du programme.

<https://www.un.org/cttravel/fr/content/synthèse-du-programme%C2%A0>

Site du Centre National de Crise belge : BELPIU.

<https://centredecrise.be/fr/que-fait-le-centre-de-crise-national/lunite-dinformation-des-passagers-belge/belpiu>

ANNEXES

Annexe 1 : Newsletter Juin 2021 du Bureau des Nations Unies contre le terrorisme

Newsletter June 2021 UNITED NATIONS OFFICE OF COUNTER-TERRORISM UN Countering Terrorist Travel Programme

High Level Advocacy

ICAO Traveler Identification Programme Symposium 2021 (TRIP2021) and First Joint ICAO/INTERPOL Passenger Data Exchange Forum on 27 May: USG Voronkov spoke about the CT Travel Programme highlighting its impact and achievements in supporting Member States to detect and prevent terrorist travel amid the challenges posed by the ongoing COVID-19 pandemic challenges.

Peer-to-Peer Platform for EU and International Experts in Border Security and Management in the MENA region by FRONTEX: CTPP provided an overview of its ongoing engagement with Sudan, Morocco and Iraq, as well as its intention to expand the initiative to other countries in the region. Other participating organizations comprised Europol, INTERPOL, EMSA, EFCA, IOM, EU DG, WCO, FRONTEX and UNODC.

103rd session of the IMO Maritime Safety Committee: The Committee endorsed WCO's paper on the new Passenger Facilitation and Control Working Group, that indicates measures to enhance maritime security, through Advance Passenger Information (API) and Passenger Name Record (PNR) for cruise ships, and other maritime modes of transport.

Highlights

- Two years passed since the launch of the Programme in May 2019
- Nigeria, Moldova, South Africa, Norway, and Kenya are the newest Member States to join the Programme increasing the total number of beneficiary Member States to 42
- A total of 13 beneficiary Member States are currently in the implementation phase (CARICOM representing 15 countries is counted one), with 3 deployments of goTravel at pre-production stage ongoing in Botswana, Côte d'Ivoire, and Azerbaijan
- CTPP's donor base is growing with the recent inclusion of Hungary that has agreed to provide in-kind support
- UNOCT and UNODC-AIRCOP organized a [virtual side-event](#) on 20 May on the margins of the 30th session of the Commission on Crime Prevention and Criminal Justice, highlighting the Programme's operational pillar and national experiences in in The Gambia, Azerbaijan, and Togo
- A virtual side-event on "Building national capacities to counter terrorist travel: Highlighting achievements, impact and lessons learned from the field" will be convened at the end of June on the margins of the High-Level UN Counter Terrorism Week

About CT Travel

The overall objective of the UN Countering Terrorist Travel Programme (CTTP) is to build Member States' capabilities to prevent, detect, investigate and prosecute terrorist offences and other serious crimes, including related to travel, by i) collecting and analysing travel information such as passenger data, namely Advance Passenger Information (API) and Passenger Name Record (PNR); ii) improving the use of international databases with known and suspected terrorists and criminals, such as the databases of the International Criminal Police Organization (INTERPOL); and iii) enhancing international information exchange, in line with UN Security Council resolutions 2178, 2396, and 2482. The detection capabilities, commonly referred to as Passenger Information Units (PIUs), that the Programme helps establish are in charge of processing passenger data provided by the transport industry using the goTravel technology, based on solid legislation and regulations established with the Programme's assistance.

CT Travel Strategy

Pillar I Legislation support for API and PNR	Pillar II Operational support for Passenger Information Units (PIUs)
Pillar III Transport industry engagement	Pillar IV Technical support for goTravel

[Corporate Online Platform](https://www.un.org/cttravel)

<https://www.un.org/cttravel> #UNitetoCounterTerrorism | @UN_OCT | #UNCCT

► Capacity Building

UN Countering Terrorist Travel Programme (CTTP)

Outreach and Engagement Strategy for Priority Member States: CTTP finalized an outreach and engagement strategy that aims to increase the number of beneficiary Member States under the programme. The strategy focuses on targeted outreach and also provides a framework for the implementation of a series of regional online awareness-raising briefings over the course of the year. More information to follow.

Deep-Dive Assessments: In April and May respectively, deep-dive assessments were organized in Mongolia and South Africa with the support of programme partners, to help uncover gaps and identify areas for support following a thorough review and analysis of existing capacities across the four key pillars: Legal, operational, transport industry engagement, and technical.

Training and Learning: CTTP, in partnership with Telefónica Educación Digital, is developing four self-paced eLearning modules to be hosted on the UNOCT Learning Management System (LMS), covering API and PNR, threat environment and the international counter-terrorism framework, Passenger Information Units (PIU), Passenger Data Single Window (PDSW), PIUs and Open-Source Intelligence (OSINT).

CTTP recently completed country-specific training programmes in Sierra Leone and The Gambia and the first-ever regional training programme covering SADC countries was held for South Africa, Namibia, Eswatini, with expert support from Botswana. In line with the CTTP's objective to encourage women's participation in the Programme's training activities, 39 out of the 99 participants

were female representatives of national agencies.

Between January and May, CTTP facilitated 6 virtual exchange visits between PIUs: Botswana/ Finland, Cote d'Ivoire/France, Cote d'Ivoire/Belgium, Sierra Leone/Netherlands, Azerbaijan/UK and Finland PIU. The visits served as a forum to share expertise, best practices and lessons learned.

Informal Working Groups: In April, CTTP, together with OSCE, organized a virtual launch of the Eastern European regional Informal Working Group (IWG) on API and PNR. The regional IWGs will provide a platform for cooperation of PIUs, whilst fostering partnerships and the exchange of information, best practices, and expert-based recommendations. The virtual launch event was attended by 82 participants from 12 OSCE Member States.

► Upcoming Activities

- Training for CARICOM, including a CTED session on Covid's impact on terrorism
- MOU e-signing ceremonies with Côte d'Ivoire, Botswana, and the Philippines
- CTTP is participating in side event on the margins of the High Event Counter Terrorism Week in June



Training Approach

CTTP has designed a week-long online blended learning course that covers all aspects of the training syllabus, which are (1) the threat environment, (2) an introduction to the CT Travel Programme, (3) international legal and regulatory framework related to API and PNR data, (4) the operationalization of a Passenger Information Unit (PIU), (5) state and industry engagement, and (6) technological support and the goTravel software, (7) maritime. Participants will be able to engage through a mix of live sessions and prerecorded lectures at their own pace and even come back to the information once the course is finished. Every video also offers a PDF file for reference after the course. Recently, a new legal case study was added to the programme. Each training is preceded by a pre-training week, 3 hours of self-study, where we explain the terms API and PNR. Here is the link to the prospectus on the website.



Beneficiary Member States

Azerbaijan	Morocco
Botswana	Iraq
CARICOM (15 Member States)	DRC
Côte d'Ivoire	Nigeria
Djibouti	Kazakhstan
The Gambia	Benin
Ghana	Moldova
The Maldives	Namibia
Mongolia	Mauritius
The Philippines	Eswatini
Sierra Leone	Israel
Sudan	Norway
Togo	Kenya
South Africa	

CT Travel :
2019 - Present

42 Beneficiary Member States

12 Member States received deep dive assessments

12 Roadmaps developed

15 Countries testing goTravel through OSCE

<https://www.un.org/cttravel>

#UNITetoCounterTerrorism | @UN_OCI | #UNCCT

Annexe 2 : Explication du Programme de contre-terrorisme des Nations Unies

UNITED NATIONS
OFFICE OF COUNTER-TERRORISM
UN Countering Terrorist Travel Programme

The **Countering Terrorist Travel Programme**, a flagship global initiative of UNOCT, assists beneficiary Member States in building their capabilities to detect and counter terrorists and serious criminals by using Advance Passenger Information (API) and Passenger Name Record (PNR) to improve the use of international databases with known and suspected terrorists and criminals, such as with INTERPOL, and enhance international information exchange, in accordance with Security Council resolutions 2178 (2014), 2396 (2017), and 2482 (2019) and relevant privacy laws.

The Secretary-General officially launched the Programme on 7 May 2019. Since then, 38 Member States officially joined the Programme, with approximately 40 more Member States indicating strong interest to do so.

In an "All-of-UN" partnership with the United Nations Counter-Terrorism Executive Directorate (CTED), the United Nations Office on Drugs and Crime (UNODC), the International Civil Aviation Organization (ICAO), the United Nations Office of Information and Communication Technology (UNOICT), and the International Criminal Police Organization (INTERPOL), the Programme comprehensively assists beneficiary Member States in legislative, operational, transport industry engagement, and technical areas. This includes the donation and deployment of the United Nations

www.un.org/ctravel 1

UNITED NATIONS
OFFICE OF COUNTER-TERRORISM
UN Countering Terrorist Travel Programme

goTravel software system. The Programme has been designed in accordance with human rights principles and United Nations policies in this regard.

The Programme is co-funded by generous contributions from the Kingdom of the Netherlands, the European Union, the United States of America, the State of Qatar, Australia, Japan, and the Republic of India.

In tandem with awareness raising activities, CT Travel focuses on arranging and conducting prerequisite assessments of confirmed beneficiary Member States. After determining a state's existing level of implementation, the Programme produces a roadmap for the Member State that identifies steps for implementation across the areas of work:

First, legislative assistance to put in place a legal framework that regulates the collection, processing and protection of data.

Second, technical assistance to set-up a Passenger Information Unit, including training and drafting standard operating procedures.

Third, facilitating air carrier engagement and connectivity, thanks to close cooperation with the transport industry.

www.un.org/ctravel 2

UNITED NATIONS
OFFICE OF COUNTER-TERRORISM
UN Countering Terrorist Travel Programme

And fourth, providing technical support to deploy, free of charge, the goTravel software to collect and process passenger data.

Emphasis is shifting to implementation of the four areas of work of the Programme based on the needs of each beneficiary Member State as outlined in the post-assessment roadmaps.

A maritime component has been added to the Programme scope to address beneficiary Member States' need to secure coastlines, formulating recommendations and proposing a framework for each area of work of the Programme and improving future collection and analysis of passenger and crew data.

Additionally, to this national implementation, the Programme offers the formation of regional Informal Working Groups (IWG). IWGs allow states in a region to meet regularly to discuss and address common challenges and interests. This good practice brings a cross-border vision and knowledge of threats while promoting the exchange of information as well as close operational and technical collaboration between PIUs in a region.

The Programme has established the Collaborative Online Platform (COP), a password-restricted forum for Programme partners, beneficiary Member States as well as the various experts involved with the Programme. The COP currently features a wide array of resources and includes a Pool of Experts. The Pool of Experts includes international experts from ministerial/policy, legal and national detection capabilities backgrounds, including those from national competent authorities, who will - on a pro bono basis - help train, mentor and advise beneficiary Member States receiving assistance within the framework of the Programme. In addition, these experts advise, share experience and lessons learned, and help train the PIUs or competent authorities of the Programme's beneficiary Member States.

The Programme has finalized an entry level training course on establishing specific governance elements to ensure institutional commitment and support for PIUs, as well as the generic Terms of Reference for PIUs. This allows the delivery of personalized SOPs for each beneficiary Member State's PIU.

www.un.org/ctravel 3

TABLE DES MATIÈRES

<i>Remerciements</i>	3
<i>Sommaire</i>	4
<i>Table des abréviations et sigles utilisés</i>	5
<i>Introduction</i>	8
<i>PARTIE 1- L'ÉMERGENCE ET L'ÉLABORATION DES UIP À L'INTERNATIONAL SUR LE MODÈLE EUROPÉEN</i>	15
SECTION 1- L'évolution du modèle de collecte des données passagers rendue nécessaire par le contexte international	15
I. Les premiers textes normatifs européens vers la création des UIP	15
A. L'identification d'une nouvelle nécessité par les organes de l'Union européenne	16
B. Le caractère obligatoire de la collecte de données passagers par la directive 2004/82/CE	18
C. L'évocation du terme UIP et l'explication de son principe par la directive 2016/681	20
II. La coopération au service de l'exportation du modèle européen à l'international	23
A. Le corpus normatif des institutions internationales et la participation de l'Union européenne	23
B. Le soutien des entités internationales dans l'implémentation du modèle des UIP par les États	27

C.	L'importance du partage des bonnes pratiques pour une implémentation facilitée.....	29
----	---	----

SECTION 2- Les défis structurels et légaux de l'implémentation du modèle des UIP au sein des États..... 32

I.	Le manque de clarté des procédures de récupération des données passagers.....	32
A.	Les disparités de qualité et quantité des données récoltées et transférées par les transporteurs aériens	33
B.	La détermination complexe des structures habilitées à recevoir les données passagers	35
C.	La multiplicité des formats de messages et protocoles de transfert des données passagers.....	37
II.	Le manque de sécurité dans l'exploitation des données et leurs transferts	39
A.	La fluctuation des champs et critères requis de collecte et d'utilisation des données passagers.....	39
B.	Les risques d'atteintes aux droits des passagers par la volonté de garantir la Sécurité et la Sûreté	42
C.	Le manque de coopération spontanée entre UIP comme conséquence des lacunes du modèle	45

PARTIE 2- L'ADAPTATION DU MODÈLE DES UIP À LA RECHERCHE D'UN SYSTÈME HARMONISÉ ET PERFORMANT.....47

SECTION 1- L'encadrement de la pratique des États et la prise en compte de leurs spécificités nationales 48

I. Le respect de la souveraineté des États en parallèle de la mise en place d'un modèle commun.....	48
A. Les observations formulées par les États quant aux résolutions des Nations-Unies	48
B. La nécessité de composer avec les particularismes nationaux.....	50
C. La marge de manœuvre laissée aux États dans la transposition des textes internationaux	52
II. L'importance de garanties et mesures pour le respect des bonnes pratiques des États	53
A. Les schémas de contrôle et de remontée de l'information à l'échelle de l'UIP pour la protection des données passagers.....	54
B. Les pouvoirs de sanction des entités à l'échelle internationale pour l'exploitation appropriée des données passagers	56
C. Les différends entre les États et leurs transporteurs aériens quant aux exigences de leur mise en conformité	57

SECTION 2- L'harmonisation des pratiques au support d'un système d'UIP

fiable et exportable..... 60

I. La composition de l'UIP comme variable importante dans la recherche d'une efficacité accrue	60
A. L'UIP comme Fenêtre Unique face aux nombreuses demandes formulées devant elle	61
B. La légitimité des UIP dans leur mission de contrôle des demandes adressées à elles.....	62

C.	L'adaptation structurelle du modèle de l'UIP au service d'une plus grande efficience.....	63
II.	Les différentes opportunités d'application pratique d'un modèle fonctionnel d'UIP	65
A.	La multiplication des accords bilatéraux et multilatéraux entre États.....	66
B.	L'extension de la récolte des données passagers à d'autres acteurs du transport.....	67
C.	La plus grande variété des finalités de l'utilisation des données par les UIP	69
	<i>Conclusion</i>	72
	<i>Bibliographie</i>	74
	<i>Annexes</i>	83
	<i>Table des matières</i>	86

RÉSUMÉ – A l’aube du 20^e anniversaire de l’attentat-suicide d’ampleur par détournement d’avions contre les tours jumelles du World Trade Center de New-York, le terrorisme reste à l’international une menace très présente qui sait exploiter les faiblesses des modes de transports actuels afin de conserver sa caractéristique première qui est son imprévisibilité.

Les Unités d’Information Passagers sont nées de la volonté des États de mettre en œuvre des solutions et initiatives afin de prévenir et réprimer ce phénomène. Aux fins de permettre une action harmonieuse, efficace et adaptée au niveau international, il est important d’en interroger les contours et les régimes juridiques qui s’y appliquent.

La présente réflexion vise à l’analyse de ce modèle récent qui tend à s’élever comme un standard international en matière de préservation de la sûreté via la surveillance du mode de transport aérien.

SUMMARY – At the dawn of the 20th anniversary of the major suicide-attack on the World Trade Center’s Twin Towers by aircraft hijacking, terrorism is still a very present international threat that exploit the weaknesses of the current modes of transportation in order to maintain its primary characteristic, which is its unpredictability.

Passenger Information Units were born out of the will of States to implement solutions and initiatives to prevent and suppress this phenomenon. In order to enable harmonious, effective and appropriate action at international level, it is important to examine the outlines and legal regimes that apply to them.

The present reflection aims at analyzing this recent model which tends to become an international standard in the preservation of security through the surveillance of air transport.

MOTS CLÉS – TERRORISME; CRIMES SÉRIEUX; UNITÉS D’INFORMATION PASSAGERS; DROIT INTERNATIONAL ET EUROPÉEN; DROIT DE L’AVIATION; SÛRETÉ AÉRIENNE; COOPÉRATION ÉTATIQUE; SOUVERAINETÉ; API ; PNR.

KEYWORDS – *TERRORISM; SERIOUS CRIME; PASSENGER INFORMATION UNITS; INTERNATIONAL AND EUROPEAN LAW; AVIATION LAW; AVIATION SECURITY; STATE COOPERATION; SOVEREIGNTY; API; PNR.*