«%ParlID»

Loi fédérale sur le traitement des données relatives aux passagers aériens pour la lutte contre les infractions terroristes et les autres infractions pénales graves (Loi sur les données relatives aux passagers aériens, LDPa)

Rapport explicatif relatif à l'ouverture de la procédure de consultation

(Mars 2022)

Aperçu

Le présent projet de loi vise à autoriser la Suisse à traiter systématiquement les données relatives aux passagers aériens pour que les autorités fédérales et cantonales puissent plus facilement prévenir les infractions terroristes et les autres infractions pénales graves et mener des enquêtes et des poursuites en la matière.

Contexte

Les entreprises de transport aérien collectent au moment de la réservation d'un billet d'avion diverses données sur les passagers dont elles ont besoin pour réserver et enregistrer le vol. Cet ensemble de données relatives aux passagers aériens, connu au niveau international sous le nom de dossier passager ou Passenger Name Record *(PNR), comprend par exemple le nom et l'adresse des passagers, mais aussi d'autres informations relatives à leurs bagages ou aux modes de paiement.*

Plus de 60 États ont reconnu le potentiel du PNR et l'exploitent depuis des années pour lutter contre le terrorisme et les autres formes de grande criminalité. Le traitement des données relatives aux passagers aériens et les analyses spécifiques de données permettent non seulement de mener des enquêtes sur des personnes déjà connues des autorités de poursuite pénale, mais aussi, grâce à de nouvelles pratiques d'enquêtes, d'en identifier d'autres jusqu'alors inconnues et pouvant présenter un lien avec le terrorisme ou les autres formes de grande criminalité.

Actuellement, l'utilisation du PNR progresse partout dans le monde. Trois résolutions du Conseil de sécurité de l'ONU, contraignantes pour la Suisse, enjoignent à la communauté internationale d'utiliser les données relatives aux passagers aériens pour prévenir le terrorisme. La Suisse, en sa qualité de membre de l'Organisation de l'aviation civile internationale (OACI), est tenue d'appliquer les normes de cette dernière en matière de données PNR.

Par sa directive (UE) 2016/681, l'Union européenne (UE) a contraint ses États membres à mettre en place un système PNR national. Cette directive ne constitue pas un développement de l'acquis de Schengen. Toutefois, la Suisse est concernée par sa mise en œuvre, car toutes les entreprises de transport aérien opérant des vols de la Suisse à destination de l'UE et inversement sont tenues de transmettre des données.

Si aujourd'hui les données PNR des vols de la Suisse à destination des États membres de l'UE, du Royaume-Uni, des États-Unis et du Canada sont transmises aux autorités compétentes, la Suisse ne peut pas systématiquement les traiter elle-même tant qu'elle ne dispose pas d'une base légale et d'un système PNR national.

Sans ce système PNR, la Suisse a moins de données à sa disposition par rapport à d'autres États Schengen pour effectuer des contrôles à l'entrée de son territoire. Elle prend donc le risque que des personnes représentant un danger pour la sécurité publique profitent de cette lacune pour pénétrer incognito dans l'espace Schengen.

Enfin, l'utilisation du PNR est également l'une des conditions des États-Unis en vue du maintien de la Suisse dans le programme d'exemption de visa (Visa Waiver Program, VWP). Celui-ci permet aux ressortissants suisses de voyager aux États-Unis sans visa à des fins professionnelles ou touristiques pendant 90 jours au plus.

Contenu du projet

La loi sur les données relatives aux passagers aériens (LDPa) vise à permettre à la Confédération de traiter les données collectées pour la réservation et l'enregistrement de vols dans le but de lutter contre les infractions terroristes et les autres infractions pénales graves.

Un nouveau service, rattaché à l'Office fédéral de la police (fedpol) et désigné au niveau international sous le nom de Passenger Information Unit *(PIU, en français "unité d'information passagers" ou UIP), est compétent pour le traitement des données. Il reçoit les données de la part des entreprises de transport aérien une première fois de 24 à 48 heures avant le départ d'un vol depuis la Suisse ou à destination de la Suisse et une deuxième fois juste avant celui-ci.*

En comparant les données relatives aux passagers aériens avant un vol avec celles issues des systèmes d'information de police, l'UIP identifie, à leur entrée en Suisse ou à leur sortie du pays, les personnes soupçonnées ou accusées de planifier ou d'avoir commis des infractions terroristes ou autres infractions pénales graves. L'UIP communique uniquement ces résultats ("concordances") aux autorités compétentes de la Confédération et des cantons, de sorte que ces dernières puissent prendre à temps les mesures nécessaires. Sur mandat de ces autorités, l'UIP doit également pouvoir effectuer des analyses ciblées des données relatives aux passagers aériens. Cette manière de procéder permet ainsi de reconnaître des personnes ou des liens indiquant des réseaux criminels actifs au niveau international.

Les données relatives aux passagers aériens sont automatiquement pseudonymisées six mois après leur enregistrement à l'UIP et effacées après cinq ans.

La moitié des collaborateurs actifs au sein de l'UIP sont détachés par les cantons, qui supportent les coûts relatifs à cet engagement. Cette configuration tient compte du fait que l'activité de l'UIP bénéficie dans une large mesure aux autorités cantonales de poursuite pénale.

Table des matières

1 Contexte

Toute personne réservant un vol communique à la compagnie aérienne ou à l'agence de voyage un nombre important d'informations, qui sont enregistrées dans les différents systèmes de réservation jusqu'après la fin du voyage. Ces informations, regroupées dans un ensemble de données relatives aux passagers aériens[1] (PNR), donnent des renseignements non seulement sur le nom et les coordonnées du passager aérien (adresse de domicile, téléphone, adresse électronique), mais aussi sur les modes de paiement, le nombre de bagages ou les autres voyageurs.

Plus de 60 États ont déjà reconnu le potentiel des données PNR pour la sécurité et exploitent ces données comme instrument efficace pour lutter contre le terrorisme et les autres formes de grande criminalité. Ils peuvent ainsi localiser suffisamment tôt les criminels lors de leurs déplacements et les identifier à leur entrée et à leur sortie ou tirer des conclusions sur des réseaux actifs au niveau international, par exemple dans le terrorisme ou la traite des êtres humains.

Aujourd'hui déjà, les entreprises de transport aérien fournissent les données PNR concernant les vols de la Suisse à destination de certains États, dont les États-Unis. La transmission de données aux États-Unis se fait depuis 2003 sur la base de l'accord du 23 décembre 2008[2]. Cet accord en remplace un autre de 2003 en la matière, mais de durée limitée. En juin 2018, les États-Unis ont déclaré que la Suisse ne serait maintenue dans le VWP qu'à condition d'utiliser elle aussi les données PNR. Ce programme permet aux ressortissants suisses de se rendre aux États-Unis sans visa à des fins professionnelles ou touristiques pendant 90 jours au plus.

Trois résolutions[3] du Conseil de sécurité de l'ONU enjoignent à tous les États membres de renforcer leurs capacités de collecte, de traitement et d'analyse de données PNR. Elles sont également contraignantes pour la Suisse.

Au niveau européen, l'Organisation pour la sécurité et la coopération en Europe (OSCE) exhorte ses membres, dont la Suisse, à utiliser les données PNR. Elle considère que l'utilisation de ces données est une mesure essentielle pour prévenir, détecter et poursuivre les infractions terroristes et soutient les États dans la mise en place d'un système PNR national.

Dans un premier temps, l'UE a fixé le traitement des données *Advance Passenger Information* (données API), qui représentent une partie des données PNR, dans sa directive (UE) 2004/82/CE (directive API)[4]. Le directive API fait partie de l'acquis de Schengen et est donc contraignante pour la Suisse.

1 Voir les explications dans le glossaire en annexe.
2 RS **0.748.710.933.6**
3 Résolution 2178 (2014) adoptée par le Conseil de sécurité à sa 7272e séance, le 24 septembre 2014, Résolution 2396 (2017) adoptée par le Conseil de sécurité à sa 8148e séance, le 21 décembre 2017, Résolution 2482 (2019) adoptée par le Conseil de sécurité à sa 8582e séance, le 19 juillet 2019
4 Directive 2004/82/CE du Conseil du 29 avril 2004 concernant l'obligation pour les transporteurs de communiquer les données relatives aux passagers, JO L 261 du 6.8.2004, p. 24

En revanche, la directive (UE) 2016/681 du 27 avril 2016 (directive PNR)[5], par laquelle l'UE oblige ses États membres à mettre en place un système PNR national, n'est pas contraignante pour la Suisse, car elle ne constitue pas un développement de l'acquis de Schengen. Toutefois, la Suisse est concernée par sa mise en œuvre étant donné que les entreprises de transport aérien ont aussi l'obligation de transmettre les données PNR pour les vols de la Suisse à destination de l'UE.

Depuis le 1er octobre 2015, la Suisse dispose de la base légale nécessaire pour traiter automatiquement les données API grâce aux art. 104*a* et 104*b* de la loi fédérale du 16 décembre 2005 sur les étrangers et l'intégration (LEI)[6]. Toutefois, comme au sein de l'UE, ces données ne sont pour l'heure pas recueillies systématiquement. Elles le sont uniquement pour des vols spécifiques en provenance d'États tiers à destination de la Suisse considérés comme risqués. Le traitement de ces données sert non seulement à améliorer le contrôle à la frontière et à lutter contre l'entrée illégale dans l'espace Schengen et le passage illégal par la zone internationale de transit des aéroports, mais aussi à lutter contre la criminalité internationale organisée et le terrorisme (art. 104*a*, al. 1, let. c, LEI).

Données API	
Données personnelles	Nom, prénom, sexe, date de naissance, nationalité
Document de voyage	Numéro, État émetteur, type et date d'expiration
Visa ou titre de séjour, si disponible	Numéro, État émetteur, type et date d'expiration
Itinéraire de vol réservé, si connu	Aéroport de départ, aéroports de transit / aéroport de destination en Suisse
Code de transport	
Nombre de personnes transportées sur le vol concerné	
Date et heure du départ et de l'arrivée prévus du vol	

Depuis le 1er janvier 2018, les autorités de poursuite pénale suisses peuvent exiger des données relatives aux passagers aériens en vertu de l'art. 21*f* de la loi fédérale du 21 décembre 1948 sur l'aviation (LA)[7], pour autant que les entreprises de transport aérien aient déjà collecté ces données "dans le cadre de leurs activités normales". Ainsi, en plus des données API, les autorités de poursuite pénale entrent en possession des données relatives aux passagers aériens suivantes:

- autres voyageurs éventuels;

5 Directive (UE) 2016/681 du Parlement européen et du Conseil du 27 avril 2016 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, JO L 119 du 4.5.2016, p. 132

6 RS **142.20**

7 RS **748.0**

- informations concernant le paiement, notamment le mode et le moyen de paiement utilisés;
- coordonnées de l'intermédiaire auprès duquel le transport a été réservé.

1.1 Nécessité d'agir et objectifs

La Suisse ne dispose actuellement ni d'une base légale ni d'un système d'information pour le traitement de données PNR. On entend par traitement toute opération relative à des données personnelles[8], quels que soient les moyens et procédés utilisés, notamment la collecte, l'enregistrement, la conservation, l'utilisation, la modification, la communication, c'est-à-dire le fait de transmettre des données personnelles ou de les rendre accessibles, l'archivage, l'effacement ou la destruction de données (art. 5 de la loi fédérale du 25 septembre 2020 sur la protection des données [LPD][9]).

Différents États, dont plusieurs partenaires économiques importants de la Suisse, demandent depuis longtemps des données PNR aux entreprises de transport aérien qui atterrissent sur leur territoire.

Ces données sont utilisées dans le but de lutter contre le terrorisme et d'autres infractions pénales graves. Le traitement systématique des données relatives aux passagers aériens permet de localiser des personnes recherchées au niveau national ou international lorsqu'elles entrent dans un pays ou en sortent. De plus, les autorités de poursuite pénale peuvent recevoir des informations sur des personnes jusqu'alors inconnues des services de police et liées au terrorisme ou à d'autres formes de grande criminalité. Le PNR peut ainsi considérablement contribuer à la détection et à la poursuite de réseaux criminels actifs au niveau international. Les entreprises de transport aérien effectuant des vols au départ de la Suisse sont aussi concernées par l'obligation de fournir des données PNR.

La Suisse a conclu avec les États-Unis en 2003 pour la première fois un accord prévoyant la communication de données. La transmission de données pour les vols de la Suisse à destination du Canada se fonde sur un protocole d'entente conclu en 2006[10].

L'échange de données entre l'UE et la Suisse doit être fixé d'un commun accord sur la base d'un traité international. D'ici à la conclusion de ce dernier, la transmission de données aux États membres de l'UE se fonde sur une solution transitoire élaborée avec le concours du Préposé fédéral à la protection des données et à la transparence (PFPDT). En mai 2018, l'Office fédéral de l'aviation civile (OFAC) a avisé les entreprises de transport aérien concernées qu'elles pouvaient transmettre les données relatives aux passagers aériens aux États membres de l'UE requérants dans l'attente de la création d'une base légale si elles en informaient les passagers dans leurs dispositions relatives au transport et que les passagers acceptaient cette transmission de données. Depuis, le PFPDT a signalé à plusieurs reprises que les bases légales nécessaires devaient être rapidement créées.

8 Voir les explications dans le glossaire en annexe.
9 FF **2020** 7397; à partir de l'entrée en vigueur de la nouvelle loi sur la protection des données: RS **235.1**
10 Disponible à l'adresse https://www.newsd.admin.ch/newsd/message/attachments/2244.pdf

Sans base légale, la Suisse ne peut pas traiter elle-même des données PNR. Cette situation pourrait avoir pour conséquence que des personnes soupçonnées d'avoir commis ou de planifier une infraction terroriste ou une autre infraction pénale grave poursuivent leur voyage par voie terrestre au sein de l'espace Schengen après avoir atterri en Suisse, contournant ainsi les systèmes PNR utilisés dans les différents États.

Afin de pouvoir traiter les données PNR à l'avenir et lutter contre le terrorisme et les autres infractions pénales graves, la Suisse a besoin tant d'une base légale formelle, créée au moyen du présent projet de loi, que d'un système d'information PNR.

Le 12 février 2020, le Conseil fédéral a chargé le Département fédéral de justice et police (DFJP) d'élaborer, en collaboration avec le Département fédéral de l'environnement, des transports, de l'énergie et de la communication, et de soumettre au Conseil fédéral un projet mis en consultation relatif à une loi fédérale sur la collecte et l'utilisation de données PNR et la transmission de ces dernières à des États qui garantissent une protection et un traitement des données répondant aux normes de la directive PNR. De plus, un mandat visant à entamer des négociations avec l'UE sur un accord relatif aux données PNR doit être mis en place en collaboration avec le Département fédéral des affaires étrangères.

1.2 Options examinées et solution retenue

Réflexions du point de vue de la technique législative

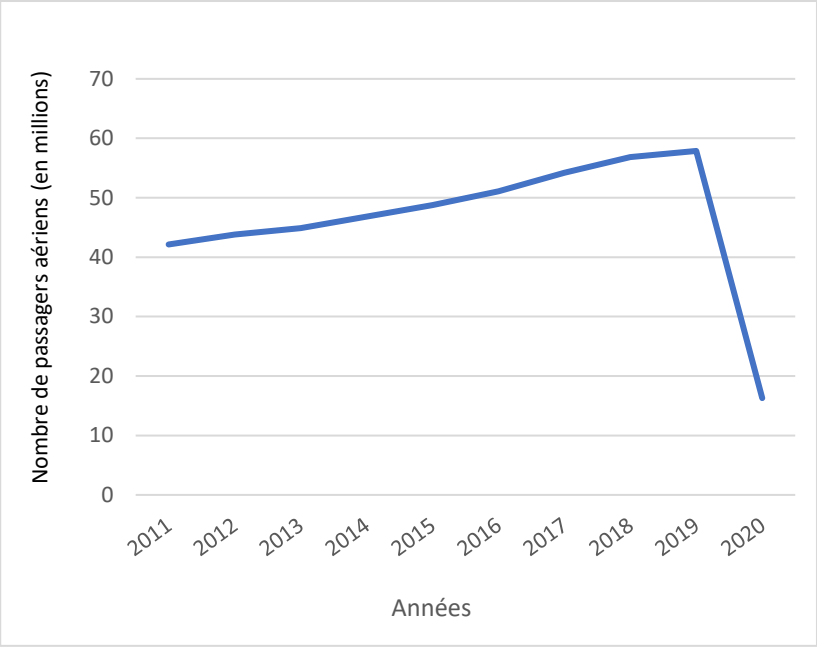
L'option de ne pas créer une nouvelle loi, mais d'intégrer les bases légales nécessaires dans des lois fédérales existantes, en l'occurrence dans la LA, la LEI ou la loi fédérale du 25 septembre 2015 sur le renseignement (LRens)[11], a été examinée. Il en aurait résulté un cadre juridique fractionné et confus qui n'aurait été ni dans l'intérêt des entreprises de transport aérien tenues d'observer cette loi, ni dans celui des passagers aériens concernés, raison pour laquelle cette option a été abandonnée.

Une nouvelle loi régissant complètement le traitement des données relatives aux passagers aériens offre un maximum de transparence et de cohérence. Ce choix se justifie également compte tenu des modalités à régler. En effet, outre la transmission des données relatives aux passagers aériens de la part des entreprises de transport aérien et les sanctions auxquelles s'exposent ces dernières en cas de violation de cette obligation, il convient également de régler l'organisation et les tâches de l'UIP, qui doit désormais être mise en place. La tâche de l'UIP consiste à traiter les données relatives aux passagers aériens et à les communiquer aux autorités compétentes en Suisse et à l'étranger. Pour ce faire, elle a accès à différents systèmes d'information de la Confédération.

Le projet implique certaines obligations nouvelles pour les entreprises de transport aérien opérant en Suisse. En 2019, 217 entreprises de transport aérien (2020: 198) proposant des vols de ligne et charters auraient été concernées. Durant l'année précédant la pandémie, elles ont transporté près de 60 millions de passagers de la Suisse à destination de l'étranger et inversement.

11 RS **121**

Graphique 1: nombre de passagers aériens qui ont quitté le territoire suisse et qui sont entrés en Suisse sur des vols de ligne et charters (source: OFAC).



Une loi sur les données relatives aux passagers aériens incluant toutes les dispositions importantes concernant le PNR permet de rendre le cadre juridique clairement reconnaissable pour les entreprises de transport aérien concernées.

Du point de vue de la protection des données aussi, il convient de saluer le fait d'avoir une loi fédérale cohérente sous la main. Pour les passagers aériens, il doit être facile d'identifier dans quels buts et à quelles conditions leurs données peuvent être traitées par l'État, et quels sont leurs droits en tant que passagers.

Utilisation des données PNR en matière de santé publique

fedpol a aussi examiné l'option d'utiliser les données relatives aux passagers aériens à des fins de protection de la santé publique. En accord avec l'Office fédéral de la santé publique, il a été décidé d'abandonner cette option. Les données relatives aux déplacements et aux séjours à des fins médicales doivent être collectées directement auprès du passager aérien concerné, le cas échéant.

Révision de la directive API

Les données API représentent une partie des données PNR et sont elles aussi traitées partout dans le monde.

En Suisse, l'obligation des entreprises de transport aérien de communiquer les données API est réglée par l'art. 104 LEI. Elle se limite actuellement aux vols à destination de la Suisse jugés risqués.

L'UE est en train de modifier la directive API. La révision devrait aboutir dans le courant de l'année 2022.

Pour la Suisse, cette révision nécessiterait le remplacement du système API actuel (art. 104*a* LEI) et probablement une modification d'autres dispositions concernées de la LEI.

Compte tenu des similitudes que présentent les données API et PNR, il a été examiné si et dans quelle mesure la révision de la directive API doit être prise en compte dans le présent projet législatif.

La différence de finalité pour laquelle le traitement de données est autorisé plaide contre une prise en compte de la révision de la directive API. En effet, le traitement des données PNR vise uniquement à prévenir et à détecter les infractions terroristes et les autres infractions pénales graves. En revanche, les données API peuvent être utilisées tant pour l'amélioration des contrôles aux frontières et la lutte contre l'immigration illégale qu'aux fins de poursuite pénale à certaines conditions. Leur traitement est donc autorisé dans un but bien plus large que celui des données PNR.

En effet, la différence de finalité implique une différence de droits d'accès et de délais de traitement autorisé.

Le contenu de la révision de la directive API n'est pas encore défini de manière exhaustive. De plus, la date de son entrée en vigueur n'est pas encore connue. Pour cette raison, l'avant-projet de la LDPa ne prend pas en compte la révision de la directive API. Les dispositions fondamentales contenues dans la LEI relatives à l'obligation de collecter et de communiquer les données API devront donc être modifiées en temps voulu.

1.3 Rapport avec le programme de la législature et la planification financière ainsi qu'avec les stratégies du Conseil fédéral

Le message relatif au système d'information national sur les données PNR et le crédit d'engagement y afférent figurent au programme de la législature 2019 à 2023 sous forme d'autre objet concernant le mise en œuvre de l'objectif 14 "La Suisse prévient la violence, la criminalité et le terrorisme et lutte efficacement contre ces phénomènes"[12].

Le système PNR contribue d'ailleurs à la mise en œuvre des objectifs 12 "La Suisse dispose d'un cadre réglant ses relations avec l'UE" et 15 "La Suisse connaît les menaces qui pèsent sur sa sécurité et dispose des instruments nécessaires pour y parer efficacement".

La LDPa fournit la base légale nécessaire à la mise en place de l'UIP au sein de fedpol. Cette unité traite les données relatives aux passagers aériens pour lutter contre le terrorisme et les autres formes de grande criminalité. Pour ce faire, elle exploite un système d'information PNR.

12 Message du 29 janvier 2020, FF **2020** 1709

Les moyens financiers destinés à la mise en place du système d'information PNR sont inscrits à la planification financière de la Confédération[13].

Dans sa Stratégie de la Suisse du 18 septembre 2015 pour la lutte antiterroriste[14], le Conseil fédéral mentionnait déjà l'utilisation d'un système PNR comme mesure potentielle pour empêcher l'entrée, la sortie et le transit indésirables de personnes soupçonnées de terrorisme.

2 Comparaison avec le droit étranger, notamment européen

UE

Plusieurs États membres de l'UE ont traité des données PNR en vertu de leur droit interne avant 2016 déjà. Le 27 avril 2016, le Parlement européen et le Conseil ont adopté la directive (UE) 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 (directive PNR). Entrée en vigueur le 24 mai 2016, elle a pour but d'harmoniser les règles de droit des États membres de l'UE, d'éliminer l'insécurité du droit, de combler les lacunes en matière de sécurité et de garantir le même niveau de protection des données pour tous les États. Le Danemark est le seul État membre à ne pas être lié par cette directive[15]. Toutefois, il a également développé depuis un système PNR sur la base de règles nationales de droit et s'est rattaché à l'échange d'informations PNR des États membres de l'UE.

En plus de la responsabilité des UIP, en charge de l'exploitation opérationnelle dans les États membres (art. 4), la directive règle le traitement des données (notamment à l'art. 6) et les obligations imposées aux transporteurs aériens concernant les transferts de données (art. 8). Les données sont dépersonnalisées[16] six mois après leur réception et effacées à l'expiration d'une période de cinq ans (art. 12). L'art. 13 est consacré à la protection des données à caractère personnel et contient des garanties importantes en matière de protection des droits fondamentaux.

La Commission européenne a réexaminé tous les éléments de la directive conformément à l'art. 19 et a présenté les résultats au Parlement européen et au Conseil dans son rapport du 24 juillet 2020[17]. Des modifications concrètes de la directive ne sont pas jugées nécessaires. Toutefois, deux procédures relatives à la protection des données et à la proportionnalité de la directive PNR, l'une engagée par l'Allemagne et l'autre par la Belgique, sont pendantes devant la Cour de justice de l'Union européenne (CJUE)[18]. Dans son rapport, la Commission européenne n'exclut pas que les arrêts respectifs rendu par la Cour puissent entraîner une modification de la directive PNR, même si elle estime que le système PNR est un instrument efficace dans la lutte contre

13 Budget 2022 avec plan intégré des tâches et des finances 2023-2025, tome 2A, p. 223
14 FF **2015** 6848
15 Directive PNR, considérant 40
16 Voir les explications dans le glossaire en annexe.
17 Rapport de la Commission au Parlement européen et au Conseil sur le réexamen de la directive (UE) 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, COM(2020) 305 final
18 Affaire C-817/19, Ligue des droits humains contre Conseil des ministres; affaires C-148/20, 149/20, 150/20, AC/DF/BD contre Deutsche Lufthansa AG.

le terrorisme et la grande criminalité. Sans l'utilisation des données PNR, il n'aurait pas été possible de procéder à des investigations approfondies ni à des arrestations. Les mesures strictes en matière de protection des données garantissent que seul un petit nombre de données à caractère personnel soit transmis aux autorités compétentes.

Les États membres de l'UE confirment que la durée de conservation des données prévue par la directive PNR est nécessaire d'un point de vue opérationnel. Ils ajoutent que les règles régissant l'accès des autorités aux données enregistrées à l'UIP et la dépersonnalisation de ces données se sont avérées suffisantes afin d'éviter des abus, mais que l'amélioration de la qualité des données reste un défi.

Dans sa communication du 21 septembre 2010 relative à la démarche globale en matière de transfert des données des dossiers passagers (PNR) aux pays tiers[19], la Commission européenne a fixé les critères devant être pris en compte lorsqu'elle décide de conclure de futurs accords avec des pays tiers. L'UE ne devrait collaborer qu'avec les pays tiers qui sont en mesure de protéger de manière adéquate les données PNR en provenance de l'UE. Les relations extérieures entre l'UE et ces pays tiers doivent également revêtir une certaine importance dans leur ensemble. La communication mentionne notamment le fonctionnement des services de police et des autorités judiciaires ainsi que la collaboration avec ceux-ci, l'État de droit et le respect général des droits fondamentaux. Le réexamen des pratiques en matière de transfert de données PNR vers des pays tiers est prévu comme mesure à moyen terme dans la stratégie de l'UE pour l'union de la sécurité pour la période 2020-2025[20].

Jusqu'à présent, l'UE a conclu des accords sur l'utilisation des données PNR avec les États-Unis[21] et l'Australie[22].

Un accord négocié avec le Canada, qui devait remplacer celui de 2006, a dû être renégocié après avoir été paraphé le 6 mai 2013. En effet, la CJUE a conclu, dans son avis du 26 juillet 2017[23], que l'accord visé était contraire à la Charte des droits fondamentaux de l'Union européenne[24].

En février 2020, la Commission européenne a été chargée d'entamer des négociations avec le Japon. La même année, elle a manifesté son intérêt à la Suisse de conclure un accord bilatéral relatif aux données PNR. Des discussions exploratoires ont commencé en 2021.

19 Communication de la Commission du 21 septembre 2010 relative à la démarche globale en matière de transfert des données des dossiers passagers (PNR) aux pays tiers, COM(2010) 492 final

20 Communication de la Commission du 24 juillet 2020 au Parlement européen, au Conseil européen, au Conseil, au Comité économique et social européen et au Comité des régions relative à la stratégie de l'UE pour l'union de la sécurité, COM(2020) 605 final, p. 28

21 Accord entre les États-Unis d'Amérique et l'Union européenne sur l'utilisation des données des dossiers passagers (données PNR) et leur transfert au ministère américain de la sécurité intérieure, JO L 215 du 11.8.2012, p. 5

22 Accord entre l'Union européenne et l'Australie sur le traitement et le transfert de données des dossiers passagers (données PNR) par les transporteurs aériens au service australien des douanes et de la protection des frontières, JO L 186 du 14.7.2012, p. 4

23 Avis 1/15 de la Cour (grande chambre) du 26 juillet 2017, ECLI:EU:C:2017:592

24 Charte des droits fondamentaux de l'Union européenne, JO C 202 du 7.6.2016, p. 389

Royaume-Uni

Le Royaume-Uni a été le premier État membre de l'UE à disposer d'un système PNR fonctionnel. Il traite des données PNR depuis 2004.

Durant les négociations sur le Brexit, le royaume et l'UE sont convenus de poursuivre l'échange de données PNR. Toutefois, le Royaume-Uni doit rendre ses analyses accessibles à l'Office européen de police (Europol), à l'unité de coopération judiciaire de l'Union européenne et aux autorités de poursuite pénale des États membres de l'UE lorsque ces derniers les demandent[25].

États-Unis

Suite aux attentats du 11 septembre 2001, les États-Unis ont élaboré l'*Aviation and Transportation Security Act*[26], contraignant ainsi les transporteurs aériens à leur octroyer l'accès aux données PNR de tous les vols à destination ou en provenance du territoire américain ou transitant par celui-ci. Depuis cet événement, le gouvernement américain s'efforce de collecter, transmettre et enregistrer les données PNR. Le premier accord avec la Suisse sur l'échange de données PNR est entrée en vigueur le 29 mars 2005, mais uniquement pour une durée de trois ans et demi en raison de sa validité limitée. La durée de validité de l'accord PNR du 23 décembre 2008[27] adopté par le Conseil fédéral est, contrairement à celle du premier, illimitée.

Les données PNR sont traitées conformément aux consignes légales en matière de protection des données contenues dans l'avis de système de dossiers (*System of Records Notice*, SORN) relatif au système automatisé de ciblage (*Automated Targeting System*, ATS). Celui-ci est établi par le Bureau des douanes et de la protection des frontières (CBP), rattaché au Département américain de la sécurité intérieure (DHS). Le SORN relatif à l'ATS exige du gouvernement américain qu'il garantisse pour les données PNR collectées sur les vols reliant les États-Unis et la Suisse la même protection que celle fournie par l'accord conclu en 2007 entre les États-Unis et l'UE sur le traitement de données PNR. Depuis le 11 août 2012, un accord révisé entre les États-Unis et l'UE [28] règle l'utilisation et le transfert des données PNR. Une évaluation de l'accord a été adoptée en janvier 2021[29].

En raison de bases légales manquantes dans son droit interne, la Suisse ne reçoit aucune donnée PNR sur les vols en provenance des États-Unis à destination de son territoire.

25 Accord de commerce et de coopération entre l'Union européenne et la Communauté européenne de l'énergie atomique, d'une part, et le Royaume-Uni de Grande-Bretagne et d'Irlande du Nord, d'autre part, JO L 149 du 30.4.2021, p. 10, art. 542 à 562

26 Public Law 107–71, 19. November 2001, 115 STAT. 597, Online: https://www.gpo.gov/fdsys/pkg/PLAW107publ71/pdf/ PLAW107publ71.pdf (28.08.2018)

27 RS **0.748.710.933.6**

28 Accord entre les États-Unis d'Amérique et l'Union européenne sur l'utilisation des données des dossiers passagers (données PNR) et leur transfert au ministère américain de la sécurité intérieure, JO L 215 du 11.8.2012, p. 5

29 Rapport de la Commission au Parlement européen et au Conseil sur l'évaluation conjointe de l'accord entre les États-Unis d'Amérique et l'Union européenne sur l'utilisation des données des dossiers passagers et leur transfert au ministère américain de la sécurité intérieure, COM(2021) 18 final

Canada

Depuis 2009, les données PNR et API sur les vols de la Suisse à destination du Canada sont transmises aux autorités canadiennes compétentes. La base légale est le protocole d'entente entre l'Agence des services frontaliers du Canada et l'Office fédéral de l'aviation civile de la Suisse concernant l'Information préalable sur les voyageurs et le Dossier passager[30] du 17 mars 2006. Les données PNR peuvent être uniquement utilisées pour l'identification de personnes s'il y a lieu de craindre que ces dernières

- importent des marchandises liées au terrorisme ou à des infractions terroristes;
- commettent d'autres infractions pénales graves de nature transnationale (dont le crime organisé);
- ont un lien possible avec de tels crimes.

Les autorités canadiennes conservent les données PNR pendant 42 mois, dans la mesure où la personne concernée ne fait pas l'objet d'une procédure, et les pseudonymisent après 24 mois.

L'Agence des services frontaliers du Canada est autorisée à communiquer les données PNR à une autre autorité canadienne uniquement dans des cas d'espèce et seulement après avoir évalué l'importance des informations PNR spécifiques qui doivent être divulguées. Les éléments PNR sont mis à disposition uniquement s'il est clairement prouvé qu'ils sont nécessaires au vu des circonstances. Dans tous les cas, un minimum d'informations est fourni. Les autorités canadiennes sont autorisées à communiquer des données PNR à un État tiers si un traité international le prévoit.

En raison de bases légales manquantes dans son droit interne, la Suisse ne reçoit aucune donnée PNR sur les vols du Canada à destination de son territoire.

3 Grandes lignes du projet

La LDPa telle qu'elle est proposée dans le projet doit permettre à la Suisse d'utiliser le PNR comme un instrument éprouvé pour lutter contre le terrorisme et les infractions pénales graves. En effet, les États-Unis, le Canada et le Royaume-Uni disposent d'un tel instrument depuis près de 20 ans et les États membres de l'UE l'utilisent depuis plusieurs années.

L'UE est le principal partenaire de sécurité de la Suisse, ce qui fait également d'elle le principal partenaire en ce qui concerne l'échange futur de données PNR. C'est pour cette raison que l'avant-projet de la LDPa se base sur la directive PNR de l'UE.

Grâce à cette loi, la Suisse remplit ses obligations internationales. Les trois résolutions du Conseil de sécurité de l'ONU[31], qui enjoignent aux États membres de renforcer leurs capacités de collecte, de traitement et d'analyse de données PNR, sont particulièrement contraignantes à cet égard. De plus, l'OACI a établi, sur mandat du Conseil de sécurité de l'ONU et en collaboration avec l'Organisation mondiale des douanes

30 Disponible à l'adresse https://www.newsd.admin.ch/newsd/message/attachments/2244.pdf

31 Résolution 2178 (2014), adoptée par le Conseil de sécurité à sa 7272e séance, le 24 septembre 2014, Résolution 2396 (2017), adoptée par le Conseil de sécurité à sa 8148e séance, le 21 décembre 2017, Résolution 2482 (2019) adoptée par le Conseil de sécurité à sa 8582e séance, le 19 juillet 2019

(OMD), les gouvernements des États membres, les transporteurs aériens et les prestataires, des normes sur la transmission des données relatives aux passagers aériens. Ces normes sont contraignantes pour tous les États membres de l'OACI, et donc aussi pour la Suisse. Enfin, pour les États-Unis, le traitement des données relatives aux passagers aériens est une condition au maintien de la Suisse dans le VWP (cf. ci-dessus, ch. 1).

3.1 Réglementation proposée

La LDPa est une condition légale pour que la Suisse puisse également traiter des données relatives aux passagers aériens et exploiter un système d'information à cet effet.

Les données relatives aux passagers aériens sont recueillies au moment de la réservation d'un billet d'avion, indépendamment de l'utilisation qu'en fait l'État pour lutter contre la grande criminalité. Elles ne doivent donc pas être collectées spécifiquement pour les buts visés par la présente loi.

Au total, les entreprises de transport aérien doivent transmettre 19 catégories différentes de données (annexe 1 LDPa).

Tous les passagers sur des vols charters et de ligne en provenance de Suisse et à destination de l'étranger et inversement sont concernés par ce traitement de données effectué par l'État.

Les entreprises de transport aérien doivent transmettre les données à l'UIP, rattachée à fedpol, à deux moments définis par la loi avant le départ à destination ou en provenance de la Suisse (art. 2). Cela permet ainsi aux autorités compétentes de la Confédération et des cantons de prendre à temps les mesures qui s'imposent contre les personnes soupçonnées à leur arrivée ou à leur départ.

Les entreprises de transport aérien doivent garantir la ponctualité de la transmission des données et respecter les prescriptions techniques (art. 4). De plus, elles doivent informer les passagers par écrit du traitement des données effectué par l'État (art. 5).

Si elles violent leur obligation de transmettre des données complètes et à temps, elles s'exposent aux sanctions prévues aux art. 23 à 25. Elles ne violent pas cette obligation si elles prouvent qu'elles ont pris toutes les mesures techniques et organisationnelles raisonnablement exigibles pour la remplir.

Les art. 6 à 12 régissent le traitement des données.

Les données relatives aux passagers aériens ne peuvent être traitées qu'à des fins de prévention, de détection, d'enquête et de poursuite pénale en matière d'infractions terroristes et autres infractions pénales graves. Les infractions visées sont mentionnées à l'annexe du présent rapport. L'UIP doit immédiatement effacer les résultats obtenus par le traitement qui ne remplissent pas ce but (art. 6).

Les art. 6 à 12 régissent le traitement des données, dont la compétence incombe à l'UIP, nouveau service qui sera rattaché à fedpol.

Dans un premier temps, les données transmises par les entreprises de transport aérien sont automatiquement comparées avec celles issues des différents systèmes d'information de police de la Confédération. Ces comparaisons permettent d'une part d'identifier, d'arrêter, voire d'extrader des personnes recherchées au niveau national ou international et, d'autre part, de compléter des informations en lien avec des infractions non élucidées ou planifiées. Dans un second temps, les données sont vérifiées manuellement et, le cas échéant, par un accès aux systèmes d'information de police et

aux autres systèmes de la Confédération (SYMIC, ORBIS, système d'information de l'OFDF) (art. 7).

Si la vérification produit un résultat positif, la concordance est transmise au service responsable du signalement ayant déclenché une concordance avec les données relatives aux passagers aériens. Il peut s'agir des autorités de poursuite pénale de la Confédération ou des cantons ou du Service de renseignement de la Confédération (SRC) (art. 8). Le service responsable du signalement décide alors des mesures devant être prises le cas échéant.

Les données relatives aux passagers aériens peuvent également être comparées avec des profils de risque et des listes d'observation, que l'UIP établit sur la base de ses propres analyses ou à la demande des autorités de poursuite pénale ou du SRC. Les profils de risque décrivent des combinaisons de données qui indiquent des activités criminelles en lien avec le terrorisme ou la grande criminalité. Les listes d'observation comportent des éléments de données PNR ou relatifs à des personnes (par ex. adresses électroniques, numéros de téléphone) dont il faut assurer le suivi dans le cadre d'infractions terroristes ou d'autres infractions pénales graves. Grâce à la comparaison avec les données PNR, ces deux instruments aident les autorités de poursuite pénale à détecter une personne encore inconnue des services de police, à identifier les membres d'une organisation criminelle ou à reconnaître des victimes potentielles de la traite d'êtres humains. Les listes d'observation devraient être utilisées uniquement pour les quelques éléments constitutifs de l'infraction que le Conseil fédéral détermine dans une ordonnance, l'accent étant mis sur les infractions terroristes et celles liées au crime organisé (art. 9).

La LDPa tient déjà compte de la LPD, qui devrait entrer en vigueur en 2023. Cette dernière prend en compte l'évolution technologique rapide et vise une large harmonisation avec la législation de l'UE en matière de protection des données.

Dans l'ensemble, les données relatives aux passagers aériens sont uniquement traitées lors de la comparaison avec les données issues des systèmes d'information de police, les profils de risque et les listes d'observation (cf. commentaire de l'art. 9). Ensuite, seule une petite partie de ces données fait l'objet d'un traitement complémentaire. Il s'agit de celles dont la comparaison donne lieu à une concordance et donc à un certain soupçon. L'étape de traitement suivante confirme si ce soupçon est justifié. En effet, les concordances peuvent être validées pour un traitement complémentaire uniquement après que leur plausibilité a été vérifiée. Si celle-ci est confirmée, il s'agit de données présentant un soupçon confirmé de lien avec le terrorisme ou la grande criminalité.

En revanche, la majeure partie des données relatives aux passagers aériens ne sont plus traitées après la comparaison. De plus, elles sont pseudonymisées six mois après avoir été transmises (art. 14): les données à caractère personnel, telles que le nom, le numéro de téléphone, l'adresse électronique ou le numéro de carte de crédit, sont en effet pseudonymisées de façon à ne plus pouvoir être attribuées à quiconque. Contrairement à l'anonymisation, la pseudonymisation peut être annulée a posteriori. Le Tribunal administratif fédéral (TAF) est compétent pour décider si les circonstances justifient une telle mesure (art. 15).

Les données sont effacées cinq ans après leur introduction dans le système d'information PNR (art. 16). D'un point de vue opérationnel, cette durée de conservation est

élémentaire, car les enquêtes sur les infractions contre lesquelles les données PNR servent à lutter s'étendent souvent sur plusieurs mois, voire plusieurs années[32].

La protection des données est aussi mise en œuvre sur le plan technique, comme le prévoit l'art. 7 LPD. Par exemple, l'accès au système d'information PNR se limite à quelques personnes (art. 13, al. 2). Il est en particulier exclu que les autorités de poursuite pénale de la Confédération et des cantons y aient un accès direct. Cette délimitation est renforcée par le fait que l'organisation de l'UIP est distincte des unités de fedpol qui mènent des enquêtes (art. 19). L'automatisme prévu pour la pseudonymisation et l'effacement des données relatives aux passagers aériens va également dans le sens de la protection technique des données.

L'UIP, qui traite des données conformément à la LDPa, est rattachée à fedpol (art. 19) et se compose à parts égales de collaborateurs provenant de la Confédération et des cantons (art. 20).

3.2 Concordance des tâches et des finances

Les dégâts que la (grande) criminalité inflige aux personnes concernées et à l'économie sont immenses. Élucider ces infractions et condamner leurs auteurs sont deux actions essentielles intimement liées à la justice dans un État de droit. Pour les victimes, elles sont synonyme d'un nouveau départ.

Il est encore plus important de prévenir de telles infractions. La sécurité est un bien crucial pour le bien-être d'une société et sa prospérité.

Le PNR y contribue considérablement.

Le PNR permet non seulement de poursuivre les grands criminels avec davantage d'efficacité et de décharger les autorités de poursuite pénale de manière ciblée, mais il contribue aussi grandement à détecter à temps la planification d'infractions pénales graves et à prévenir le passage à l'acte.

- Actuellement, les autorités de poursuite pénale doivent demander précisément les itinéraires de voyage des grands criminels auprès des différentes entreprises de transport aérien, ce qui est fastidieux. Des liens importants avec des criminels actifs au sein d'organisations passent souvent inaperçus. Le PNR permet aux autorités de poursuite pénale d'avoir recours à des ensembles de données compacts, les ensembles de données PNR, collectés systématiquement et enregistrés dans un système centralisé. En plus d'afficher les itinéraires de voyage, ceux-ci peuvent donner des indications sur propos les voyageurs, les voyageurs accompagnants, la fréquence des voyages et leurs destinations. Le PNR contribue considérablement à ce que les autorités de poursuite pénale obtiennent plus facilement et plus rapidement des informations importantes concernant des suspects, leurs habitudes de voyage et leurs personnes de liaison.

32 Rapport de la Commission au Parlement européen et au Conseil sur l'évaluation conjointe de l'accord entre les États-Unis d'Amérique et l'Union européenne sur l'utilisation des données des dossiers passagers et leur transfert au ministère américain de la sécurité intérieure, COM(2021) 18 final, p. 9

- La criminalité suit souvent certains schémas comportementaux, qui peuvent être plus facilement constatés grâce au PNR. Il est ainsi possible de détecter et de prévenir à temps les infractions planifiées.

Le PNR tire profit des données recueillies au moment de la réservation d'un vol. La charge de travail à fournir de la part des entreprises de transport aérien se limite à la transmission de ces données au service compétent de l'État. Le PNR n'exige aucun effort supplémentaire considérable de leur part, raison pour laquelle cet instrument peut être qualifié d'efficace. Il est toutefois aussi effectif, sinon comment expliquer qu'il soit utilisé depuis près de 20 ans pour lutter contre les infractions terroristes et les autres infractions pénales graves dans plus de 60 États, dont les États-Unis, le Canada, l'Australie, le Royaume-Uni et les membres de l'Union européenne.

Pour ce qui est de l'introduction du PNR en Suisse, il faut tabler sur des dépenses récurrentes qui se limitent principalement au traitement des données collectées auprès des entreprises de transport aérien. Les résultats du traitement des données sont notamment à la disposition des autorités de poursuite pénale de la Confédération et des cantons et simplifient les tâches de ces dernières.

Il est prévu que les cantons supportent les coûts relatifs à la moitié des collaborateurs qu'ils ont détachés au sein de l'UIP. Cette répartition des coûts montre que la sécurité du pays et la protection de la population sont une tâche commune de la Confédération et des cantons. Comme les données PNR sont un projet qui dépasse les frontières des cantons, mais aussi du pays, il est justifié que la Confédération prenne le solde à sa charge, notamment les coûts relatifs à la mise en place du système d'information requis.

3.3 Questions de mise en œuvre

En plus des données PNR que la Confédération recevra à l'avenir en cas d'adoption de la LDPa, les entreprises de transport aérien lui livrent aujourd'hui déjà, en l'occurrence au Secrétariat d'État aux migrations (SEM), les données API de certains vols jugés risqués en provenance d'États tiers à destination de la Suisse. Depuis 2015, ces données sont automatiquement traitées en vertu des art. 104*a* et 104*b* LEI.

Conformément aux normes techniques internationales de l'OACI, de l'OMD et de l'Association du transport aérien international (IATA), une interface unique (*single window*) doit être prévue pour la transmission de données PNR et API. Elle vise à épargner du travail inutile aux entreprises de transport aérien.

Cela signifie qu'il convient de définir une interface unique sur le plan technique pour les données API et PNR lors de la mise en place du système PNR suisse. Ainsi, les entreprises de transport aérien peuvent fournir les données à cette interface unique, qui les attribue ensuite automatiquement à l'UIP ou au SEM.

4 Commentaire des dispositions

1. Loi fédérale sur le traitement des données relatives aux passagers aériens pour la lutte contre les infractions terroristes et les autres infractions pénales graves

Section 1 Objet

Art. 1

Cette disposition présente l'essentiel de la loi, qui règle les obligations des entreprises de transport aérien, en plus du traitement et de l'analyse des données relatives aux passagers aériens. Néanmoins, ces obligations ne sont pas nouvelles. Les entreprises de transport aérien les remplissent déjà depuis de nombreuses années, par exemple vis-à-vis des États-Unis et du Canada, et depuis 2018 vis-à-vis des États membres de l'UE. La seule nouveauté est qu'elles doivent remplir ces obligations également vis-à-vis de la Suisse.

Les 19 catégories de *données relatives aux passagers aériens* devant être traitées se trouvent à l'annexe 1 LDPa et correspondent à celles de la directive PNR de l'UE. Les données relatives aux passagers aériens comprennent uniquement celles des passagers, et non celles de l'équipage. En font aussi partie les données personnelles conformément à l'art. 5, let. a, LPD. La LDPa constitue la base légale du traitement de ces données.

Le traitement n'est autorisé que s'il s'agit de lutter contre des infractions qui sont d'une gravité particulière et représentent un danger sérieux pour la sécurité publique. L'art. 6, al. 2 et 3, précise les éléments constitutifs de l'infraction prévus par le code pénal et le droit pénal accessoire.

L'art. 6, al. 3, LPD demande que la personne concernée soit informée de la finalité du traitement des données ou que ce traitement soit prévu par la loi[33], raison pour laquelle les entreprises de transport aérien doivent informer les passagers aériens que les données de ces deniers sont traitées en vertu de la présente loi dans le but de lutter efficacement contre le terrorisme et d'autres infractions pénales graves (cf. art. 5).

Les *entreprises de transport aérien* ne sont définies nulle part dans le droit en vigueur, raison pour laquelle elles sont décrites plus en détail à l'art. 1, let. b. Cette description se fonde sur celle qui a été élaborée dans le cadre de la loi du 25 septembre 2020 sur le CO_2 (art. 2, let. i)[34]. Elle est nécessaire à la LDPa, d'autant plus que les entreprises de transport aérien ont pour obligation de communiquer les données à temps (art. 4) et d'informer leurs passagers que les données de ces derniers seront traitées en vertu de la présente loi (art. 5). L'art. 23 prévoit des sanctions en cas de violation de ces obligations.

N'est pas considéré comme entreprise de transport aérien toute activité qui concerne l'aviation légère, c'est-à-dire les vols d'école, d'entraînement et de contrôle, les vols touristiques, les sports aériens ainsi que les vols privés.

33 Message du 15 septembre 2017 concernant la loi fédérale sur la révision totale de la loi fédérale sur la protection des données et sur la modification d'autres lois fédérales; FF **2017** 6644

34 https://www.bafu.admin.ch/dam/bafu/fr/dokumente/klima/rechtliche-grundlagen/definition-luftverkehrsunternehmen.pdf.download.pdf

Section 2 Obligations des entreprises de transport aérien

Art. 2 Transmission des données relatives aux passagers aériens à l'UIP

Les entreprises de transport aérien sont tenues de transmettre à l'UIP les données relatives aux passagers aériens visées à l'annexe 1 de l'avant-projet pour les vols au départ et à destination de la Suisse (al. 1). Les vols à destination de l'Euroairport de Bâle-Mulhouse-Fribourg soumis au droit suisse (munis du code d'aéroport IATA "BSL") sont également considérés comme des vols à destination de la Suisse au sens de la présente loi, indépendamment du fait que l'aéroport se trouve sur un terrain situé en dehors de la Suisse. Il en va de même pour les vols au départ de cet aéroport à destination de l'étranger.

Les données relatives aux passagers aériens sont transmises à l'UIP à deux moments différents: au plus tôt 48 heures mais au plus tard 24 heures avant le départ programmé du vol ainsi qu'immédiatement après la fin de l'embarquement (al. 2). La première transmission de données ne fournit certes que des informations provisoires, mais elle ménage à l'UIP un certain délai avant l'atterrissage de l'avion, ce qui pourrait avoir une importance certaine dans le cas des vols de courte distance. La seconde transmission permet de communiquer définitivement les données de tous les passagers présents à bord.

Les entreprises de transport aérien ne peuvent pas transmettre à l'UIP de données sensibles[35] au sens de l'art. 5 LPD. Toutefois, si de telles données venaient à être transmises par erreur, l'UIP doit immédiatement les effacer lorsqu'elle les identifie (al. 3).

Les données peuvent être fournies soit selon la méthode *pull*, soit selon la méthode *push*. Dans le premier cas, l'UIP accède au système de réservation des transporteurs aériens. Dans le second, les entreprises de transport aérien procèdent elles-mêmes à la transmission. La méthode *push* offre un niveau de protection des données plus élevé et va être utilisée dans la mise en œuvre du système PNR en Suisse. Elle est illustrée par le terme de *transmission* des données. Par ailleurs, le type de transmission est régi par les normes de l'OACI en la matière. Cette dernière a établi ces normes relatives à la transmission de données PNR sur mandat du Conseil de sécurité de l'ONU, en collaboration avec l'OMD, les gouvernements des États membres, les transporteurs aériens et les prestataires. Ces dispositions sont contraignantes pour tous les États membres de l'OACI, et donc aussi pour la Suisse. Par conséquent, une réglementation supplémentaire n'est pas nécessaire au niveau de la loi. Compte tenu des évolutions technologiques continues, il est toutefois indispensable de pouvoir préciser les modalités techniques en cas de besoin. L'al. 4 autorise fedpol à adopter les dispositions correspondantes au niveau de l'ordonnance.

Art. 3 Transmission de données relatives aux passagers aériens à des autorités étrangères

Aujourd'hui déjà, les entreprises de transport aérien fournissent des données relatives aux passagers aériens aux États à destination desquels des vols partent de Suisse, en l'occurrence aux États-Unis et au Canada. Pour ces deux pays, un accord avec la Suisse

35 Voir les explications dans le glossaire en annexe.

constitue la base légale de la transmission des données. Un accord est prochainement prévu avec l'UE.

Ces accords garantissent que le niveau de protection des données transmises à l'étranger soit comparable à celui de la Suisse. De plus, ils assurent à la Suisse une certaine réciprocité, dans la mesure où elle reçoit elle aussi des données relatives aux passagers aériens de chacun de ces États.

Art. 4 Devoir de diligence

Les entreprises de transport aérien doivent transmettre à l'UIP les données de *tous* les passagers à temps (cf. art. 2, al. 2) et conformément aux prescriptions techniques (cf. art. 2, al. 4). On attend d'elles qu'elles prennent toutes les mesures raisonnablement exigibles pour remplir cette obligation. Dans le cas contraire, elles s'exposent aux sanctions administratives prévues à l'art. 23.

Les données relatives aux passagers aériens sont pour la plupart saisies manuellement au moment de la réservation d'un billet d'avion, soit par le passager, soit par un collaborateur de l'aéroport ou de l'agence de voyage. Par conséquent, les données PNR comportent souvent des erreurs. Plus le nombre d'erreurs qui se glissent ou qui sont volontairement introduites est élevé lors de la collecte de données, moins ces données sont utilisables.

Il serait toutefois disproportionné d'obliger les entreprises de transport aérien à vérifier l'exactitude de toutes les données relatives aux passagers aériens. Comme la qualité des données est cependant essentielle à un traitement concluant en vertu de la présente loi, les entreprises de transport aérien devraient concevoir leur système de réservation de façon qu'il refuse les saisies manifestement erronées (par ex. prénom "Aaaaa" ou adresse électronique sans "@"). De telles mesures sont considérées comme raisonnablement exigibles (cf. art. 23, al. 2, let. b).

Art. 5 Obligation d'informer

Les entreprises de transport aérien doivent informer les passagers par écrit que les données de ces derniers seront traitées non seulement dans le cadre de leur vol, mais aussi en vertu de la présente loi. L'information peut figurer dans leurs conditions générales.

L'obligation d'informer visée à l'art. 5 se justifie bien qu'elle répète la disposition prévue à l'art. 20, al. 1, let. b, LPD, notamment car les données relatives aux passagers aériens sont traitées:

- dans deux contextes totalement différents, l'un factuel, l'autre juridique (réalisation technique de la réservation du vol / mise en œuvre de la LDPa);
- à des fins différentes (réservation du vol / lutte contre la criminalité);
- sous la responsabilité d'acteurs différents (entreprises de transport aérien / fedpol).

L'information ne comprend pas seulement le fait que les données sont transmises à l'UIP. Elle doit aussi permettre de reconnaître la finalité du traitement des données (cf. art. 6, al. 3 LPD). Les modalités supplémentaires dont il faudra informer les personnes concernées seront précisés dans l'ordonnance relative à la LPD.

Section 3 Traitement des données

Art. 6 Principes

Le traitement des données n'est autorisé que s'il faut lutter contre des infractions qui sont d'une gravité particulière et représentent un danger sérieux pour la sécurité publique. L'al. 3 précise les éléments constitutifs de l'infraction prévus par le code pénal et le droit pénal accessoire.

Les al. 2 et 3 mentionnent les *infractions terroristes et autres infractions pénales graves*, sans toutefois les définir précisément. Deux types d'infractions sont distingués: les infractions terroristes et les autres infractions pénales graves.

Sont qualifiées de *terroristes* au sens de la LDPa toutes les infractions visées au ch. 22 de l'annexe 1 LEIS, indépendamment de l'ampleur de la peine. Ces infractions terroristes sont mentionnées à l'annexe 1 du présent rapport.

La plupart de ces infractions sont des crimes et sont donc passibles d'une peine privative de liberté de plus de trois ans (art. 10, al. 2, CP). Les éléments constitutifs de l'infraction ci-après sont en revanche des délits, conformément à l'art. 10, al. 3, CP:

- menaces alarmant la population (art. 258 CP);
- provocation publique au crime ou à la violence (art. 259 CP);
- émeute (art. 260, al. 1, CP);
- groupements illicites (art. 275ter CP).

Ils ne tombent dans la catégorie des infractions terroristes que s'ils sont motivés par le terrorisme.

Deux catégories d'infractions pénales sont qualifiées de *graves* au sens de la LDPa: d'une part, les autres crimes conformément à l'annexe 1 LEIS, dans la mesure où ils peuvent être attribués à une catégorie d'infractions en vertu de la directive PNR de l'UE (cf. annexe 2 de la loi); d'autre part, les infractions relevant de la compétence de l'Office fédéral de la douane et de la sécurité des frontières (OFDF) en matière de poursuite pénale et qui sont passibles d'une peine privative de liberté maximale d'au moins trois ans.

Tant les infractions terroristes que les infractions pénales graves sont fixées par la loi. L'annexe 2 compare les catégories d'infractions PNR aux catégories correspondantes de l'annexe 1 LEIS, ce qui permet de comprendre quelles infractions prévues par la LEIS doivent être considérées comme des infractions pénales graves en vertu de l'art. 6, al. 3, let. a. Il est ainsi possible d'affirmer sans le moindre doute que telle ou telle infraction prévue par la LEIS est comprise dans les catégories d'infractions PNR, justifiant ainsi le traitement des données relatives aux passagers aériens.

Malgré leur légalité, les infractions prévues à l'al. 3, let. b, relevant de la compétence de l'OFDF en matière de poursuite pénale doivent être précisées par voie d'ordonnance. Cette précision déclaratoire garantit la sécurité du droit et la transparence (al. 4). En effet, cette solution simplifie les éventuelles modifications du droit pénal accessoire notamment.

Une vue d'ensemble actuelle de toutes les infractions déterminantes se trouve en annexe du présent rapport.

Les résultats obtenus par le traitement des données relatives aux passagers aériens qui permettraient de prévenir, de détecter ou de poursuivre d'autres infractions que celles qui sont mentionnées doivent être effacés immédiatement.

Le SRC est également tenu de respecter cette obligation. En effet, il peut aussi traiter des données relatives aux passagers aériens pour lutter contre les infractions terroristes et les autres infractions pénales graves, mais seulement si ce traitement sert à l'accomplissement de ses tâches, prévues à l'art. 6, al. 1, let a, ch. 1 et 3 à 5, LRens.

L'UIP n'est autorisée à traiter des données sensibles que de manière restreinte. Les entreprises de transport aérien ne peuvent pas lui livrer de telles données (cf. art. 2, al. 3). Si l'UIP en reçoit tout de même de leur part, elle doit les effacer immédiatement. Il se peut que des données sensibles soient collectées lorsque les données relatives aux passagers aériens sont comparées avec celles contenues dans les systèmes d'information ou lorsque l'UIP accède à ces systèmes (cf. art. 7). De plus, il est possible que des données sensibles soient concernées lors de la création de profils de risque et de listes d'observation sur demande d'une autorité. Par conséquent, l'art. 6, al. 6 prévoit que l'UIP est uniquement autorisée à traiter les données sensibles suivantes:

- données biométriques[36] identifiant une personne physique de façon unique;
- données sur les poursuites ou sanctions pénales ou administratives.

L'UIP doit effacer immédiatement les autres données sensibles qu'elle reçoit. Ce principe s'applique à toutes les tâches qu'elle effectue conformément à la présente loi.

Art. 7 Comparaison des données avec des systèmes d'information

Les données relatives aux passagers aériens sont comparées automatiquement avec celles issues des différents systèmes d'information de police dès qu'elles entrent dans le système d'information PNR (al. 1).

La loi ne mentionne aucune technologie spécifique, mais uniquement les buts de la comparaison. Cette formulation neutre d'un point de vue technologique garantit que les systèmes d'information remis en question puissent être remplacés sans qu'une révision de la disposition légale soit à chaque fois requise. En plus de cet avantage, elle renforce la pertinence de la disposition et limite la comparaison au strict nécessaire. Ainsi, elle est aussi convaincante pour ce qui est de la protection des données.

La comparaison automatique sert à la première identification, à la localisation et, le cas échéant, à l'arrestation de personnes qui entrent en Suisse ou quittent la Suisse par voie aérienne et sont recherchées au niveau national ou international en raison de liens avec des infractions terroristes ou autres infractions pénales graves (art. 6, al. 2 et 3). Elle peut en outre fournir des informations utiles liées à des infractions non élucidées. Les concordances qui ne remplissent pas le but défini par la loi doivent être effacées immédiatement (cf. art. 6, al. 5).

La comparaison automatique de toutes les données relatives aux passager aériens s'effectue à l'aide des systèmes d'information de police suivants:

36 Voir les explications dans le glossaire en annexe.

- système de recherches informatisées de personnes et d'objets (art. 15 de la loi fédérale du 13 juin 2008 sur les systèmes d'information de police de la Confédération [LSIP][37]);
- partie nationale du Système d'information Schengen (art. 16 LSIP);
- systèmes d'information de la Police judiciaire fédérale (PJF; art. 10 et 11 LSIP);
- système informatisé de gestion et d'indexation de dossiers et de personnes de l'Office fédéral de la police (art. 18 LSIP).

Le *système de recherches informatisées de personnes et d'objets (RIPOL)* contient des données sur les personnes signalées comme étant recherchées, des informations sur des infractions non élucidées, sur des personnes impliquées dans une infraction, sur des titulaires de documents d'identité d'origine suspecte ainsi que d'autres renseignements servant à élucider des infractions. Il aide les autorités compétentes de la Confédération et des cantons, en particulier lorsqu'il s'agit d'arrêter des personnes et d'écarter les menaces pour la sécurité publique. La comparaison des données relatives aux passagers aériens avec celles du RIPOL contribue non seulement à la réussite des recherches, mais aussi aux progrès dans les enquêtes non élucidées sur des infractions terroristes et autres infractions pénales graves au sens du présent avant-projet. Toute personne autorisée à effectuer des comparaisons avec le RIPOL reçoit automatiquement les concordances communiquées au moyen de la banque de données *Automated Search Facility* (ASF) d'INTERPOL. Cette banque de données contient des informations sur des personnes, des véhicules volés ainsi que sur des documents d'identification dérobés ou perdus.

Le *Système d'information Schengen (SIS)* contient des signalements de personnes et d'objets (par ex. relatifs à des documents d'identité volés) recherchés au sein de l'espace Schengen. La comparaison des données relatives aux passagers aériens avec celles du SIS peut mener à l'arrestation de personnes qui doivent être recherchées au niveau international puis extradées, qui doivent comparaître devant un tribunal dans le cadre d'une procédure pénale ou qui sont signalées aux fins de surveillance discrète, car on suppose qu'elles ont commis une infraction pénale grave.

Les deux systèmes d'information ci-après, différents du RIPOL et du SIS, contiennent également des informations relatives aux enquêtes en cours de la Confédération et des cantons, raison pour laquelle ils doivent également être utilisés pour procéder à la comparaison automatique des données relatives aux passagers aériens:

Le *système d'information de la PJF* (JANUS) contient des informations relatives aux enquêtes de police judiciaire de la Confédération ainsi qu'aux enquêtes préliminaires et aux enquêtes de police judiciaire des cantons (art. 10 LSIP). De plus, il comprend des informations importantes concernant la coopération de la PJF avec les autorités de poursuite pénale et les polices judiciaires des cantons ainsi qu'avec les autorités étrangères engagées dans la lutte contre la criminalité organisée active au niveau international (art. 11 LSIP).

37 RS **361**

Le *système informatisé de gestion et d'indexation de dossiers et de personnes de l'Office fédéral de la police* (IPAS) contient des informations relatives aux enquêtes de police judiciaire en cours et aux activités de police préventive menées par les autorités de poursuite pénale et de police suisses ou étrangères, notamment aussi la PJF ou le service compétent d'INTERPOL.

Chaque concordance obtenue par une comparaison automatique doit ensuite être vérifiée manuellement par l'UIP (al. 3) avant de pouvoir être communiquée à l'autorité compétente. Cette étape doit notamment empêcher que des concordances communiquées donnent lieu à des mesures sur la base d'une saisie erronée des données relatives aux passagers aériens, qu'elle soit intentionnelle ou non. L'obligation de vérification résulte de l'art. 6, al. 5, LPD, qui prévoit que celui qui traite des données doit s'assurer qu'elles sont exactes.

Malgré la vérification manuelle, l'ensemble des questions ne peuvent souvent pas être éclaircies et les doutes entourant l'identité de la personne ne peuvent pas être entièrement écartés.

Les motifs de signalement peuvent en outre soulever des questions. En effet, le traitement des données relatives aux passagers aériens n'est autorisé que s'il sert à la lutte contre les infractions terroristes et les autres infractions pénales graves. Il faut que les éléments constitutifs de l'infraction soient connus ou puissent être considérés comme existants sur la base d'informations de fond issues de banques de données pour pouvoir déterminer que la concordance obtenue correspond à l'une de ces infractions. Contrairement au RIPOL, qui permet de consulter les détails de l'infraction et l'élément constitutif de l'infraction, les concordances obtenues au moyen d'une comparaison dans le SIS indiquent uniquement les catégories d'infractions (par ex. "meurtre"), mais pas les faits pertinents ni l'élément constitutif de l'infraction en cause. D'autres systèmes d'information doivent être consultés afin de fournir ces éléments de réponse. La concordance doit être effacée si les indices relatifs à une infraction terroriste ou autre infraction pénale grave ne sont pas suffisants. D'ailleurs, elle doit également être effacée si le signalement figurant dans le SIS révèle un élément constitutif de l'infraction qui ne figure pas dans les catégories d'infractions PNR.

Les accès visant à établir la plausibilité permettent de vérifier les concordances obtenues lors de la première comparaison pour ce qui est de l'identité de la personne et du motif du signalement. Cela garantit un traitement des données relatives aux passagers aériens conforme au but défini par la loi et le signalement des bonnes personnes aux autorités de poursuite pénale compétentes et au SRC.

Une fois la comparaison automatique effectuée, les systèmes d'information ci-après devraient pouvoir être consultés manuellement dans le but d'établir la plausibilité de l'identité d'une personne et des motifs de signalement:

a) établissement de la plausibilité de l'identité d'une personne:

- SYMIC (loi fédérale du 20 juin 2003 sur le système d'information commun aux domaines des étrangers et de l'asile [LDEA][38]): le système d'information central sur la migration contient des données relatives à l'identité des personnes enregistrées (par ex. nom, prénom, date de naissance) et fournit

38 RS **142.51**

des informations sur le statut de séjour des étrangers qui se trouvent en Suisse.

- ORBIS (art. 109*c*, let. f, LEI): le système national d'information sur les visas fournit des informations sur les demandes de visa et donne accès aux données de toutes les personnes disposant d'un visa valable dans l'espace Schengen. Par exemple, une personne peut être identifiée au moyen du numéro de passeport vérifiable.

b) établissement de la plausibilité des motifs de signalement:

- index national de police (art. 17 LSIP): ce système fournit des informations sur les communications des cantons.
- SIRENE-IT (art. 5 de l'ordonnance N-SIS du 8 mars 2013[39]): l'accès à ce système d'information permet, grâce à des informations de fond complémentaires, d'attribuer un signalement contenu dans le Système d'information Schengen à un élément constitutif de l'infraction précis dans le domaine de la criminalité organisée et du terrorisme.
- I-24/7 (art. 352, al. 1, CP): ce système contient des informations permettant d'établir les motifs de signalements internationaux (INTERPOL)
- système d'information de l'OFDF: ce système contient notamment des informations importantes relatives aux éléments constitutifs de l'infraction relevant de la compétence de cette autorité en matière de poursuite pénale.

Les systèmes d'information avec lesquels la comparaison automatique a été effectuée doivent également être consultés manuellement, non seulement pour établir la plausibilité du motif du signalement, mais aussi pour déterminer l'autorité compétente à laquelle la concordance vérifiée doit être transmise en vertu de l'art. 8.

La manière de procéder en deux temps permet un traitement des données aussi restreint que possible. En effet, le traitement effectué après la comparaison automatique que prévoit l'al. 1 ne se limite plus qu'aux données présentant un premier soupçon. Une fois ces données vérifiées par l'accès prévu à l'al. 3, leur nombre diminue et seules les données confirmant le premier soupçon sont affichées. Les autres données ne sont plus concernées.

La comparaison automatique et l'accès manuel aux différents systèmes nécessitent des modifications de la LEI (ORBIS), de la LSIP (RIPOL, JANUS, index national de police) et de la LDEA (SYMIC), lesquelles sont présentées à l'annexe 3 LDPa. Compte tenu de la révision en cours de la législation douanière, la base légale éventuellement nécessaire pour ce qui est de l'accès manuel au système d'information de l'OFDF sera exposée dans le message ad hoc.

Art. 8 Transmission des résultats

Les autorités de poursuite pénale de la Confédération et des cantons ainsi que le SRC peuvent être les destinataires de concordances vérifiées. Font également partie des

39 RS **362.0**

autorités de poursuite pénale de la Confédération le Commissariat Gardes de sûreté dans l'aviation (SIBEL), rattaché au Service fédéral de sécurité (art. 4, let. b, de la loi sur l'organisation des autorités pénales [LOAP][40]), ainsi que l'OFDF (art. 4, let. c, LOAP).

L'UIP transmet les concordances vérifiées conformément à l'art. 7, al. 3, à l'autorité:

- qui est responsable du signalement ayant déclenché la concordance; ou
- (dans le cas de signalements d'un autre État) qui doit décider si des mesures doivent être prises sur la base de la transmission de l'UIP, et si oui lesquelles.

Art. 9 *Comparaison des données avec des profils de risque et les listes d'observation*

L'UIP doit pouvoir créer des profils de risque et des listes d'observation pour traiter les données relatives aux passagers aériens (al. 1). Pour que l'utilisation de ces instruments soit concluante, il est indispensable qu'elle dispose de connaissances spécialisées, de valeurs empiriques et d'informations de fond, ce qui est garanti, car:

- l'UIP se compose de collaborateurs possédant des connaissances spécialisées propres aux autorités fédérales et cantonales compétentes (cf. commentaire de l'art. 20);
- les autorités de poursuite pénale de la Confédération et des cantons et le SRC peuvent demander l'établissement de profils de risque et de listes d'observation (al. 1).

L'al. 2 constitue la base légale permettant à l'UIP de comparer les données relatives aux passagers aériens avec les profils de risque et les listes d'observation.

Seules les informations pouvant être attribuées à une catégorie de données prévue à l'annexe 1 de la loi peuvent faire l'objet de profils de risque et de listes d'observation. Il est ainsi exclu d'utiliser des données sensibles telles que l'ethnie ou l'appartenance religieuse (cf. art. 2, al. 3)

Les *profils de risque* décrivent des combinaisons de données dont l'expérience montre qu'elles sont récurrentes dans le cadre d'activités criminelles en lien avec des infractions terroristes ou autres infractions pénales graves. Ils doivent couvrir les différentes infractions mentionnées dans la liste correspondante. Toutefois, ils ne peuvent que se composer des catégories de données qualifiées de données relatives aux passagers aériens à l'annexe 1 du présent avant-projet (al. 3).

Les *listes d'observation* se composent d'informations qui sont déjà connues, qui peuvent être attribuées à une catégorie de données prévue à l'annexe 1 de la loi et qui concernent des personnes ou des organisations soupçonnées d'avoir commis ou de planifier des infractions terroristes ou autres infractions pénales graves. La comparaison des données relatives aux passagers aériens avec les listes d'observation permet par exemple de chercher certaines adresses électroniques ou certains numéros de téléphone ou de carte de crédit, le but étant d'établir des liens encore inconnus avec des

40 RS **173.71**

personnes soupçonnées d'avoir commis des infractions terroristes ou autres infractions pénales graves. Il est ainsi possible d'identifier notamment les personnes de liaison d'auteurs connus ou les membres d'organisations criminelles (al. 4).

Les profils de risque et les listes d'observation doivent être vérifiés régulièrement pour en confirmer le caractère fondé et l'efficacité (al. 5). L'UIP efface les contenus qui ne répondent plus à ces exigences.

Le Conseil fédéral détermine dans une ordonnance les modalités de la vérification, à savoir l'autorité compétente et la périodicité (al. 6, let. a), ce qui permet de mieux tenir compte des enseignements qui seront tirés à l'avenir au moyen de ces instruments lors du traitement des données relatives aux passagers aériens.

Le Conseil fédéral déterminera également par voie d'ordonnance pour quelles infractions parmi les catégories pertinentes pour le traitement de données relatives aux passagers aériens il est permis d'utiliser des listes d'observation. Dans ce contexte, l'accent doit être mis sur les infractions terroristes et celles en lien avec le crime organisé.

Art. 10 Collaboration avec le SRC

Le SRC a une position particulière en matière de lutte contre les infractions terroristes et les autres infractions pénales graves; sa recherche d'informations précède généralement la poursuite pénale et sert à anticiper et à prévenir les menaces pour la sécurité intérieure ou extérieure.

Par conséquent, le SRC peut traiter les données relatives aux passagers aériens pour accomplir ses tâches en toute autonomie. Toutefois, le traitement autonome de ces données est autorisé de manière très restrictive. Il n'est ainsi pas prévu que le SRC obtienne un accès direct au système d'information PNR. À la place, l'UIP lui transmet les données par voie électronique dans le cadre d'une procédure automatisée, comme le prévoit l'art. 104*b* LEI pour les données API. La transmission automatique est aussi appropriée en raison du volume de données. Le SRC reçoit les données relatives aux passagers aériens des aéroports de départ et d'arrivée qu'il a définis au préalable sur la base de sa propre évaluation des risques. Il peut ainsi surveiller les déplacements de personnes sur les trajets qui constituent des risques pour la sécurité.

Cette proposition se fonde sur la solution retenue aux art. 104*a* et 104*b* LEI concernant l'utilisation des données API par le SRC. Dans son message du 2 mars 2018 relatif à la révision de la loi fédérale sur les étrangers[41], le Conseil fédéral expliquait à ce sujet:

"En 2015, la délégation des Commissions de gestion a, sur la base d'un rapport interne et d'un avis juridique du Préposé fédéral à la protection des données et à la transparence (PFPDT), déclaré légitime l'utilisation des données API par le SRC sans que celui-ci n'ait accès au système API. Dans un souci de sécurité du droit, il convient toutefois de créer, à l'occasion de la présente révision, une base légale explicite sur la transmission électronique des données API. De plus, le SRC doit pouvoir demander au SEM d'étendre l'obligation des entreprises de transport aérien de communiquer des données à d'autres lieux de départ de vols dans le but de prévenir les menaces que représentent pour la sécurité intérieure ou extérieure le terrorisme, l'espionnage et la prolifération."

41 FF **2018** 1712

Une autre restriction s'impose au SRC dans le traitement des données relatives aux passagers aériens: il ne peut traiter ces données que pour lutter contre les infractions terroristes et les autres infractions pénales graves liées à ses tâches, prévues à l'art. 6, al. 1, let. a, ch. 1 et 3 à 5, LRens (al. 2). Le tableau ci-dessous présente les éléments constitutifs de l'infraction concernés. Les infractions de la catégorie 1 (terrorisme) justifient un traitement des données relatives aux passagers aériens uniquement en cas de motivation terroriste. Cela s'applique dans tous les cas où l'élément constitutif de l'infraction ne présuppose pas expressément une motivation terroriste, comme en cas d'émeute (art. 260 CP).

Art. 6, al. 1, let. a, ch. 1 et 3 à 5, LRens	**Éléments constitutifs de l'infraction au sens de l'art. 6, al. 2 et 3, pour la répressions desquels un traitement est autorisé en vertu de la LRens**
Ch. 1: terrorisme	Menaces alarmant la population, provocation publique au crime ou à la violence, émeute, actes préparatoires délictueux, organisations criminelles et terroristes, mise en danger de la sécurité publique au moyen d'armes, financement du terrorisme, recrutement, formation et voyage en vue d'un acte terroriste, groupements illicites (art. 258, 259, 260, al. 1, 260*bis*, 260*ter*, 260*quater*, 260*quinquies*, 260*sexies*, 275*ter*, CP)
	Interdiction d'organisation (art. 74 LRens)
	Dispositions pénales conformément à la loi fédérale du 12 décembre 2014 interdisant les groupes "Al-Qaïda" et "État islamique" et les organisations apparentées[42] (art. 2)
Ch. 3: dissémination d'armes nucléaires, biologiques ou chimiques, y compris leurs vecteurs et tous les biens et technologies à des fins civiles ou militaires qui sont nécessaires à leur fabrication (prolifération NBC) ou le commerce illégal de substances radioactives, de matériel de guerre et d'autres biens d'armement,	Délits et crimes conformément à la loi sur les armes[43] (art. 33, al. 3)
	Emploi, avec dessein délictueux, d'explosifs ou de gaz toxiques (art. 224, al. 1, CP)
	Fabriquer, dissimuler et transporter des explosifs ou des gaz toxiques (art. 226 CP)
	Danger imputable à l'énergie nucléaire, à la radioactivité et aux rayonnements ionisants (art. 226bis CP)
	Actes préparatoires punissables (art. 226ter CP)
	Infractions aux mesures de sécurité et de sûreté (art. 88, al. 2, de la loi sur l'énergie nucléaire [LENu][44])

42 RS **122**
43 RS **514.54**
44 RS **732.1**

Ch. 4: attaques visant des infrastructures d'information, de communication, d'énergie, de transport et autres qui sont indispensables au fonctionnement de la société civile, de l'économie et de l'État (infrastructures critiques),	Infractions relatives à des articles nucléaires ou à des déchets radioactifs (art. 89, al. 2, LENu) Soustraction de données (art. 143 CP) Détérioration de données (art. 144bis, al. 3, CP) Utilisation frauduleuse d'un ordinateur (art. 147, al. 1 et 2, CP) Inondation. Écroulement (art. 227, ch. 1, CP) Dommages aux installations électriques, travaux hydrauliques et ouvrages de protection (art. 228, ch. 1, CP)
Ch. 5: extrémisme violent.	Dommages à la propriété (art. 144, al. 3, CP) Incendie intentionnel (art. 221, al. 1 et 2, CP) Explosion (art. 223, ch. 1, CP) Dommages à la propriété (art. 144, al. 3, CP) Incendie intentionnel (art. 221, al. 1 et 2, CP) Explosion (art. 223, ch. 1, CP) Emploi, avec dessein délictueux, d'explosifs ou de gaz toxiques (art. 224, al. 1, CP) Fabriquer, dissimuler et transporter des explosifs ou des gaz toxiques (art. 226 CP) Inondation. Écroulement (art. 227, ch. 1, CP) Dommages aux installations électriques, travaux hydrauliques et ouvrages de protection (art. 228, ch. 1, CP) Mise en danger de la sécurité publique au moyen d'armes (art. 260^{quater} CP)

Le SRC doit effacer les données relatives aux passagers aériens 96 heures au plus après les avoir reçues (al. 3). En fixant cette durée de conservation, la loi répond à une règlementation du SRC relative au système de "stockage des données résiduelles". La même règlementation s'applique d'ailleurs aussi aux données API transmises automatiquement au SRC.

Art. 11 Transmission de données sur demande

Les données relatives aux passagers aériens peuvent contribuer de manière significative à la réussite des enquêtes portant sur des infractions terroristes ou des infractions pénales graves. Elles doivent aussi être utilisées pour apporter certains éclaircissements. L'UIP est donc autorisée, sur demande, à effectuer des recherches spécifiques parmi les données du système d'information PNR (al. 1).

La recherche demandée doit être suffisamment précise et circonscrite. De plus, la demande doit exposer de manière concluante les raisons pour lesquelles les données sollicitées sont nécessaires pour élucider ou prévenir une infraction terroriste ou une autre infraction pénale grave. Les recherches d'ordre général, c'est-à-dire celles dont

la teneur n'est pas spécifiée et qui produisent une multitude de résultats divers, ne sont en revanche pas autorisées. Aucune suite ne doit donc être donnée aux demandes allant dans ce sens.

Le fait qu'Europol (let. c) soit habilité, au même titre que les autorités suisses mentionnées à l'art. 8, à soumettre une demande sans que la communication des données soit régie par un traité international s'explique notamment par l'accord que la Suisse a conclu avec Europol le 24 septembre 2004[45]. Cet accord règle la coopération en matière de lutte contre toute forme sérieuse de criminalité internationale. L'échange de données entre la Suisse et Europol est uniquement autorisé s'il s'agit d'infractions combattues en vertu tant de cet accord que de la LDPa. Par conséquent, il est exclu de transmettre à Europol des données relatives aux infractions qui, bien qu'elles soient mentionnées dans l'accord, n'entrent pas dans le domaine d'application de la LDPa.

En revanche, s'il s'agit d'infractions qui ne sont pas régies par l'accord, mais qui sont des infractions terroristes ou des infractions pénales graves au sens de la LDPa, l'UIP a l'autorisation de transmettre des données à Europol conformément à l'art. 16, al. 1, LPD, le Conseil fédéral ayant confirmé que tous les États membres de l'UE garantissent un niveau adéquat de protection des données[46]. Cette règle s'applique également à l'association des États membres et donc à Europol.

Art. 12 Information en cas de soupçon

L'utilisation de profils de risque et de listes d'observation peut indiquer qu'une infraction terroriste ou une autre infraction pénale grave a été commise, est en train d'être commise ou est planifiée. L'UIP doit transmettre spontanément les résultats sur lesquels ce soupçon se fonde aux autorités de poursuite pénale compétentes. Toutefois, cette communication a lieu uniquement si le soupçon de l'UIP est concret. Il est réputé concret lorsqu'il concerne une personne en particulier et que plusieurs indices montrent qu'une infraction terroriste ou une autre infraction pénale grave a été commise ou est planifiée.

Les autorités de poursuite pénales auxquelles le soupçon concret a été communiqué décident de la suite de la procédure.

Les données sensibles qui peuvent être transmises conformément à l'al. 2 sont les données biométriques identifiant une personne physique de façon unique et les données sur les poursuites ou sanctions pénales ou administratives (cf. art. 6, al. 5). L'UIP ne peut donc ni traiter ni transmettre d'autres données sensibles.

Section 4 Système d'information PNR

Art. 13

L'UIP exploite le système d'information PNR.

45 RS **0.362.2**
46 https://www.edoeb.admin.ch/dam/edoeb/fr/dokumente/2021/20211115_Staatenliste_f.pdf.download.pdf/20211115_Staatenliste_f.pdf

L'accès est limité aux collaborateurs de l'UIP ainsi qu'aux personnes chargées de l'entretien, de la programmation ou de la surveillance dans la mesure où cet accès est absolument nécessaire à l'accomplissement de leurs travaux.

Section 5 Protection des données

L'*obligation* d'accorder une si grande importance à la protection des données tient au fait que, dans la lutte contre les infractions terroristes et les autres infractions pénales graves, les données de personnes ne présentant aucun lien avec de telles infractions sont aussi collectées, puis traitées. Cet état de fait est toutefois inévitable, sauf à remettre en question les objectifs fixés par la loi.

Il en va de même pour ce qui est de la disponibilité relativement longue des données, effacées après seulement cinq ans. Le rapport de la Commission européenne du 24 juillet 2020 sur le réexamen de la directive PNR mentionne à ce sujet[47]:

"Les enquêtes et les poursuites concernant ce type d'infractions demandent généralement des mois et souvent des années de travail. Dans cette logique, les États membres ont confirmé que la période de conservation de cinq ans était nécessaire d'un point de vue opérationnel. La disponibilité des données historiques garantit que, lorsqu'un individu est accusé d'avoir commis une infraction pénale grave ou d'être impliqué dans des activités terroristes, il est possible d'examiner l'historique de ses déplacements et de trouver les personnes ayant voyagé avec lui, d'identifier les complices ou les autres membres potentiels d'un groupe criminel ainsi que les victimes éventuelles."

La protection des données est garantie non seulement par les dispositions prévues dans la présente section, mais en particulier aussi par l'obligation des entreprises de transport aérien d'informer leurs passagers du traitement des données en vertu de la présente loi (art. 5), la manière de procéder en deux temps à la comparaison des données (art. 7) et la conclusion de traités internationaux limitée aux États garantissant un niveau de protection des données comparable à celui de la Suisse (art. 21).

Art. 14 Pseudonymisation

Les données relatives aux passagers aériens comprennent plusieurs catégories de données permettant d'identifier leur titulaire. Elles sont automatiquement pseudonymisées six mois après avoir été introduites dans le système d'information PNR.

Cette règle s'applique aux données ci-après d'une personne:

- nom(s), ainsi que nombre et noms des autres personnes voyageant avec elle;
- adresse et coordonnées (adresse électronique, numéro de téléphone et de portable);
- toutes les informations relatives aux modes de paiement, y compris l'adresse de facturation;

47 Rapport de la Commission au Parlement européen et au Conseil sur le réexamen de la directive (UE) 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, COM(2020) 305 final

- informations "grands voyageurs";
- renseignements généraux permettant d'identifier immédiatement le passager aérien dont les données PNR sont saisies;
- données API collectées, le cas échéant.

Ces données ne peuvent donc plus être mises en relation avec leur titulaire, mais uniquement avec un pseudonyme. Toute personne souhaitant annuler la pseudonymisation a besoin de la table de concordance, conservé en lieu sûr, sur lequel chacun des pseudonymes utilisés est relié au nom de la personne concernée.

Conformément au message concernant la nouvelle loi sur la protection des données, la pseudonymisation est une mesure technique adéquate permettant de garantir la sécurité des données personnelles (art. 8 LPD)[48]. De plus, dans ce message, le Conseil fédéral déclare que la loi sur la protection des données ne s'applique pas aux données "si une ré-identification par un tiers est impossible (les données ont été anonymisées complètement et définitivement) ou ne paraît possible qu'au prix d'efforts tels qu'aucun intéressé ne s'y attèlera. Cette dernière règle vaut aussi pour les données pseudonymisées[49]."

Le délai de six mois avant la pseudonymisation correspond à la solution qui avait été retenue dans la loi fédérale du 18 mars 2016 sur la surveillance de la correspondance par poste et télécommunication[50], notamment en ce qui concerne l'enregistrement des données secondaires de télécommunication (art. 26, al. 5). Les données sont également enregistrées indépendamment de tout soupçon, peuvent être attribuées à une personne spécifique et, le cas échéant, traitées par l'État dans le but de lutter contre la criminalité, comme c'est le cas pour les données relatives aux passagers aériens.

Art. 15 Levée de la pseudonymisation

Comme le mentionne clairement le rapport de la Commission européenne sur le réexamen de la directive PNR cité ci-avant, les enquêtes sur les infractions terroristes et les autres infractions pénales graves s'étendent sur plusieurs années. Les expériences faites en Suisse confirment également ce propos. Il doit donc être possible d'effectuer des requêtes dans la base de données du système d'information PNR même si les données datent de plus de six mois et qu'elles ont été pseudonymisées. Compte tenu de ces requêtes effectuées sur des éléments anciens, il faut que la pseudonymisation puisse être annulée.

La demande de levée de la pseudonymisation doit être déposée à l'UIP, qui la transmet au TAF accompagnée de sa recommandation, pour autant que les raisons de la demande soient suffisantes (al. 2). Les motifs de la demande sont réputés suffisants:

- si les données devant faire l'objet d'une levée de la pseudonymisation sont définies. Cette condition est remplie lorsque la demande de levée de la pseudonymisation concerne par exemple une personne ou un vol en particulier;

48 FF **2017** 6650
49 FF **2017** 6640
50 RS **780.1**

- s'il est rendu vraisemblable que la levée de la pseudonymisation fournit des informations déterminantes à des fins de prévention, de détection, d'enquête et de poursuite en matière d'infractions terroristes et autres infractions pénales graves. Les informations déterminantes requises doivent être décrites avec la plus grande précision possible.

Si la demande n'est pas ou pas suffisamment motivée, l'UIP en informe l'autorité requérante, qui a la possibilité d'apporter des corrections à sa demande.

Le TAF statue sur l'éventuelle levée de la pseudonymisation dans un délai de cinq jours ouvrables (al. 4). Les droits allemand[51] et autrichien[52] prévoient la compétence d'un tribunal en application de l'art. 12, al. 3, de la directive PNR de l'UE.

Le délai octroyé au TAF est de cinq jours ouvrables au maximum (al. 4). Ce délai maximum ne dispense pas pour autant le tribunal de statuer immédiatement en cas d'urgence. Il y a notamment urgence en cas de menace d'attentat terroriste.

La clé technique de levée de la pseudonymisation est conservée auprès de l'UIP et son accès est protégé. L'UIP ne peut l'utiliser que si le TAF approuve une demande de levée de la pseudonymisation.

La communication de données qui datent de moins de six mois est régie par l'art. 11 et ne nécessite aucune participation du TAF.

Art. 16 Durée de conservation et effacement des données

Les données relatives aux passagers aériens sont effacées automatiquement cinq ans après leur introduction dans le système d'information PNR (al. 1).

La durée de conservation de cinq ans prévue à l'art. 16 se fonde sur la directive PNR et garantit ainsi la compatibilité du système PNR suisse avec celui des États membres de l'UE. Cette compatibilité est une condition essentielle au traité concernant l'échange de données relatives aux passagers aériens que la Suisse souhaiterait conclure avec l'UE.

La durée de conservation relativement longue résulte en premier lieu de l'utilisation des données relatives aux passagers aériens comme instrument de lutte contre les infractions terroristes et les autres infractions pénales graves. Les enquêtes sur ces infractions, notamment celles visant à détecter des réseaux internationaux, s'étendent souvent sur plusieurs années. À l'occasion du réexamen de la directive PNR effectuée par la Commission européenne, les États membres de l'UE ont confirmé que la durée de conservation des données prévue par la directive PNR était nécessaire d'un point de vue opérationnel. De plus, les règlementations relatives à l'accès par les autorités

51 Gesetz über die Verarbeitung von Fluggastdaten zur Umsetzung der Richtlinie (EU) 2016/681 (Fluggastdatengesetz - FlugDaG), § 5 Abs. 2, BGBl 117s1484

52 Bundesgesetz über die Verarbeitung von Fluggastdaten zur Vorbeugung, Verhinderung und Aufklärung von terroristischen und bestimmten anderen Straftaten (PNR-Gesetz – PNR-G), § 6 Abs. 2, BGBl. I Nr. 64/2018

compétentes aux données stockées par l'UIP et leur dépersonnalisation (soit leur pseudonymisation au sens de l'art. 14 du projet de loi) se sont révélées suffisantes pour prévenir les abus[53].

La longue durée de conservation des données, dont la majorité ne prête à aucun soupçon, est un changement de paradigme pour la Suisse. Ce dernier se justifie par le but principal de la présente loi, à savoir la lutte efficace contre la grande criminalité au niveau national et international à l'aide du PNR.

Le Conseil fédéral fixe dans une ordonnance la durée de conservation maximale des concordances résultant d'une comparaison au sens des art. 7 et 9 (al. 2), ce qui permet de satisfaire aux différentes procédures pour lesquelles les autorités ont besoin des données présentant un soupçon confirmé, notamment les enquêtes et les procédures pénales.

Art. 17 Surveillance

Au niveau de l'office, le service de protection des données de fedpol veille à ce que les dispositions relatives à la protection des données contenues dans la présente loi et la loi fédérale sur la protection des données soient respectées.

Cette surveillance porte tant sur le traitement des données effectué par l'UIP que sur les aspects techniques de la protection des données garantis par le système d'information PNR, dont font partie la pseudonymisation automatique des données après six mois et leur effacement automatique après cinq ans.

Malgré la fonction de surveillance assumée par le service de protection des données de fedpol, la surveillance du PFPDT prévue à l'art. 4 LPD est réservée.

Art. 18 Droit d'accès

En vertu de l'art. 5, un passager aérien est informé par l'entreprise de transport aérien que ses données sont traitées conformément à la présente loi. Conformément à l'art. 18 de la présente loi et aux art. 25 à 28 LPD, toute personne souhaitant des renseignements doit les demander à fedpol.

Compte tenu du but visé par le traitement des données, il est entendu que les renseignements ne peuvent pas toujours être communiqués, du moins pas en intégralité. fedpol devra se prévaloir de ce droit conformément à l'art. 26, al. 2, let. b, LPD, lorsque:

- la communication de renseignements est refusée dans l'intérêt public prépondérant, notamment lorsqu'il est question de la sécurité intérieure ou extérieure de la Suisse; ou
- la communication de renseignements est susceptible de compromettre une enquête, une instruction ou une procédure administrative ou judiciaire.

53 Rapport de la Commission au Parlement européen et au Conseil sur le réexamen de la directive (UE) 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, COM(2020) 305 final

La communication de renseignements est également exclue lorsque les données datent déjà de plus de six mois et ont donc été pseudonymisées. Le demande de levée de la pseudonymisation est uniquement du ressort des autorités de poursuite pénale et du SRC, conformément à l'art. 15, al. 1.

Si l'UIP a transmis les données de la personne concernée à une autre autorité, fedpol la consulte avant la communication de renseignements, ce qui permet de garantir la prise en compte à temps des éventuels motifs de restrictions du droit d'accès en vertu de l'art. 25 LPD.

Section 6 Organisation et personnel de l'UIP

Art. 19 Organisation

L'UIP est rattachée à fedpol. Cette attribution résulte d'une part de la finalité du traitement des données. Elle se justifie d'autre part par la vaste expérience de fedpol dans le domaine des systèmes d'information, ce qui devrait avoir une répercussion positive sur la mise en place et l'exploitation du système d'information PNR.

Pour ce qui est de la particularité des données relatives aux passagers aériens, dont il convient de garantir la protection, il est justifié que l'UIP soit distincte, sur le plan de l'organisation, des unités de fedpol qui assument des tâches d'enquêtes. Ces unités sont soumises aux mêmes conditions que les autres autorités de poursuite pénale de la Confédération et des cantons si elles souhaitent recevoir des données de l'UIP.

L'UIP est le point de contact unique des entreprises de transport aérien et des autorités étrangères en matière de données PNR. La question de savoir si l'UIP assure un service permanent reste ouverte. Même si la Suisse applique une interdiction des vols de nuit, les entreprises de transport aérien transmettent tout de même les données relatives aux passagers aériens à l'UIP durant la nuit.

Art. 20 Personnel

Le traitement des données relatives aux passagers aériens offre une importante plus-value tant pour les autorités de poursuite pénale de la Confédération que pour celles des cantons.

Compte tenu du système fédéraliste de la Suisse, la poursuite pénale relève généralement de la compétence première des cantons. En revanche, la Confédération s'engage dans la poursuite de certaines infractions pénales graves, telles que le terrorisme ou le crime organisé, et dans celle de diverses infractions relevant du droit pénal accessoire fédéral, dont font partie les éléments constitutifs de l'infraction contenus par exemple dans les lois sur l'énergie nucléaire[54], sur la protection des marques[55], sur la transplantation[56] ou sur les armes[57].

54 RS **732.1**
55 RS **232.11**
56 RS **810.21**
57 RS **514.54**

Dans ce contexte, la lutte contre les infractions terroristes et les autres infractions pénales graves se veut être une tâche commune de la Confédération et des cantons, chacun ayant ses spécificités, et l'UIP apporte son soutien aux autorités compétentes.

L'aspect international de l'accomplissement des tâches, notamment, plaide en faveur d'un rattachement de l'UIP à la Confédération sur le plan organisationnel, ce qui ne signifie toutefois pas que la Confédération doit supporter seule les coûts liés à cette nouvelle tâche. La Confédération et les cantons supportent à parts égales les frais liés aux collaborateurs employés au sein de l'UIP.

Le modèle envisagé prévoit le détachement auprès de l'UIP de collaborateurs provenant de la Confédération et des cantons pour une durée déterminée. Les modèles de collaboration particuliers comme ceux qui sont proposés ici existent déjà dans les centres de coopération policière et douanière de Genève et de Chiasso[58], ainsi qu'au Service de protection des témoins.

La présente loi et l'ordonnance qui y est relative, d'une part, et une convention entre la Confédération et les cantons, d'autre part, constituent la base de la coopération en vertu de la présente loi. La question de savoir si les cantons règlent leur participation par un concordat est encore ouverte à l'heure actuelle.

Le commentaire bâlois sur la Constitution[59] souligne à ce sujet:

"Comme la Constitution fédérale ne prévoit pas que les conventions fixant des règles de droit conclues entre la Confédération et les cantons soient une forme d'acte législatif à part entière (art. 163 Cst.), les conditions-cadres de la convention doivent au moins être fixées par une loi fédérale (art. 164 Cst.) ou, en cas de dispositions d'une importance mineure, par une ordonnance. Ce n'est qu'en vertu de cette base juridique […] qu'une convention peut être conclue avec les cantons."

L'objet de la convention entre la Confédération et les cantons est le détachement de collaborateurs au service de l'UIP.

Il doit ressortir de la loi:

- dans quel but les cantons détachent leurs collaborateurs;
- dans quelles proportions la Confédération et les cantons participent aux ressources en personnel de l'UIP.

Le personnel de l'UIP se compose à parts égales de collaborateurs de la Confédération et des cantons (al. 1). L'autorité supporte les coûts relatifs au détachement de ses collaborateurs (al. 4).

La loi doit aussi mettre en évidence que les collaborateurs restent engagés auprès de l'autorité qui les détache malgré leur engagement au sein de l'UIP, ce qui signifie que cette dernière reste leur employeur d'un point de vue contractuel. Cette condition est remplie par les al. 2 (droit partagé de donner des instructions) et 4 (susmentionné).

58 Cf. convention du 2 avril 2014 relative à l'exploitation nationale des centres communs de coopération policière et douanière (CCPD) de Genève et de Chiasso, RS **360.4**

59 Schweizerisches Verfassungsrecht, 3.A., Basel 2016; Waldmann Bernhard / Belser Eva Maria / Epiney Astrid (Hrsg.), Basler Kommentar Bundesverfassung, Basel 2015, Art. 48 N 37

Les principales différences par rapport aux rapports de travail actuels nécessitent également une base légale. Il s'agit:

- du droit conféré à fedpol de donner des instructions spécifiques (al. 2), qui remplace celui de l'employeur contractuel pendant la durée de l'engagement des collaborateurs auprès de l'UIP;
- de l'obligation des collaborateurs de garder le secret (art. 3), qui doit également être respectée vis-à-vis de leur employeur contractuel.

L'employeur contractuel conserve le droit de donner des instructions en matière de discipline (al. 2) et l'obligation de prendre à sa charge le salaire et les éventuels frais, indemnités pour travail supplémentaire et primes de ses collaborateurs. Le montant de ces indemnités en faveur des collaborateurs provenant des cantons est régi par les dispositions cantonales en la matière.

Pour compléter ces dispositions légales, le Conseil fédéral peut prévoir d'autres règlementations au niveau de l'ordonnance (al. 5).

Indépendamment de la présente loi, l'art. 1, al. 1, let. f, de la loi sur la responsabilité[60] s'applique aux collaborateurs des cantons engagés au sein de l'UIP.

Les qualifications recherchées pour les collaborateurs détachés à l'UIP doivent figurer dans la convention avec les cantons. Entrent notamment en ligne de compte les collaborateurs disposant de connaissances éprouvées de la procédure pénale.

De plus, la convention doit contenir des informations sur la manière de procéder lorsqu'un collaborateur:

- se révèle être inadapté à la tâche;
- adopte un comportement pouvant entraîner des mesures disciplinaires.

Il convient aussi de régler la procédure en cas de désaccords entre fedpol et un canton.

En dehors de l'UIP, les collaborateurs ne disposent pas librement des éléments dont ils ont connaissance durant leur engagement, conformément à l'al. 3. Cette disposition s'applique également une fois leur engagement terminé. Par conséquent, l'échange informel de contenus soumis à la protection des données est interdit entre l'UIP et l'unité qui détache ses collaborateurs.

Il est en revanche souhaitable que les collaborateurs, une fois revenus de leur engagement à l'UIP, transmettent à leurs collègues le savoir méthodologique qu'ils y ont acquis en matière de traitement des données relatives aux passagers aériens. On peut par exemple penser aux expériences faites sur la manière de concevoir et d'utiliser des profils de risque et des listes d'observation avec autant d'efficacité que possible. Ainsi, le modèle de détachement garantit un transfert de compétences de l'UIP aux autorités qui détachent leurs collaborateurs.

60 RS **170.32**

Section 7 Conclusion de traités et de conventions et assistance administrative

Art. 21 Conclusion de traités et de conventions

La LDPa et la loi sur la protection des données produisent des effets contraignants uniquement pour la Suisse.

Lorsque la Suisse transmet des données relatives aux passagers aériens à un autre État, il y a lieu de veiller à ce que le droit interne de cet État garantisse une protection des données communiquées comparable à celle de la Suisse. La liste des États, disponible au format électronique, indique si un État garantit cette protection[61].

Si la protection des données est jugée comparable à celle de la Suisse, les données peuvent être communiquées à l'État en question sans traité international (art. 16, al. 1, LPD). Néanmoins, l'art. 21, al. 1, de la présente loi demande également la conclusion d'un traité international dans ce cas. En effet, il n'y a que de cette manière que la Suisse peut s'assurer la réciprocité de la transmission des données pour lutter contre le terrorisme et les autres infractions pénales graves et recevoir les données relatives aux passagers aériens sur les vols au départ de ces États à destination de la Suisse.

L'al. 2 octroie à fedpol la compétence de conclure des conventions avec des autorités étrangères en toute autonomie. Cette compétence est restreinte aux aspects opérationnels, techniques ou administratifs. Les questions fondamentales en matière de protection des données ou les droits et les obligations des autorités doivent en revanche toujours faire l'objet d'un traité international conclu par le Conseil fédéral en vertu de l'al. 1.

Art. 22 Assistance administrative

L'assistance administrative que l'UIP octroie à une UIP étrangère en l'absence d'un traité international réglant plus en détail la communication des données entre la Suisse et l'État en question se limite à des cas exceptionnels dûment justifiés. La transmission de données relatives aux passagers aériens n'est pas autorisée s'il n'existe aucun soupçon fondé contre la personne accusée d'avoir commis ou de planifier une infraction terroriste ou une autre infraction pénale grave.

La communication est restreinte aux données devant être précisées suffisamment dans la demande de l'UIP requérante. De plus, ces données doivent être indispensables pour écarter une menace imminente. La directive PNR prévoit également une exception similaire (art. 9, al. 1 et 2).

Une levée de la pseudonymisation n'est pas autorisée pour l'assistance administrative prévue par la présente disposition.

61 https://www.edoeb.admin.ch/dam/edoeb/fr/dokumente/2021/20211115_Staatenliste_f.pdf.download.pdf/20211115_Staatenliste_f.pdf

Section 8 Sanctions administratives

Art. 23 Sanctions en cas de violation des obligations des entreprises de transport aérien

Une violation du devoir de diligence et de l'obligation d'informer prévus aux art. 4 et 5 est sanctionnée indépendamment du fait que l'entreprise en question prouve que la faute ne lui est pas imputable, comme le prévoit l'art. 122*b* LEI depuis le 1er octobre 2015. À l'époque, le Conseil fédéral a renoncé à une telle preuve en justifiant qu'elle n'aurait pu être apportée qu'en menant d'importantes recherches à l'étranger, chose qui se serait révélée quasiment impossible en pratique[62].

La violation d'une obligation d'une entreprise de transport aérien est présumée lorsque cette dernière:

- omet de fournir les données relatives aux passagers aériens à l'UIP ou les lui fournit trop tard;
- ne respecte pas les prescriptions techniques de fedpol en fournissant les données relatives aux passagers aériens à l'UIP;
- ne fournit pas toutes les données des passagers.

Il en va de même:

- si les données transmises sont manifestement fausses; ou
- si les passagers aériens n'ont pas été informés (par écrit) du traitement des données prévu par la présente loi (cf. art. 5).

Est qualifiée de *grave* une violation du devoir de diligence lorsqu'elle est constatée à plusieurs reprises ou que l'ensemble des données d'un vol n'est pas livré. Il y a défaut de livraison lorsque les données transmises se révèlent être majoritairement fausses.

Dans les cas de peu de gravité, les autorités peuvent renoncer à introduire une procédure, par exemple lorsque cette dernière serait disproportionnée.

Il n'y a pas de sanction, malgré une éventuelle contestation, lorsque l'entreprise de transport aérien prouve qu'elle a pris toutes les mesures de précaution raisonnablement exigibles. C'est par exemple le cas si une panne de courant dont elle n'est pas responsable se produit et rend impossible toute transmission des données.

Dans la moitié des cas, les données relatives aux passagers aériens devraient provenir d'un lieu d'embarquement situé à l'étranger. C'est pourquoi l'al. 5 garantit que les violations des obligations survenues à l'étranger puissent également faire l'objet d'une sanction.

Art. 24 Procédure

Si une violation de l'obligation des entreprises de transport aérien de communiquer des données personnelles fait l'objet d'une sanction en vertu de l'art. 122*b* LEI, elle

62 Message du 8 mars 2013 relatif à la modification de la loi fédérale sur les étrangers (violation du devoir de diligence et de l'obligation de communiquer par les entreprises de transport aérien; systèmes d'information), FF **2013** 2305

n'est pas sanctionnée une nouvelle fois en vertu de la LDPa. En revanche, les violations de l'obligation d'informer prévue à l'art. 5 peuvent être sanctionnées indépendamment de la LEI, étant donné que seule la LDPa prévoit une sanction de ces violations, ce qui n'est pas le cas de la LEI.

Annexe 1 Données relatives aux passagers aériens

Le *statut du passager* (ch. 10) comprend les vols déjà effectués et les vols prévus. Les confirmations, l'enregistrement, la non-présentation ou la présentation à la dernière minute sans réservation doivent être indiqués.

On parle de *scission des données* (ch. 11) lorsque des personnes effectuent séparément un voyage réservé conjointement. Dans un tel cas, les données relatives aux passagers aériens concernées ne doivent pas être à nouveau collectées. Les données initialement récoltées sont divisées.

On parle de *partage de code* (ch. 15) lorsqu'une entreprise de transport aérien différente de celle indiquée par le numéro de vol opère ce dernier.

Annexe 2 Catégories d'infractions PNR au sens de l'art. 6, al. 3, let. a

Sont considérées comme *graves* au sens de l'art. 6, al. 3, let. a, de la présente loi uniquement les infractions pénales énumérées à l'annexe 1 LEIS, pour autant qu'elles soient passibles d'une peine privative de liberté de plus de trois ans et qu'elles puissent être attribuées à une catégorie d'infraction PNR visée à l'annexe 2 de la présente loi.

L'annexe 2 compare les catégories d'infractions PNR aux catégories correspondantes de l'annexe 1 LEIS, ce qui permet de comprendre quelles infractions prévues par la LEIS doivent être considérées comme des infractions pénales graves en vertu de l'art. 6, al. 3, let. a.

Annexe 3 Modification d'autres actes

1. Loi fédérale du 20 juin 2003 sur le système d'information commun aux domaines des étrangers et de l'asile[63]

Art. 9, al. 1, let. c[bi]

Comme l'art. 7 de l'avant-projet ne prescrit aucune technologie pour la comparaison automatique des données relatives aux passagers aériens avec celles issues des différents systèmes d'information de la Confédération, l'autorisation d'accès manuel au système SYMIC octroyée à l'UIP doit être prévue.

2. Loi fédérale du 16 décembre 2005 sur les étrangers et l'intégration[64] (LEI)

Art. 109c, let. f, ch. 1

Comme la comparaison automatique des données relatives aux passagers aériens avec celles issues des différents systèmes d'information de la Confédération est régie de

63 RS **142.51**
64 RS **142.20**

manière neutre d'un point de vue technologique à l'art. 7 de l'avant-projet, l'autorisation d'accès manuel au système ORBIS octroyée à l'UIP doit être prévue à l'art. 109*c* LEI.

3. Loi du 17 juin 2005 sur le Tribunal administratif fédéral[65]

Art. 36c

En sa qualité d'instance indépendante, le Tribunal administratif fédéral examine si la pseudonymisation prévue à l'art. 15 LDPa peut être levée. En plus de vérifier si les raisons de la demande sont suffisantes, il pèse les intérêts en matière de sécurité poursuivis par la levée de la pseudonymisation par rapport à ceux de la protection des données.

4. Loi fédérale du 13 juin 2008 sur les systèmes d'information de police de la Confédération[66] (LSIP)

Art. 10, al. 4, let. d

Art. 11, al. 2, let. b

Comme l'art. 7 de l'avant-projet ne prescrit aucune technologie pour la comparaison automatique des données relatives aux passagers aériens avec celles issues des différents systèmes d'information de la Confédération, l'autorisation de comparaison automatique et d'accès manuel au système JANUS octroyée à l'UIP doit être prévue aux art. 10 et 11 LSIP.

Art. 15, al. 6, let. a^{bis}

Comme l'art. 7 de l'avant-projet ne prescrit aucune technologie pour la comparaison automatique des données relatives aux passagers aériens avec celles issues des différents systèmes d'information de la Confédération, l'autorisation de comparaison automatique et d'accès manuel au système RIPOL octroyée à l'UIP doit être prévue à l'art. 15 LSIP.

Art. 17, al. 4, let. m

Comme l'art. 7, al. 3, de l'avant-projet ne prescrit aucune technologie pour l'accès aux différents systèmes d'information de la Confédération, l'autorisation octroyée à l'UIP doit être ajoutée.

5. Loi fédérale du 21 décembre 1948 sur l'aviation[67]

Art. 29, al. 5

Les entreprises de transport aérien ne peuvent plus décoller de Suisse ou y atterrir en toute impunité si elles ont été sommées à plusieurs reprises et sans succès de payer les sanctions prévues à l'art. 23.

Il n'est notamment pas possible de poursuivre une entreprise de transport aérien étrangère si elle ne possède pas de siège social en Suisse et si les conditions préalables à

65 RS **173.32**
66 SR **361**
67 RS **748.0**

une poursuite ne sont pas réunies à un éventuel domicile spécial (art. 50 de la loi fédérale du 11 avril 1889 sur la poursuite pour dettes et la faillite[68]).

Dans ce cas, les conditions préalables au retrait de l'autorisation d'exploitation sont les suivantes:

- une sanction en vertu de l'art. 23 LDPa est entrée en force;
- l'entreprise de transport aérien a été sommée de payer la sanction à plusieurs reprises et sans succès.

Le retrait de l'autorisation d'exploitation doit être appliqué en dernier recours. Toutefois, toutes les autres circonstances indirectement liées aux impayés doivent avoir été prises en considération. Par conséquent, l'obligation légale de retirer l'autorisation d'exploitation est abandonnée.

5 Conséquences

5.1 Conséquences en termes de finances et de personnel pour la Confédération

Compte tenu du développement et de l'exploitation d'un système d'information technique ainsi que de la mise en place et de l'organisation d'une UIP, l'introduction d'un système PNR national est un projet complexe, dont les coûts peuvent être décrits dans trois catégories, à savoir les coûts de projet, les coûts d'exploitation et les coûts en personnel.

Coûts de projet

La conception, le développement et l'introduction d'un système PNR ainsi que la mise en place d'une UIP entraînent des coûts de projet, dont le montant dépend de l'option choisie: possibilité d'utiliser le système PNR de l'ONU *goTravel* (option 1) ou achat et développement en interne d'un système PNR (option 2). Les deux options ont certes une influence sur le financement du projet, mais pas sur le contenu de la loi.

- L'option 1, la solution de l'ONU *goTravel*, est le système PNR actuellement utilisé par l'ONU. Il peut être repris sans modifications majeures et immédiatement utilisé. Différents pays en font déjà l'usage. Cette option est pour l'heure privilégiée par le DFJP. Une preuve de concept est actuellement en cours pour évaluer, en plus des possibilités techniques, quelles exigences du système PNR suisse sont remplies. Les fonctionnalités manquantes pourraient être ajoutées ultérieurement. Les coûts de projet pour cette option s'élèvent à environ 11,6 millions de francs (dont 6,82 millions de francs de dépenses avec incidences financières) pour la période 2020-2025.
- L'option 2, achat et développement d'une solution PNR, couvre sur le plan financier tant l'appel d'offres (OMC) et l'adaptation d'un système existant sur le marché que le développement d'un système propre par la Confédération. Comme l'option 1 est actuellement privilégiée et examinée en détail, c'est uniquement en cas d'abandon de cette dernière qu'il faudrait vérifier de manière approfondie quels systèmes PNR disponibles sur le marché entrent en ligne de compte ou si la Confédération doit mettre elle-même un système

68 RS **281.1**

en place. Les coûts de projet pour cette option s'élèvent à un total d'environ 22,5 millions de francs (dont 16,82 millions de francs de dépenses avec incidences financières) pour la période 2020-2026. Conformément à l'art. 21 de la loi du 7 octobre 2005 sur les finances[69], un crédit d'engagement devrait être demandé.

L'évaluation du système de l'ONU prendra fin en mai 2022, ce qui permettra de constater si ce système peut être intégré à l'environnement informatique de la Confédération. Si l'évaluation est concluante, l'option 1 privilégiée et l'option 2 seront départagées. Dans le cas contraire, l'option 1 sera abandonnée et l'option 2 développée plus concrètement.

Le budget du projet PNR suisse pourra être présenté plus précisément dans le message.

Dans tous les cas, le développement ou l'adaptation du système commencera seulement lorsque l'entrée en vigueur de la base légale sera définitivement arrêtée.

Coûts d'exploitation du système d'information PNR et de l'UIP dès 2025

L'exploitation du système d'information PNR et de l'infrastructure de l'UIP impliquent des coûts, notamment pour le loyer des locaux, la maintenance de la structure TIC (matériel, logiciels, réseaux, etc.), le mobilier, les éventuels appareils techniques nécessaires, les amortissements et les acquisitions de remplacement.

Les coûts concrets de l'infrastructure et de l'exploitation seront calculés au cours du projet.

Coûts en personnel

Les besoins en personnel de l'UIP dépendent de la forme de l'exploitation, des données à analyser et des routes aériennes qui devraient progressivement être prises en compte. Actuellement, l'effectif devrait s'élever à 20 équivalents plein temps (EPT) puis, une fois l'UIP complètement mise en place, à 30 EPT.

5.2 Conséquences pour les cantons

De nombreux éléments constitutifs de l'infraction qui seront combattus grâce aux données PNR relèvent de la compétence des cantons en matière de poursuite pénale. En mettant le système d'information PNR à la disposition de ces derniers, la Confédération fournit les instruments nécessaires afin que les autorités cantonales de poursuite pénale accèdent plus simplement et plus rapidement aux informations qui simplifient la prévention de la grande criminalité et la lutte contre celle-ci.

Les cantons participent aux coûts de l'UIP en détachant des collaborateurs. Ils prennent l'indemnisation de ces derniers à leur charge durant leur engagement au sein de l'UIP.

Les données PNR permettent aux autorités cantonales de poursuite pénale de recevoir des informations sur des personnes recherchées au niveau national ou international qui arrivent en Suisse ou viennent de quitter le pays par voie aérienne. Ainsi, les cantons (ou en coopération avec d'autres autorités) peuvent prendre à temps les mesures

69 RS **611.0**

qui s'imposent. L'UIP répond aussi aux demandes importantes des autorités de poursuite pénale grâce à ses analyses ciblées. De plus, le système PNR épargne aux cantons des requêtes fastidieuses auprès des entreprises de transport aérien lorsqu'il s'agit de suivre les itinéraires empruntés à des fins criminelles. Il pourrait aussi fournir des renseignements utiles sur des infractions non élucidées.

Dans l'ensemble, la LDPa contribue considérablement à renforcer l'efficience et l'efficacité de la poursuite pénale et de la prévention de la criminalité. Les cantons en profitent grandement.

Conséquences financières pour les cantons

Un système PNR suisse ne peut être fonctionnel que si les cantons participent à l'exploitation au niveau de leur personnel. C'est pourquoi il est prévu que la Confédération et les cantons fournissent et financent les collaborateurs à parts égales. Les coûts résiduels (dont les coûts d'investissement et d'exploitation du système d'information PNR et le reste des coûts d'exploitation de l'UIP) sont à la charge de la Confédération. Les autres modalités font l'objet d'une convention entre la Confédération et les cantons. La Conférence des directrices et directeurs des départements cantonaux de justice et police et la Conférence des commandants des polices cantonales de Suisse sont en faveur d'un système PNR national. Leurs membres se montrent prêts à participer à l'UIP avec leur personnel. Une convention en ce sens sera élaborée avec les cantons lors de la phase de conception du projet au début de l'année 2022.

Charge opérationnelle

Les cantons devront également réfléchir dans quelle mesure ils intégreront le traitement des données PNR à leur corps de police et quelles conséquences cette intégration aura sur l'organisation et les ressources. D'une part, ils devront former des spécialistes dans leur corps de police pour transmettre les profils, les listes d'observation et les demandes de recherche concluants à l'UIP et coopérer étroitement avec celle-ci au cas par cas.

D'autre part, la décision et l'exécution de mesures subséquentes résultant de l'analyse de données PNR incombera toujours aux autorités compétentes en la matière.

Étant donné qu'une majorité des premières mesures sont prises à l'arrivée des personnes à l'aéroport, l'utilisation des données relatives aux passagers aériens devrait engendrer une charge de travail plus importante pour les cantons abritant un aéroport international que pour les autres. Il convient de tenir compte de cet aspect.

5.3 Conséquences pour l'économie, la société et l'environnement

La LDPa ne devrait pas engendrer de nouvelles tâches administratives pour les entreprises de transport aérien. En effet, les données relatives aux passagers aériens sont collectées lors de la réservation d'un billet d'avion, et ce indépendamment de la présente loi. De plus, elles sont déjà utilisées par 62 États en raison d'engagements internationaux. La transmission des données PNR n'a donc plus rien de nouveau pour les entreprises de transport aérien.

Le projet a pour objectif principal le renforcement de la sécurité. Une meilleure sécurité dans l'ensemble de la société est une condition importante au maintien et au renforcement de la place économique suisse. Il convient de noter que la transmission de données PNR est de plus en plus une condition préalable aux vols à destination de certains pays. La poursuite de l'inclusion de la Suisse au trafic aérien international revêt d'une grande importance sur le plan économique.

Le terrorisme et la grande criminalité déstabilisent la société et minent la confiance en l'État de droit. Les instruments pouvant être utilisés pour lutter contre ces infractions contribuent considérablement au développement positif de la société.

Les États-Unis, qui ont fait du PNR une condition du maintien de la Suisse dans le VWP, attendent d'elle qu'elle fasse des progrès concrets quant à l'introduction d'un système PNR national. Ce programme permet aux ressortissants de certains États, dont la Suisse, de se rendre et de séjourner aux États-Unis sans visa à des fins professionnelles ou touristiques pendant 90 jours au plus. En cas d'exclusion du VWP, les inconvénients pour la Suisse seraient majeurs: les personnes en voyages d'affaires ne pourraient plus entrer facilement aux États-Unis, ce qui nuirait fortement aux relations commerciales entre les deux pays.

Le traitement de données personnelles effectué indépendamment de tout soupçon représente un changement de paradigme pour la Suisse. Néanmoins, l'intervention dans la sphère privée des passagers aériens se limite principalement à la comparaison des données avec celles issues des systèmes d'information de police, conformément à l'art. 7, al. 1. L'objectif des données PNR, c'est-à-dire le renforcement de la sécurité de l'ensemble de la société, justifie cette pratique.

6 Aspects juridiques

6.1 Constitutionnalité

La LDPa décrit les contours d'une nouvelle tâche ayant trait tant à la politique de sécurité qu'au trafic aérien.

En tant que nouvelle tâche de la Confédération, le traitement de données relatives aux passagers aériens est motivé principalement par la politique de sécurité. La sauvegarde de la sécurité intérieure, tâche commune de la Confédération et des cantons (art. 57, al. 1, Cst.), est une priorité. La LDPa constitue la base légale de l'exploitation d'un système d'information central fournissant des informations importantes qui soutiennent les autorités compétentes de la Confédération et des cantons dans l'accomplissement de leurs tâches de sécurité. La répartition des tâches entre ces autorités n'est pas affectée à cet égard. La constitutionnalité de la LDPa peut aussi être clairement affirmée de ce point de vue-là.

Enfin, la LDPa présente un lien étroit avec le trafic aérien, puisque les entreprises de transport aérien sont obligées de transmettre des données et doivent s'attendre à des sanctions en cas de violation éventuelle. L'art. 87 Cst. attribue à la Confédération la compétence exclusive de légiférer en matière de transport aérien.

6.2 Compatibilité avec les obligations internationales de la Suisse

En mettant en place l'UIP et la réglementation du traitement des données relatives aux passagers aériens, la Suisse, en sa qualité de membre de l'ONU, met en œuvre les

résolutions contraignantes du Conseil de sécurité en la matière. En même temps, elle met en application les normes de l'OACI que doit respecter l'aviation suisse et s'assure de rester dans le VWP des États-Unis. Ce statut important n'est que provisoire pour l'instant.

L'avant-projet de LDPa s'appuie largement sur la directive PNR de l'UE, ce qui devrait être propice à la conclusion d'un accord en la matière avec l'UE. L'accord du 21 juin 1999 entre la Confédération suisse et la Communauté européenne sur le transport aérien[70] n'est pas concerné.

6.3 Forme de l'acte

Le présent projet de loi fédérale règle le traitement des données relatives aux passagers aériens, qui comprennent aussi des données personnelles. La comparaison automatique des données relatives aux passagers aériens avec celles contenues dans les différents systèmes d'information de la Confédération peut donner lieu au traitement ultérieur de données sensibles.

Ce traitement peut porter atteinte au droit constitutionnel à la protection de la sphère privée des passagers aériens et n'est autorisé que sur la base d'une loi formelle (art. 164, al. 1, let. b, Cst.).

La nécessité de disposer d'une loi fédérale est aussi justifiée par la nouvelle tâche incombant à la Confédération de par la mise en œuvre de la LDPa (art. 164, al. 1, let. e, Cst.).

6.4 Conformité aux principes de subsidiarité et d'équivalence fiscale

Le principe de subsidiarité veut que la collectivité supérieure d'un État fédéral ne se charge d'une tâche en tout ou en partie que si elle est manifestement mieux à même de l'accomplir que les collectivités subordonnées (art. 5*a* Cst.). Il exige implicitement que l'accomplissement des tâches se fasse au plus près des citoyens, qui sont ainsi mieux à même d'influer sur le processus politique.

Dans le cas présent, il n'est guère pertinent que les cantons soient les premiers à s'organiser en vue du traitement commun des données relatives aux passagers aériens. La Confédération se conforme à trois résolutions contraignantes de l'ONU au moyen de cette loi en mettant sur pied et en exploitant un système d'information central voué à ce traitement. Ce système d'information est notamment au service des autorités de poursuite pénale de la Confédération et des cantons, auxquelles sont envoyées spontanément ou sur demande de précieuses informations destinées à leurs tâches respectives. La proximité avec la population est peu indiquée pour ce type de tâches. Ce qu'il faut, c'est une solution uniforme, qui constitue une raison supplémentaire pour que la compétence échoie à la Confédération (cf. art. 43*a*, al. 1, Cst.).

Le principe de l'équivalence fiscale, quant à lui, veut que la collectivité publique prenne en charge les coûts de toute prestation de l'État dont elle bénéficie (art. 43*a*, al. 2, Cst.).

Le traitement des données relatives aux passagers aériens a une utilité tant par sa portée nationale que d'un point de vue concret pour les autorités fédérales et cantonales.

70 RS **0.748.127.192.68**

Une facturation spécifique aux différents cantons occasionnerait des dépenses considérables, d'où la force probante de la solution pragmatique, selon laquelle les cantons fournissent à leurs frais la moitié des collaborateurs chargés de traiter les données relatives aux passagers aériens.

6.5 Délégation de compétences législatives

L'*art. 2, al. 4*, confère à fedpol la compétence de préciser au besoin par voie d'ordonnance les normes industrielles internationales de l'OACI, de l'OMD et de l'IATA.

L'*art. 6, al. 4*, de l'avant-projet prévoit que le Conseil fédéral précise par voie d'ordonnance les infractions pénales graves mentionnées à l'art. 6, al. 3, let. b. Comme exposé dans les explications relatives à cette disposition, il ne s'agit pas ici d'une délégation de compétences législatives. L'infraction pénale grave est déjà définie clairement à l'art. 6, al. 3, let. b. Les éléments constitutifs de l'infraction sont précisés par voie d'ordonnance uniquement pour des raisons de transparence et de sécurité du droit.

L'*art. 9, al. 6*, dispose que le Conseil fédéral détermine aussi par voie d'ordonnance les éléments constitutifs de l'infraction déterminants qui autorisent le traitement ultérieur de données relatives aux passagers aériens après que la comparaison avec des listes d'observation a donné une concordance. L'accent est mis sur les infractions terroristes et celles liées au crime organisé.

Conformément à l'*art 16, al. 2,* le Conseil fédéral fixe dans une ordonnance la durée de conservation maximale des données résultant d'une comparaison. À la différence des données relatives aux passagers aériens (art. 16, al. 1), il y a lieu de ne pas limiter la durée de conservation des concordances résultant d'une comparaison avec les données issues des systèmes d'information de police ou avec des profils de risque et des listes d'observation. Dans le cas contraire, des données risqueraient, selon la situation, de devoir être effacées avant même la clôture d'une procédure. Leur disponibilité doit pouvoir être garantie pendant une procédure en cours. La fixation de la durée de conservation par voie d'ordonnance crée la marge de manœuvre nécessaire.

La Constitution fédérale ne prévoit pas que les conventions fixant des règles de droit conclues entre la Confédération et les cantons soient une forme d'acte législatif à part entière (cf. art. 163 Cst.). Par conséquent, il faut fixer au moins le cadre de la convention, autrement dit ses grandes lignes, dans une loi au sens formel, ou dans une ordonnance pour ce qui est des dispositions d'une importance mineure. Ce n'est qu'en vertu de cette base juridique qu'une convention peut être conclue avec les cantons[71]. C'est pourquoi l'*art. 20, al. 5* prévoit la possibilité que le Conseil fédéral fixe dans une ordonnance les conditions-cadres régissant une convention avec les cantons sur le détachement de collaborateurs et leur engagement au sein de l'UIP.

L'*art. 21, al. 1*, octroie au Conseil fédéral la compétence de conclure seul des traités internationaux sur le traitement des données relatives aux passagers aériens, mais seulement avec des États dont le droit interne garantit une protection des données comparable à celle de la Suisse. fedpol peut conclure des conventions portant sur des aspects opérationnels, techniques ou administratifs qui complètent ces traités (art. 21, al. 2).

71 Bernhard Waldmann/Zeno Schnyder von Wartensee, in Commentaire bâlois de la Constitution fédérale, n° 37 ad art. 48

6.6 Protection des données

La LDPa s'inscrit dans le droit fil de la LPD, qui devrait entrer en vigueur en 2023. Dans son message du 15 septembre 2017[72], le Conseil fédéral explique que la LPD visait notamment à renforcer les dispositions légales de protection des données pour faire face au développement fulgurant des nouvelles technologies. La LDPa illustre cette adaptation du droit fédéral en matière de protection de données, ce qui est d'autant plus important que cette protection joue un rôle central dans le traitement des données au sens de la LDPa.

L'ensemble de données relatives aux passagers aériens comprend différentes catégories. Celles qui relèvent de la protection des données sont avant tout les données personnelles. Il s'agit de toutes les informations concernant une personne physique identifiée ou identifiable (art. 5, let. a, LPD). En font partie le nom, le numéro de téléphone, l'adresse de domicile et l'adresse électronique. Après comparaison avec les données des différents systèmes d'information de la Confédération (cf. art. 7, al. 1), des données sensibles peuvent s'y ajouter. La LDPa dispose que celles-ci ne peuvent être traitées que s'il s'agit de données biométriques ou éventuellement de données sur les poursuites ou sanctions pénales et administratives. Toutes les autres données sensibles qui seraient éventuellement obtenues lors du traitement de données relatives aux passagers aériens au sens de la présente loi doivent être immédiatement effacées (art. 6, al. 5).

Les données relatives aux passagers aériens ne peuvent être traitées que dans le but prévu par la loi (art. 6, al. 4, LPD). Les données relatives aux passagers aériens ne peuvent être traitées au titre de la LDPa que si elles servent à la lutte contre les infractions terroristes et autres infractions pénales graves (art. 6, al. 1). Les résultats qui ne remplissent pas ce but doivent être effacés immédiatement (art. 6, al. 5).

Si des données personnelles sont traitées, il y a lieu de s'assurer qu'elles sont exactes (art. 6, al. 5, LPD). L'UIP a l'obligation de vérifier manuellement chacune des concordances obtenues par une comparaison des données relatives aux passagers aériens avec celles des systèmes d'information de la Confédération et d'établir leur plausibilité (art. 7, al. 3).

Les données relatives aux passagers aériens sont comparées avec celles des systèmes d'information de la Confédération en deux étapes (art. 7, al 1 et 3). D'abord, toutes les données disponibles sont comparées. Ensuite, seules celles qui correspondent à des données contenues dans les systèmes d'information et qui justifient donc de premiers soupçons font l'objet d'un traitement complémentaire. Leur plausibilité est vérifiée manuellement et, le cas échéant, par un accès spécifique à des systèmes d'information supplémentaires de la Confédération. Cette seconde étape du traitement vise prioritairement à garantir l'exactitude de la concordance et sa conformité au but légal du traitement. Les concordances ne présentant pas de lien avec des infractions terroristes ou d'autres infractions pénales graves au sens de l'art. 6, al. 2 et 3, doivent être effacées

72 FF **2017** 6565

immédiatement. Cette manière de procéder en deux temps contribue à ce que les données relatives aux passagers aériens ne soient traitées que dans la mesure nécessaire au but visé par la présente loi et à l'exactitude des données.

La sécurité des données relatives aux passagers aériens est accrue six mois après leur enregistrement dans le système d'information PNR par la pseudonymisation (art. 14). Le message sur la révision totale de la loi fédérale sur la protection des données qualifie la pseudonymisation de mesure technique appropriée pour garantir la sécurité des données (art. 8 LPD)[73]. Dans ledit message, le Conseil fédéral déclare en outre que la LPD "ne s"applique pas aux données qui ont été anonymisées si une ré-identification par un tiers est impossible (les données ont été anonymisées complètement et définitivement) ou ne paraît possible qu'au prix d'efforts tels qu'aucun intéressé ne s'y attèlera. Cette dernière règle vaut aussi pour les données pseudonymisées."[74]

73 FF **2017** 6650
74 FF **2017** 6640

Annexe 1

A. Infractions terroristes au sens de l'art. 6, al. 2

Infractions terroristes au sens des art. 1 à 4 de la décision-cadre 2002/475/JAI	**Applicables en cas de motivation terroriste:** Menaces alarmant la population, provocation publique au crime ou à la violence, émeute, actes préparatoires délictueux, organisations criminelles et terroristes, mise en danger de la sécurité publique au moyen d'armes, financement du terrorisme, recrutement, formation et voyage en vue d'un acte terroriste, groupements illicites (art. 258, 259, 260, al. 1, 260bis, 260ter, 260^{quater}, 260^{quinquies}, 260^{sexies} et 275ter CP) Interdiction d'organisations (art. 74 LRens[75]) Dispositions pénales conformément à la loi fédérale du 12 décembre 2014 interdisant les groupes « Al-Qaïda » et « État islamique » et les organisations apparentées[76] (art. 2)

B. Infractions pénales graves au sens de l'art. 6, al. 3, let. a

Annexe II de la directive PNR de l'UE	**Infractions selon le droit suisse[77]**
Participation à une organisation criminelle	Organisations criminelles et terroristes (art. 260ter)
Traite d'êtres humains	Mariage forcé, partenariat forcé, traite d'êtres humains (art. 181*a* et 182, al. 1, 2 et 4, CP)
Exploitation sexuelle des enfants et pédopornographie	Mise en danger du développement de mineurs: actes d'ordre sexuel avec des enfants, encouragement à la prostitution, pornographie (art. 187, ch. 1, 195, let. a, et 197, al. 4, CP)
Trafic de stupéfiants et de substances psychotropes	Dispositions pénales de la loi du 3 octobre 1951 sur les stupéfiants[78] (art. 19, al. 2, et 20, al. 2)

75 RS **121**
76 RS **122**
77 Infractions au sens de l'annexe 1 de la loi du 12 juin 2009 sur l'échange d'informations Schengen (RS **362.2**) qui sont passibles d'une peine privative de liberté de plus de trois ans
78 RS **812.121**

Annexe II de la directive PNR de l'UE	Infractions selon le droit suisse[77]
Trafic d'armes, de munitions et d'explosifs	Mise en danger de la sécurité publique au moyen d'armes (art. 260quater CP)
	Délits et crimes au sens de la loi du 20 juin 1997 sur les armes[79] (art. 33, al. 3)
Corruption	Corruption active, corruption passive, corruption d'agents publics étrangers (art. 322ter, 322quater et 322septies CP)
Fraude	Escroquerie, utilisation frauduleuse d'un ordinateur, abus de cartes-chèques et de cartes de crédit, falsification de marchandises, banqueroute frauduleuse et fraude dans la saisie (art. 146, al. 1 et 2, 147, al. 1 et 2, 148, 155, ch. 2, et 163, ch. 1, CP)
	Escroquerie en matière de prestations et de contributions (art. 14, al. 4, de la loi fédérale du 22 mars 1974 sur le droit pénal administratif [DPA])[80])
Blanchiment du produit du crime et faux monnayage	Fabrication de fausse monnaie, falsification de la monnaie, importation, acquisition et prise en dépôt de fausse monnaie, blanchiment d'argent (art. 240, al. 1, 241, al. 1, 244, al. 2, et 305bis, ch. 2, CP)
Cybercriminalité	Soustraction de données, détérioration de données, utilisation frauduleuse d'un ordinateur (art. 143, 144bis, al. 3, et 147, al. 1 et 2, CP)
Infractions graves contre l'environnement, y compris le trafic d'espèces animales menacées et le trafic d'espèces et d'essences végétales menacées	Exposition injustifiée de tiers à l'irradiation (art. 43, al. 2, de la loi du 22 mars 1991 sur la radioprotection[81])
Aide à l'entrée et au séjour irréguliers	Incitation à l'entrée, à la sortie ou au séjour illégaux (art. 116, al. 1, let. a, abis et c, en relation avec l'al. 3 de la loi fédérale du 16 décembre 2005 sur les étrangers et l'intégration[82])
Meurtre, coups et blessures graves	Meurtre, assassinat, meurtre passionnel, lésions corporelles graves, mutilation d'organes génitaux féminins (art. 111, 112, 113, 122 et 124 CP)

79 RS **514.54**
80 RS **313.0**
81 RS **814.50**
82 RS **142.20**

Annexe II de la directive PNR de l'UE	Infractions selon le droit suisse[77]
Trafic d'organes et de tissus humains	Crime au sens de la loi du 8 octobre 2004 sur la transplantation[83] (art. 69, al. 2) Crime au sens de la loi du 19 décembre 2003 relative à la recherche sur les cellules souches[84] (art. 24, al. 3)
Enlèvement, séquestration et prise d'otage	Extorsion et chantage, séquestration et enlèvement, circonstances aggravantes d'une séquestration et d'un enlèvement, prise d'otage, actes exécutés sans droit pour un État étranger (art. 156, 183, 184, 185, et 271, ch. 2 et 3, CP)
Vol organisé ou vol à main armée	Vol, brigandage (art. 139, ch. 3, et 140 CP)
Trafic de biens culturels, y compris d'antiquités et d'œuvres d'art	---
Contrefaçon et piratage de produits	Falsification de marchandises (art. 155, ch. 2, CP) Violation du droit à la marque, usage frauduleux, usage d'une marque de garantie ou d'une marque collective contraire au règlement, usage d'indications de provenance inexactes (art. 61, al. 3, 62, al. 2, 63, al. 4, et 64, al. 2, de la loi du 28 août 1992 sur la protection des marques[85]) Violation du droit sur un design (art. 41, al. 2, de la loi du 5 octobre 2001 sur les designs[86]) Violation du droit d'auteur, violation de droits voisins (art. 67, al. 2, et 69, al. 2, de la loi du 9 octobre 1992 sur le droit d'auteur[87]) Violation du brevet (art. 81, al. 3, de la loi du 25 juin 1954 sur les brevets[88])
Falsification de documents administratifs et trafic de faux	Falsification des poids et mesures, monnaies et timbres de valeur étrangers, faux dans les titres, obtention frauduleuse d'une constatation fausse, titres étrangers, faux dans les

83 RS **810.21**
84 RS **810.31**
85 RS **232.11**
86 RS **232.12**
87 RS **231.1**
88 RS **232.14**

Annexe II de la directive PNR de l'UE	Infractions selon le droit suisse[77]
	titres commis dans l'exercice de fonctions publiques (art. 248, 250, 251, ch. 1, 253, 255 et 317, ch. 1, CP)
Trafic de substances hormonales et d'autres facteurs de croissance	Disposition pénale au sens de la loi du 17 juin 2011 sur l'encouragement du sport[89] (art. 22, al. 2)
	Crime au sens de la loi du 15 décembre 2000 sur les produits thérapeutiques[90] (art. 86, al. 2 et 3, LPTh)
Trafic de matières nucléaires et radioactives	Danger imputable à l'énergie nucléaire, à la radioactivité et aux rayonnements ionisants, actes préparatoires punissables (art. 226bis et 226ter CP)
	Infractions aux mesures de sécurité et de sûreté, infractions relatives à des articles nucléaires ou à des déchets radioactifs (art. 88, al. 2, et 89, al. 2, de la loi du 21 mars 2003 sur l'énergie nucléaire[91])
Viol	Viol (art. 190 CP)
Infractions graves relevant de la Cour pénale internationale	Génocide, crimes contre l'humanité, infractions graves aux conventions de Genève, attaque contre des civils ou des biens de caractère civil, traitement médical immotivé, atteinte au droit à l'autodétermination sexuelle ou à la dignité de la personne, recrutement ou utilisation d'enfants soldats, méthodes de guerre prohibées, utilisation d'armes prohibées (art. 264, 264*a* et 264*c* à *h* CP)
Détournement d'avion / de navire	Extorsion et chantage, séquestration et enlèvement, prise d'otage (art. 156, 183 et 185 CP)
Sabotage	Dommages à la propriété, incendie intentionnel, explosion, emploi, avec dessein délictueux, d'explosifs ou de gaz toxiques, fabriquer, dissimuler et transporter des explosifs ou des gaz toxiques, inondation, écroulement, dommages aux installations électriques, travaux hydrauliques et ouvrages de protection (art. 144, al. 3, 221, al. 1 et 2, 223, ch. 1, 224, al. 1, 226, 227, ch. 1, et 228, ch. 1, CP)

89 RS **415.0**
90 RS **812.21**
91 RS **732.1**

Annexe II de la directive PNR de l'UE	Infractions selon le droit suisse[77]
Trafic de véhicules volés	Recel (art. 160 CP)
Espionnage industriel	--

C. Infractions pénales graves au sens de l'art. 6, al. 3, let. a

Infractions relevant de la compétence de l'Office fédéral de la douane et de la sécurité des frontières (OFDF) en matière de poursuite pénale et qui sont passibles d'une peine privative de liberté d'au moins trois ans

1. Escroquerie en matière de prestations et de contributions, faux dans les titres, obtention frauduleuse d'une constatation fausse, suppression de titres, entrave à l'action pénale (art. 14, al. 4, 15, 16, al. 1, et 17, ch. 1, de la loi fédérale du 22 mars 1974 sur le droit pénal administratif[92]);
2. les infractions suivantes, pour autant qu'elles relèvent de la compétence de l'OFDF en matière de poursuite pénale et soient liées à une infraction préalable passible d'une peine privative de liberté de trois ans au moins:
   art. 37 de la loi fédérale du 21 juin 1996 sur l'imposition des véhicules automobiles[93]; art. 39 de la loi du 21 juin 1996 sur l'imposition des huiles minérales (Limpmin)[94];
3. les infractions supplémentaires suivantes:

   art. 36, al. 2, en relation avec l'art. 40 LAlc;

   art. 38, al. 2, en relation avec l'art. 42 Limpmin;

   art. 86, al. 1 à 3, en relation avec l'art. 90, al. 1, LPTh;

   art. 26, al. 2, en relation avec l'art. 27 de la loi du 16 mars 2012 sur les espèces protégées[95];

   art. 63, al. 1 et 2, en relation avec l'art. 65 de la loi du 20 juin 2014 sur les denrées alimentaires[96];

   art. 26, al. 1, en relation avec l'art. 31, al. 3, de la loi fédérale du 16 décembre 2005 sur la protection des animaux[97].

92 RS **313.0**
93 RS **641.51**
94 RS **641.61**
95 RS **453**
96 RS **817.0**
97 RS **455**

Glossaire

Données API	Données que les entreprises de transport aérien doivent transmettre à un État avant le départ de certains vols (API: *advance passenger information*). En Suisse, les données API sont régies par les art. 104 et 104*a* de la loi fédérale du 16 décembre 2005 sur les étrangers et l'intégration (RS *142.20*). *Pertinence eu égard aux données relatives aux passagers aériens: les données API sont une catégorie de l'ensemble de données PNR.*
Traitement de données	Toute opération relative à des données personnelles, quels que soient les moyens et procédés utilisés, notamment la collecte, l'enregistrement, la conservation, l'utilisation, la modification, la communication, l'archivage, l'effacement ou la destruction. *Pertinence eu égard aux données relatives aux passagers aériens: la LDPa prévoit le traitement de données pour la lutte contre les infractions terroristes et autres infractions pénales graves et règle leur protection, en complément à la loi sur la protection des données.*
Données sensibles	→ Données personnelles qui ne peuvent être traitées qu'à certains conditions. Sont considérées comme des données sensibles: 1. les données sur les opinions ou les activités religieuses, philosophiques, politiques ou syndicales; 2. les données sur la santé, la sphère intime ou l'origine raciale ou ethnique; 3. les données génétiques; 4. les → données biométriques; 5. les données sur des poursuites ou sanctions pénales et administratives; 6. les données sur des mesures d'aide sociale.

	Pertinence eu égard aux données relatives aux passagers aériens: on peut être en présence de données sensibles lorsque l'on compare les données relatives aux passagers aériens avec celles des systèmes d'information de la Confédération ou que l'on tente d'établir leur plausibilité en accédant à ces systèmes. L'avant-projet de LDPa n'autorise toutefois leur traitement que s'il s'agit de → données biométriques ou de données sur des poursuites ou sanctions pénales et administratives (cf. art. 9, al. 4). Toutes les autres données sensibles doivent être effacées immédiatement.
Données biométriques	Données personnelles obtenues sur les caractéristiques physiques, physiologiques ou comportementales d'un individu par un procédé technique spécifique et qui permettent ou confirment son identification univoque. Il s'agit par exemple d'une empreinte digitale numérique, d'images faciales, d'images de l'iris ou d'enregistrements vocaux. Les données biométriques sont considérées comme des → données sensibles et ne peuvent être traitées qu'à certaines conditions. *Pertinence eu égard aux données relatives aux passagers aériens: le traitement de données relatives aux passagers aériens peut produire des données biométriques en cas de comparaison avec les données issues des systèmes d'information ou d'accès à ces systèmes. Le service compétent est autorisé à les traiter dans le but défini par la loi.*
Ensemble de données	Groupe de données logiques, cohérentes et consécutives de longueur fixe ou variable. *Pertinence eu égard aux données relatives aux passagers aériens: l'ensemble de données relatives aux passagers aériens comprend 19 catégories de données collectées lors de la réservation de billets d'avion. En règle générale, à chaque passager aérien*

	correspond un ensemble de données. De plus en plus d'États utilisent ces ensembles de données pour lutter contre le terrorisme et les autres infractions pénales graves. La Suisse prévoit de les traiter dans l'avant-projet de LDPa, qui a été mis en consultation au cours du premier semestre de 2022.
Dépersonnaliser	Synonyme de → pseudonymiser. *Pertinence eu égard aux données relatives aux passagers aériens: tant la directive PNR de l'UE que les lois ad hoc de l'Allemagne et de l'Autriche utilisent la notion de dépersonnalisation.*
Pseudonymiser	Munir d'un pseudonyme des données de sorte qu'elles ne puissent plus être attribuées à une personne spécifique. La pseudonymisation peut être annulée si un service autorisé à cet effet remplace le pseudonyme par le nom associé à la personne d'origine. Dès lors, les données sont de nouveau attribuables à cette personne. C'est la table de concordance qui indique quel pseudonyme correspond à quel nom. Les données pseudonymisées sont toujours considérées comme des données personnelles au sens de la protection des données, pour autant que la table de concordance soit encore disponible. *Pertinence eu égard aux données relatives aux passagers aériens: les données relatives aux passagers aériens traitées en Suisse selon la LDPa sont pseudonymisées automatiquement au bout de six mois. Le Tribunal administratif fédéral statue sur une éventuelle levée de la pseudonymisation.*
Données personnelles	Toutes les indications relatives à une personne physique identifiée ou identifiable. Une personne physique est identifiable si elle peut être reconnue directement ou indirectement, par exemple à l'aide d'informations qui peuvent être déduites des circonstances ou du contexte (numéro d'identification, données de localisation,

	spécificités concernant son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale). L'identification peut être possible grâce à une seule information (numéro de téléphone, numéro de maison, numéro AVS, empreintes digitales) ou par la comparaison de différentes informations (adresse, date de naissance, état civil). La possibilité purement théorique qu'une personne soit identifiée ne suffit pas pour supposer qu'elle soit identifiable. Les données personnelles comprennent aussi les → données sensibles, pour lesquelles le droit de la protection des données prescrit une protection accrue. *Pertinence eu égard aux données relatives aux passagers aériens: l'ensemble de données relatives aux passagers aériens que les entreprises de transport aérien doivent transmettre à l'UIP comprend aussi des données personnelles, qui ne sont toutefois pas sensibles. Si des données sensibles devaient être transmises, l'UIP a l'obligation légale de les effacer.*
Visa Waiver Program (VWP)	Programme d'exemption de visa permettant aux ressortissants de certains pays de se rendre aux États-Unis à des fins professionnelles ou touristiques (objet du voyage: visite) si la durée de leur séjour n'excède pas 90 jours. *Pertinence eu égard aux données relatives aux passagers aériens: la Suisse doit introduire les données PNR pour que les États-Unis la maintiennent dans le programme d'exemption de visa.*