23.xxx

Message
relatif à loi sur les données relatives aux passagers aériens

du …

Madame la Présidente,
Monsieur le Président,
Mesdames, Messieurs,

Par le présent message, nous vous soumettons le projet de loi sur les données relatives aux passagers aériens, en vous proposant de l'adopter.

Nous vous prions d'agréer, Madame la Présidente, Monsieur le Président, Mesdames, Messieurs, l'assurance de notre haute considération.

…

Au nom du Conseil fédéral suisse:

La présidente de la Confédération, Viola Amherd
Le chancelier de la Confédération, Viktor Rossi

Condensé

Le présent projet de loi vise à autoriser la Suisse, comme de nombreux autres États, à traiter systématiquement les données relatives aux passagers aériens pour que les autorités fédérales et cantonales puissent plus facilement lutter contre la grande criminalité.

Contexte

Au cours des dernières décennies, le trafic de passagers aériens a fortement augmenté partout dans le monde, ce qui représente un défi non seulement pour l'infrastructure des aéroports, mais aussi pour les autorités chargées des contrôles à l'entrée et à la sortie du pays. Après le coup d'arrêt aux voyages pendant la pandémie de COVID-19, des données provisoires de l'Office fédéral de l'aviation civile (OFAC) font à nouveau état en 2023 de plus de 53 millions de passagers qui sont entrés en Suisse ou ont quitté notre pays sur des vols de ligne et charters.

Malgré ce nombre élevé d'entrées et de sorties, il doit rester possible d'identifier les personnes qui se servent du trafic aérien pour poursuivre des objectifs criminels, notamment lorsqu'il s'agit de grande criminalité, dont font partie les infractions terroristes et les autres infractions pénales graves.

Le terrorisme et la grande criminalité sont principalement de nature transnationale.

Par conséquent, 69 États utilisent aujourd'hui déjà les informations relatives aux passagers aériens comme instrument pour lutter contre la grande criminalité.

Les entreprises de transport aérien collectent au moment de la réservation d'un billet d'avion des données relatives aux passagers aériens, 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), se compose de 19 catégories de données et comprend par exemple le nom et l'adresse des passagers, mais aussi d'autres informations relatives à leurs bagages ou aux modes de paiement.*

Le traitement des données relatives aux passagers aériens permet non seulement de mener des enquêtes sur des personnes déjà connues des autorités de poursuite pénale, mais aussi d'en identifier d'autres jusqu'alors inconnues et présentant un lien avec la grande criminalité. Par exemple, on constate que certaines combinaisons de données apparaissent fréquemment en lien avec la traite d'êtres humains ou le trafic de stupéfiants.

Actuellement, l'utilisation du PNR progresse partout dans le monde. Trois résolutions du Conseil de sécurité de l'ONU, également contraignantes pour la Suisse, enjoignent à la communauté internationale de traiter les données relatives aux passagers aériens pour prévenir le terrorisme.

Par sa directive (UE) 2016/681 (ci-après directive PNR), l'Union européenne (UE) a contraint ses États membres à mettre en place un système PNR national.

La directive PNR de l'UE 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 communiquer les données PNR de leurs passagers.

Aujourd'hui, les données PNR des vols de la Suisse sont communiquées aux États membres de l'UE, au Royaume-Uni, à la Norvège et aux États-Unis. La Suisse ne peut cependant pas systématiquement les traiter elle-même tant qu'elle ne dispose pas de la base légale requise et d'un système PNR national.

Sans ce système PNR, la Suisse ne dispose pas – par rapport à d'autres États Schengen – d'informations cruciales sur certaines personnes qui entrent en Suisse et donc dans l'espace Schengen, afin d'assurer la sécurité publique.

Par ailleurs, de plus en plus d'États menacent d'infliger de lourdes amendes aux entreprises de transport aérien suisses qui ne communiquent pas de données PNR voire de leur retirer leurs droits d'atterrissage, ce qui aurait des conséquences économiques fatales pour la Suisse.

*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 constitue la base légale qui autorise la Confédération à traiter les données relatives aux passagers aériens. Le PNR permettra à la Suisse de disposer, avant qu'un passager entre ou sorte du pays par voie aérienne, d'informations indiquant si ce dernier est potentiellement dangereux ou est recherché. Sur la base de ces informations, les autorités compétentes, notamment les autorités de police et de poursuite pénale, décideront si un passager aérien doit faire l'objet d'un examen approfondi, voire être arrêté.

Un nouveau service, rattaché à l'Office fédéral de la police (fedpol) et désigné sous le nom de Passenger Information Unit *(PIU, en français "unité d'information passagers" ou UIP), traitera les données relatives aux passagers aériens à l'intention des autorités compétentes. 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 à destination ou en provenance de la Suisse et une deuxième fois juste avant celui-ci. Directement après leur enregistrement, ces données sont automatiquement comparées avec celles issues des systèmes d'information de police ainsi qu'avec des profils de risque et des listes d'observation.

L'UIP communique les concordances ainsi obtenues aux autorités compétentes de la Confédération et des cantons après les avoir vérifiées manuellement, de sorte que ces dernières puissent prendre à temps les mesures nécessaires. Les catégories d'infractions figurant en annexe à la loi sur les données relatives aux passagers aériens permettent de déterminer les éléments constitutifs de l'infraction justifiant une communication des données relatives aux passagers aériens à une autorité.

Conformément aux résultats de la consultation, le projet de loi sur les données relatives aux passagers aériens tient compte de plusieurs éléments clés établis par l'arrêt de la Cour de justice de l'Union européenne (CJUE), notamment une durée de conservation réduite pour les données relatives aux passagers aériens ne présentant aucun indice de grande criminalité et le retrait de certaines catégories d'infractions.

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 aussi aux cantons.

Exemples de l'utilité des données PNR dans la lutte contre le terrorisme et la grande criminalité

Exemple 1: empêcher l'entrée sur le territoire en cas de soupçon de terrorisme

Madame X réserve sur Internet un vol au départ d'une ville canadienne à destination de la Suisse. Elle saisit alors les informations demandées lors de la réservation, notamment son nom, ses coordonnées et sa date de naissance.

La compagnie aérienne transmet ces informations à l'unité d'information passagers (UIP) du pays de départ et du pays de destination 48 à 24 heures avant le vol.

Les UIP comparent automatiquement ces données avec les systèmes d'information de police auxquels elles ont accès. Lors de la comparaison, l'UIP suisse trouve une concordance. Les spécialistes de l'UIP vérifient alors manuellement la concordance pour confirmer le résultat de la comparaison. Résultat : Madame X est signalée dans le Système d'Information Schengen (SIS) pour soutien et appartenance à une organisation terroriste.

L'UIP transmet ensuite la concordance à l'autorité compétente (en général, une police cantonale ou fedpol) en Suisse. L'autorité suisse compétente envoie immédiatement une demande aux autorités du pays de départ : elles doivent empêcher Madame X de prendre le vol vers la Suisse.

Le jour suivant, Mme X se rend à l'aéroport pour prendre son vol. Comme elle n'a pas de bagages, elle se rend directement à la porte d'embarquement. Alors qu'elle s'apprête à embarquer, Mme X est arrêtée.

Les données PNR permettent d'identifier des personnes dans les systèmes d'information de police avant le départ du vol et de renforcer la coopération policière internationale.

Exemple 2: prévention de la traite d'êtres humains à des fins d'exploitation sexuelle

Une police cantonale sait, dans le cadre d'une enquête en cours contre un trafiquant d'êtres humains, que des jeunes femmes atterrissent régulièrement à Zurich en provenance d'une ville d'Europe de l'Est à des fins d'exploitation sexuelle. Elles sont accompagnées par une personne encore inconnue. Par ailleurs, la police cantonale sait que les billets d'avion pour les jeunes femmes sont toujours réservés par le biais de la même agence de voyage et payés avec la même carte de crédit. Le soupçon : l'accompagnateur inconnu est un trafiquant d'êtres humains et achète les billets pour les jeunes femmes et pour lui-même auprès de la même agence de voyage et avec la même carte de crédit.

La police cantonale contacte alors l' UIP et demande que les données connues de l'accompagnant – numéro de carte de crédit et agence de voyage –soient placées sur une liste d'observation. L'UIP examine la demande et compare désormais les données des passagers qui volent de cette ville d'Europe de l'Est à destination de Zurich avec la liste d'observation.

Quelques semaines plus tard, l'UIP constate une concordance avec la liste d'observation pour un passager – un hit. L'UIP vérifie manuellement le hit et transmet ensuite l'information à la police cantonale. La police cantonale prend alors la décision : l'homme encore inconnu est arrêté et interrogé à son entrée. Cet interrogatoire et d'autres enquêtes renforcent le soupçon qu'il est un trafiquant d'êtres humains.

La police cantonale soumet alors une demande à l'UIP pour vérifier si l'homme a voyagé au cours des six derniers mois avec d'autres jeunes femmes sur le même trajet. Le délégué à la protection des données de l'UIP examine si la demande remplit les conditions juridiques nécessaires et la transmet ensuite au Tribunal administratif fédéral. Ce dernier décide qu'il est possible d'accéder aux données des vols concernés des derniers six mois pour procéder à la vérification.

L'UIP procède aux interrogations individuelles : il apparaît que l'homme a emprunté à maintes reprises cette liaison aérienne avec d'autres victimes potentielles au cours des six derniers mois.

Grâce à ces informations supplémentaires, la police cantonale peut mener des investigations ciblées et réussit à identifier d'autres victimes et à les libérer du réseau de traite d'êtres humains.

Grâce, entre autres, à l'utilisation des données PNR, il est possible de prévenir les cas de traite d'êtres humains, les élucider et protéger les victimes.

Table des matières

Message

1 Contexte

1.1 Aperçu

Toute personne réservant un vol met à la disposition de l'entreprise de transport aérien, directement ou indirectement par l'intermédiaire de 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 renseignent 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. Ces données forment l'ensemble de données relatives aux passagers aériens, aussi connu sous le nom de dossier passager ou *Passenger Name Record* (PNR).

Actuellement, 69 États demandent aux entreprises de transport aérien ces données afin de disposer, avant même que des personnes entrent ou sortent de leur territoire, d'informations sur celles qui sont recherchées au niveau national ou international dans le contexte du terrorisme et d'autres infractions pénales graves (grande criminalité). D'autres États sont sur le point d'introduire l'utilisation de données PNR.

Trois résolutions[1] du Conseil de sécurité de l'ONU enjoignent aux États membres de renforcer leurs capacités de collecte, de traitement et d'analyse de données PNR et de les utiliser pour lutter contre le terrorisme. 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 le traitement de ces données est une mesure essentielle pour lutter contre les infractions terroristes et soutient les États dans la mise en place d'un système PNR national.

La directive (UE) 2016/681 du 27 avril 2016 (directive PNR)[2] contraint les États membres de l'UE à mettre en place un système PNR national. Elle n'est pas juridiquement contraignante pour la Suisse, car elle ne constitue pas un développement de l'acquis de Schengen. Toutefois, la Suisse est concernée

1 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

2 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 mai 2016, p. 132

par sa mise en œuvre étant donné que les entreprises de transport aérien ont l'obligation de transmettre les données PNR pour les vols de la Suisse à destination de l'UE.

La Suisse devra également utiliser les données PNR pour lutter contre la grande criminalité. La présente loi vise à créer les bases légales à cette fin. Ainsi, la Suisse remplit ses obligations internationales et contribue de façon significative à la lutte contre la grande criminalité au niveau tant national qu'international.

Certes, les entreprises de transport aérien suisses transmettent déjà des données PNR concernant des vols de la Suisse à destination d'autres pays. Outre des États membres de l'UE, le Royaume-Uni, la Norvège, le Canada et les États-Unis font partie des pays destinataires de ces données.

En juin 2018, les États-Unis ont déclaré pour la première fois que la Suisse ne serait maintenue dans le VWP qu'à condition d'utiliser les données PNR à des fins de lutte contre la grande criminalité. 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.

Outre une dimension de politique de sécurité, le système PNR revêt ainsi pour la Suisse également une dimension économique. Par ailleurs, de plus en plus d'États menacent d'infliger de lourdes amendes aux entreprises de transport aérien suisses qui ne communiquent pas de données PNR voire de leur retirer leurs droits d'atterrissage.

1.2 Nécessité d'agir et objectifs visés

Au niveau international, la Suisse est tenue d'introduire un système PNR et de contribuer ainsi à la lutte mondiale contre la grande criminalité. Des considérations en matière de sécurité nationale plaident également en faveur de l'introduction d'un système PNR. De même, des considérations économiques toujours plus nombreuses incitent aussi à emprunter cette voie.

Dans tous les cas, il convient de veiller à un équilibre entre les préoccupations sécuritaires et économiques et les exigences en matière de protection des données. C'est ce qu'a montré la consultation menée en 2022.

On entend par traitement toute opération relative à des données (personnelles), notamment la collecte, l'enregistrement, la conservation, l'utilisation et la modification. Le traitement de données concerne aussi l'archivage, l'effacement ou la destruction de données. Enfin, cette notion comprend aussi la communi-

cation de données (personnelles), c'est-à-dire le fait de transmettre ces données ou de les rendre accessibles (cf. art. 5, let. d et e, de la loi fédérale du 25 septembre 2020 sur la protection des données [LPD][3]).

De nombreux États, dont plusieurs partenaires économiques importants de la Suisse, demandent depuis longtemps des données PNR aux entreprises de transport aérien.

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

Des données PNR concernant des vols de la Suisse à destination de l'UE sont aussi communiquées. Cette communication à l'État membre de l'UE dans lequel le vol en provenance de la Suisse atterrit 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'OFAC a avisé les entreprises de transport aérien concernées qu'elles étaient autorisées à communiquer les données relatives aux passagers aériens aux États membres de l'UE requérants dans l'attente de la création d'une base légale. Toutefois, leurs dispositions relatives au transport, que les passagers doivent accepter, doivent informer ces derniers de la communication de données. De façon analogue, la communication de données à la Norvège a également été rendue possible.

Depuis, le PFPDT a signalé à plusieurs reprises que les bases légales nécessaires devaient être rapidement créées en Suisse. La communication réciproque de données devra être régie par des traités internationaux.

Afin de pouvoir traiter systématiquement 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, une loi fédérale sur la collecte et l'utilisation de données 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 (DFAE).

Le 13 avril 2022, le Conseil fédéral a ouvert la procédure de consultation relative à l'avant-projet de loi sur les données relatives aux passagers aériens, qui s'est terminée fin juillet 2022.

3 RS **235.1**

1.3 Solutions étudiées et solution retenue

Inspiration du droit européen

L'avant-projet de loi sur les données relatives aux passagers aériens mis en consultation s'appuyait largement sur la directive PNR de l'UE, facilitant ainsi la conclusion d'un accord avec l'UE sur l'échange de données PNR. En effet, le nombre de passagers arrivant de l'UE en Suisse représente plus du tiers du trafic de passagers aériens dans les aéroports suisses. Il est donc important que la Suisse reçoive ces données de l'UE.

L'échange de données PNR est dans l'intérêt de la Suisse et de l'UE, notamment en raison du statut de notre pays en tant que membre associé de l'espace Schengen. La Suisse ne peut pas être une passoire qui permet les entrées dans l'espace Schengen car elle ne dispose pas de données PNR.

Le 21 juin 2022, alors que la loi sur les données relatives aux passagers aériens était encore en consultation, la CJUE a rendu un arrêt[4] dans lequel elle interprète les dispositions de la directive PNR comme étant conformes aux normes pertinentes de la Charte des droits fondamentaux de l'Union européenne[5] (Charte des droits fondamentaux).

La CJUE a notamment clarifié ce qui suit:

- seule la lutte contre la criminalité *grave* justifie, conformément au principe de proportionnalité, l'ingérence grave dans les droits fondamentaux garantis dans le cadre du PNR[6];
- une durée de conservation de six mois pour toutes les données doit être considérée comme admissible;
- une durée de conservation de cinq ans au maximum se justifie si les données présentent des indices objectifs d'infraction terroriste ou d'une autre infraction pénale grave.

L'arrêt de la CJUE n'est pas juridiquement contraignant pour la Suisse. Celle-ci n'est dès lors pas liée à cet arrêt. Toutefois, si la Suisse envisageait d'adapter intégralement la loi sur les données relatives aux passagers aériens à la directive PNR de l'UE, elle devrait également prendre en compte l'interprétation de ce texte et donc l'arrêt de la CJUE.

Plusieurs participants à la consultation sur la loi sur les données relatives aux passagers aériens s'appuient sur cet arrêt pour mettre en avant leurs exigences. Celles-ci sont largement prises en compte dans le présent projet de loi.

4 Affaire C-817/19, ECLI:EU:C:2022:491
5 Charte des droits fondamentaux de l'Union européenne, JO C 326 du 26 octobre 2012, p. 391
6 Affaire C-817/19, ECLI:EU:C:2022:491, ch. marg. 148

Grâce à ces diverses adaptations, la loi sur les données relatives aux passagers aériens s'appuie toujours sur la directive PNR de l'UE.

Solution retenue

La solution retenue se base sur l'avant-projet de loi sur les données relatives aux passagers aériens et tient compte des résultats de la procédure de consultation.

Diverses exigences formulées par les participants à la consultation, qui se fondent sur l'arrêt de la CJUE, ont également été prises en considération.

Il s'agit de tenir compte dans le présent projet:

- d'une réduction de la durée de conservation des données ne présentant aucun indice de grande criminalité;
- du retrait de certaines catégories d'infractions (restriction à la grande criminalité);
- d'un renforcement de la protection des données;
- de l'extension du droit d'accès des personnes concernées.

Cette solution intègre des éléments importants de l'arrêt de la CJUE dans le projet de loi sur les données relatives aux passagers aériens sans altérer considérablement l'efficience et l'efficacité du PNR en tant qu'instrument de lutte contre la grande criminalité.

Le projet est ainsi un juste équilibre entre la préservation de la sécurité (intérêt public) et un degré suffisant de protection des données personnelles (intérêt privé).

Réflexions du point de vue de la technique législative

Le Conseil fédéral a examiné l'option de ne pas créer une nouvelle loi, mais d'intégrer les bases légales nécessaires au PNR dans des lois fédérales en vigueur, en l'occurrence dans la loi fédérale du 21 décembre 1948 sur l'aviation (LA)[7] ou la loi fédérale du 16 décembre 2005 sur les étrangers et l'intégration (LEI)[8].

Il en aurait résulté un cadre juridique 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. De plus, la loi sur les données relatives aux passagers aériens vise des objectifs relevant non seulement de la politique économique, mais aussi de la politique de sécurité, ce qui n'est que partiellement compatible avec les objectifs des lois mentionnées. Par conséquent, ces options ont été abandonnées.

7 RS **748.0**
8 RS **142.20**

Une nouvelle loi régissant complètement le traitement des données relatives aux passagers aériens offre notamment un maximum de transparence aux personnes qui voyagent par voie aérienne et seront concernées par le traitement des données prévu. Pour elles, il sera plus 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.

Le caractère international du PNR justifie aussi le choix de cette solution. On comprend ainsi rapidement comment le PNR est réglé en Suisse, ce qui facilite la communication avec les États étrangers partenaires.

Grâce à la loi sur les données relatives aux passagers aériens, qui contient toutes les dispositions importantes relatives au PNR, le cadre juridique est clairement identifiable aussi pour les entreprises de transport aérien concernées.

Celles-ci auront désormais quelques nouvelles obligations à remplir. En effet, elles devront communiquer les données PNR non seulement à l'unité en charge du PNR à l'étranger, mais aussi à l'UIP nationale. Pas moins de 237 entreprises de transport aérien auraient été concernées par cette extension de la communication de données à l'UIP nationale. Elles ont transporté plus de 53 millions de passagers de la Suisse à destination de l'étranger et inversement sur des vols de ligne et charters.

1.4 Données PNR et autres données relatives aux passagers aériens

Données API

Avant le nouveau millénaire, le nombre de passagers des vols de ligne et charters a augmenté de façon spectaculaire partout dans le monde, ce qui a mis à rude épreuve les infrastructures des aéroports et les ressources en personnel des autorités chargées du contrôle à la frontière. De plus en plus, on a constaté que les passagers et leurs bagages n'étaient plus *tous* contrôlés.

Les données *Advance Passenger Information* (API), que les entreprises de transport aérien doivent transmettre "au préalable" (*in advance*), permettent aux autorités chargées du contrôle aux frontières de recevoir les informations nécessaires sur les passagers aériens avant leur entrée dans le pays ou leur sortie, afin d'effectuer un contrôle de façon ciblée sur la base d'une évaluation des risques.

Après les attentats du 11 septembre 2001, les États-Unis ont commencé à utiliser les données API également aux fins de lutte contre le terrorisme.

Par sa directive 2004/82/CE (directive API)[9], l'UE a contraint ses États membres à créer les bases légales nécessaires à l'utilisation de données API pour faciliter les contrôles aux frontières et lutter contre l'immigration illégale.

Faisant partie de l'acquis de Schengen, la directive API est juridiquement contraignante pour la Suisse. Depuis 2008, notre pays contraint les entreprises de transport aérien à collecter les données API et à les communiquer à l'autorité compétente sur la base de l'art. 104 LEI.

La Suisse n'utilise les données API que depuis 2019 également pour lutter contre le terrorisme et la criminalité internationale organisée (cf. 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	

Contrairement aux données PNR, les données API ne sont pas collectées automatiquement au moment de la réservation d'un billet d'avion, mais doivent être récoltées par les entreprises de transport aérien directement avant le décollage pour leur utilisation par l'État. La Suisse ne contraint les entreprises de transport aérien à collecter et à communiquer les données API que pour des vols spécifiques considérés comme risqués en provenance d'États tiers.

9 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 août 2004, p. 24

Avec l'utilisation de données PNR, les données API figureront dans la catégorie 18 de l'ensemble de données relatives aux passagers aériens (cf. annexe 1 du projet de loi). Toutefois, elles ne seront collectées que si elles sont effectivement disponibles. Cette condition est remplie uniquement si l'État de destination du vol exige la transmission préalable de ces données. Le droit applicable au PNR vaut aussi pour les données API concernées en raison de leur transfert dans la catégorie 18 de l'ensemble de données relatives aux passagers aériens.

Révision de la directive API

Fin 2022, la Commission européenne a proposé une nouvelle réglementation des données API au moyen de deux projets de règlement[10]. Le premier (*API Border*), qui régit l'utilisation des données API pour les contrôles effectués à l'entrée du territoire, est contraignant pour tous les États faisant partie de l'espace Schengen, et donc aussi pour la Suisse. Ce règlement ne présente aucun intérêt dans le cadre de la loi sur les données relatives aux passagers aériens.

Le second projet de règlement (*API Police*), qui prévoit la collecte et la communication de données API à des fins de prévention et de détection des infractions terroristes et de la grande criminalité ainsi que pour les enquêtes et les poursuites en la matière, n'est pas pertinent dans le cadre de Schengen et est contraignant uniquement pour les États membres de l'UE.

La Commission européenne table sur une mise en œuvre de la révision de la directive API *au plus tôt* en 2030.

API Police prévoit que les données API ne soient traitées à l'avenir au sein de l'UE plus que dans le cadre du PNR. De plus, les entreprises de transport aérien seront tenues de collecter ces données automatiquement dans la mesure où les documents le permettent.

On ne sait pas encore dans quelle mesure la Suisse souhaite introduire *API Police*, qui en tant que règlement non pertinent dans le cadre de Schengen n'est pas juridiquement contraignant pour notre pays.

10 Proposition de règlement du Parlement européen et du Conseil relatif à la collecte et au transfert des informations préalables sur les passagers (API) en vue de renforcer et de faciliter les contrôles aux frontières extérieures, modifiant le règlement (UE) 2019/817 et le règlement (UE) 2018/1726, et abrogeant la directive 2004/82/CE du Conseil, COM/2022/729 final; proposition de règlement du Parlement européen et du Conseil relatif à la collecte et au transfert des informations préalables sur les passagers 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, et modifiant le règlement (UE) 2019/818, COM/2022/731 final"

Toutefois, la question pour la Suisse est de savoir si les données API, conçues différemment en Suisse que dans l'UE, doivent continuer à être traitées hors du cadre du PNR. Cela pourrait notamment se justifier pour les vols en provenance d'États qui ne disposent pas d'un système PNR et qui ne doivent donc communiquer systématiquement que les données API à la Suisse. Notamment la Russie et divers États du Proche-Orient comptent parmi ces États.

Outre le décalage temporel par rapport au processus législatif en cours en Suisse sur le PNR, il n'est *actuellement* pas nécessaire, d'un point de vue juridique, d'adapter la loi sur les données relatives aux passagers aériens à la révision de la directive API. Par conséquent, celle-ci n'est pas prise en compte dans le présent projet de loi sur les données relatives aux passagers aériens.

Listes de passagers

L'art. 21*f* LA habilite les autorités de poursuite pénale à demander aux entreprises de transport aérien des "listes de passagers" "afin de prévenir ou de poursuivre des crimes ou des délits". Les entreprises de transport aérien doivent fournir les données ci-après à la demande des autorités de poursuite pénale, "pour autant qu'elles les aient déjà collectées dans le cadre de leurs activités normales":

a. nom, prénom, adresse, date de naissance, nationalité et numéro du document de voyage;

b. date, heure et numéro du vol;

c. lieux de départ, de transit et de destination finale du transport;

d. autres voyageurs éventuels;

e. informations concernant le paiement, notamment le mode et le moyen de paiement utilisés;

f. coordonnées de l'intermédiaire auprès duquel le transport a été réservé.

Contrairement aux données PNR, les listes de passagers ne peuvent pas être traitées de façon systématique.

Dans son message du 31 août 2016[11] concernant la révision partielle 1+ de la loi fédérale sur l'aviation (LA 1+), le Conseil fédéral donne les explications suivantes:

"Afin de compléter les mécanismes de contrôle standardisés appliqués systématiquement aujourd'hui afin de prévenir les attentats contre l'aviation, il est prévu d'instaurer un contrôle individuel des passagers en fonction des risques et sur la base des listes des passagers. Des instruments analogues figurent déjà dans la législation douanière et dans celle sur les étrangers afin de combattre

11 FF **2016** 6913 6920

les infractions douanières et les migrations illégales. Dans le but de prévenir et d'élucider les agissements criminels, les transporteurs aériens seraient tenus de communiquer les listes de passagers aux organes de poursuite pénale si ceux-ci en font la demande."

1.5 Relation avec le programme de la législature, le plan financier et les stratégies du Conseil fédéral

Dans la Stratégie de la Suisse pour la lutte antiterroriste du 18 septembre 2015[12], le Conseil fédéral mentionnait déjà l'utilisation du PNR comme mesure pour empêcher l'entrée, la sortie et le transit de personnes soupçonnées de terrorisme.

Le présent projet de loi figure dans le message du 29 janvier 2020 sur le programme de la législature 2019 à 2023[13] sous forme d'autre objet concernant la mise en œuvre de l'objectif 14 "La Suisse prévient la violence, la criminalité et le terrorisme et lutte efficacement contre ces phénomènes".

L'utilisation du 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".

Étant donné que le cadre de développement financier des départements est désormais fixé sur la base des objectifs de législature, les moyens nécessaires au projet et à la future mise en œuvre du PNR ont été demandés via la planification des besoins destinés au cadre de développement du DFJP à partir de 2025.

1.6 Classement d'interventions parlementaires

Il n'y a aucune intervention parlementaire pendante qui devrait être classée compte tenu du présent message.

2 Procédure préliminaire, consultation comprise

2.1 Projet mis en consultation

Du 13 avril au 31 juillet 2022, les cantons, les partis politiques et les milieux intéressés ont pu se prononcer dans le cadre de la consultation relative à l'avant-projet de loi sur les données relatives aux passagers aériens.

12 FF **2015** 6843
13 FF **2020** 1709 1829

Le projet s'inspirait de la directive PNR de l'UE. Le but était de créer les meilleures conditions possibles pour conclure un accord sur l'échange de données PNR entre la Suisse et l'UE. En effet, cette dernière est le principal partenaire de la Suisse en matière d'économie et de sécurité. De plus, le trafic de personnes est intense entre l'UE et la Suisse, ce qui a également son importance dans le cadre du PNR.

2.2 Résumé des résultats de la procédure de consultation

Quarante-neuf participants à la consultation, qui s'est déroulée du 13 avril à la fin juillet 2022, ont pris position sur la loi sur les données relatives aux passagers aériens.

Sur ces 49 participants, 40 ont évalué l'avant-projet de manière positive ou neutre:

25 cantons	*Seul le canton d'Uri n'a pas pris position sur le projet*
2 partis	Le Centre, PLR
13 organisations/institutions	Aerosuisse, ASA, CCDJP, CCPCS, CPS, easyjet, economiesuisse, FSFP, FST, SWISS, USS, TAF, Zurich Aéroport

Les cantons ont souligné l'importance du PNR en matière de politique de sécurité et la majorité d'entre eux a accueilli favorablement les améliorations que l'utilisation du PNR apportera dans la lutte contre la grande criminalité. Ils se sont parfois montrés critiques à l'égard de l'obligation de détacher et de financer la moitié des collaborateurs de l'UIP.

Les représentants du secteur aérien ont quant à eux souhaité une réglementation pragmatique et inspirée des normes internationales. Pour eux, il faut à tout prix renoncer à un *swiss finish*, c'est-à-dire à des réglementations spécifiques à la Suisse.

Neuf participants à la consultation ont critiqué voire rejeté l'avant-projet:

4 partis	PS, Les Verts, UDC, Parti pirate
3 organisations	AlgorithmWatch, FSA, Société numérique
2 personnes privées	R.S., Law_firm

Se référant à l'arrêt de la CJUE, la plupart de ces participants ont surtout rejeté une durée de conservation unique pour *toutes* les données (cinq ans selon l'avant-projet) et l'étendue des catégories d'infractions. Certains participants ont aussi critiqué le manque d'importance accordée à la protection des données. Ils ont majoritairement fondé leurs critiques en s'appuyant sur l'arrêt susmentionné de la CJUE et ont formulé des propositions d'amélioration.

De plus amples explications figurent dans le rapport du 1er mars 2024[14] sur le résultat de la procédure de consultation.

2.3 Prise en compte des résultats de la consultation

Grâce au PNR, le Conseil fédéral se fixe pour objectif de donner un signal clair en matière de politique de sécurité aux niveaux national et international: la grande criminalité ne doit pas déstabiliser notre société.

La lutte contre la grande criminalité ne doit cependant pas se faire aux dépens de la protection des données. La consultation montre qu'un équilibre entre les intérêts publics en matière de politique de sécurité visés à l'aide du PNR et la protection des droits fondamentaux de la personnalité des individus est indispensable.

L'arrêt de la CJUE, auquel plusieurs participants ont fait référence, a eu une influence non négligeable sur les résultats de la consultation.

Bien que cet arrêt n'ait aucun effet contraignant pour la Suisse, le Conseil fédéral tient compte, dans le présent projet de loi, de certains éléments centraux de cette décision dans la mesure où cela a été demandé dans le cadre de la consultation et ne remet pas en cause l'efficacité du système PNR. L'arrêt reconnaît par ailleurs la conformité de l'utilisation des données PNR aux droits fondamentaux.

Comme indiqué dans l'arrêt, la même durée de conservation ne doit pas s'appliquer pour les données faisant l'objet d'indices objectifs laissant penser que le passager concerné pourrait représenter une menace dans le domaine des infractions terroristes ou de la grande criminalité et les données ne faisant pas l'objet de tels indices. Selon la CJUE, une durée de conservation de cinq ans ne se justifie que pour les données présentant des indices objectifs de grande criminalité. Toutes les autres données doivent par contre être effacées au bout de six mois.

14 www.fedlex.admin.ch > Procédures de consultation > Procédures de consultation terminées > 2022 > DFJP

Certaines prises de position lors de la consultation font remarquer à juste titre l'importance économique de la loi sur les données relatives aux passagers aériens: la Suisse doit se maintenir dans le trafic aérien international pour préserver les emplois locaux dans le secteur aérien et le tourisme ainsi que l'attractivité du pays de manière générale. L'utilisation du PNR est une condition sine qua non pour atteindre cet objectif. En effet, un nombre croissant d'États menacent de faire du PNR une condition à l'octroi des droits d'atterrissage.

Sur le plan économique toujours, la Suisse a tout intérêt à tenir compte des normes internationales lors de la mise en œuvre technique pour éviter des coûts supplémentaires aux entreprises de transport aérien et aux aéroports en raison de solutions spéciales coûteuses. Toutefois, cette demande se heurte à nouveau à certaines exigences en matière de droit sur la protection des données formulées lors de la consultation.

Les demandes visant à différencier la durée de conservation des données relatives aux passagers aériens et à retirer certaines catégories d'infractions sont essentielles pour le Conseil fédéral.

La différenciation de la durée de conservation des données relatives aux passagers aériens nécessite notamment des modifications de la loi qui n'ont pas été explicitement exigées. On peut notamment mentionner:

- la distinction entre les données marquées qui présentent des indices objectifs d'un lien avec la grande criminalité et les données qui n'en présentent pas et ne doivent donc pas être marquées;
- la possibilité de supprimer le marquage des données si les clarifications complémentaires menées par les autorités compétentes ne confirment pas les indices ou si le soupçon initial pesant sur une personne recherchée s'avère sans objet;
- une différenciation du droit d'accès lorsqu'il concerne les données d'un vol ayant eu lieu plus de six mois auparavant.

3 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. Entrée en vigueur le 24 mai 2016, celle-ci a pour but d'harmoniser les règles de droit des États membres de l'UE en lien avec le PNR, 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 s'est depuis volontairement rattaché à l'échange d'informations PNR des autres États membres de l'UE.

La directive harmonise notamment la responsabilité des UIP, en charge de l'exploitation opérationnelle dans les États membres de l'UE (art. 4), le traitement autorisé des données (notamment à l'art. 6) et les obligations imposées aux transporteurs aériens concernant la communication de données (art. 8).

La Commission européenne a réexaminé la directive PNR deux ans plus tard et a présenté les résultats au Parlement européen et au Conseil dans son rapport du 24 juillet 2020[16]. Elle y conclut que le PNR peut être utilisé comme un instrument efficace dans la lutte contre 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 États membres de l'UE confirment par ailleurs qu'une durée de conservation de cinq ans des données PNR indépendamment de tout soupçon est nécessaire d'un point de vue opérationnel. Ils ajoutent néanmoins que l'amélioration de la qualité des données reste un défi.

Par son arrêt du 21 juin 2022, la CJUE a confirmé la conformité de la directive PNR avec la Charte des droits fondamentaux, interprétant les dispositions de la directive comme conformes aux normes pertinentes de la charte.

Jusqu'à présent, l'UE a conclu des accords sur l'échange de données PNR avec les États-Unis[17] et l'Australie[18].

En 2017, la CJUE a examiné des questions sur un tel accord entre l'UE et le Canada dans le cadre d'un avis de droit[19]. La cour exigeait notamment du Canada qu'il efface les données PNR de l'UE directement après le départ de la personne concernée. L'accord avec le Canada n'a toujours pas été conclu.

En février 2020, la Commission européenne a été chargée d'entamer des négociations avec le Japon.

15 Directive PNR, cons. 40

16 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

17 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 août 2012, p. 5

18 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 juillet 2012, p. 4

19 CJUE, avis 1/15 du 26 juillet 2017; ECLI:EU:C:2017:592

La même année, elle a manifesté son intérêt à la Suisse de conclure un accord bilatéral relatif aux données PNR. Fin 2020, la Commission européenne et la Suisse, représentée par le DFAE, l'OFAC et fedpol, ont commencé des discussions exploratoires, qui ont été très constructives.

En revanche, l'intention de la Suisse de tenir compte de l'arrêt de la CJUE, notamment la réduction de la durée de conservation des données et le retrait de certaines catégories d'infractions, a reçu un écho favorable auprès de la Commission européenne.

Le 8 février 2023, la Commission européenne a proposé des négociations sur un accord bilatéral relatif au PNR à la Suisse, à la Norvège et à l'Islande. Elle entend les mener parallèlement mais séparément avec ces trois États associés à Schengen. Pour ce faire, la Suisse a besoin d'un mandat de négociations avec l'UE. Lors de sa séance du 1er novembre 2023, le Conseil fédéral l'a adopté sous réserve de l'approbation des Commissions de politique extérieure des Chambres fédérales et de la Conférence des gouvernements cantonaux. Celles-ci ont approuvé le mandat de négociations.

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-Uni et l'UE sont convenus de poursuivre l'échange de données PNR. Pour ce faire, ils ont négocié un accord relatif au PNR et l'ont intégré à l'art. 542 ss de leur accord de commerce et de coopération[20].

La Suisse a conclu un accord de police[21] avec le Royaume-Uni après le Brexit. Cependant, comme il ne contient aucune base d'échange complet de données PNR, la Suisse concluera un autre accord relatif au PNR avec le Royaume-Uni.

États-Unis

Suite aux attentats du 11 septembre 2001, les États-Unis ont élaboré l'*Aviation and Transportation Security Act*[22], contraignant ainsi les entreprises de transport aérien 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.

20 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

21 RS **0.360.367.1**

22 https://www.congress.gov/bill/107th-congress/senate-bill/1447

Le premier accord sur l'échange de données PNR que les États-Unis ont conclu avec la Suisse est entrée en vigueur le 29 mars 2005, mais uniquement pour une durée de trois ans et demi en raison de sa validité limitée. L'accord ultérieur est entré en vigueur le 23 décembre 2008[23].

En vertu de cet accord, le gouvernement américain s'engage à garantir 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[24].

Canada

Depuis 2009, les données PNR et API sur les vols de la Suisse à destination du Canada sont communiquées 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 du 17 mars 2006[25].

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

Cet accord laisse entrevoir à la Suisse la possibilité de recevoir les données PNR et API en provenance du Canada dès que la base légale nécessaire au traitement de données PNR aura été créée en Suisse.

4 Présentation du projet

Soixante-neuf États dans le monde utilisent les données PNR: 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 depuis quelques années.

23 RS **0.748.710.933.6**
24 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
25 Signature d'une convention avec le Canada sur les données relatives aux passagers aériens

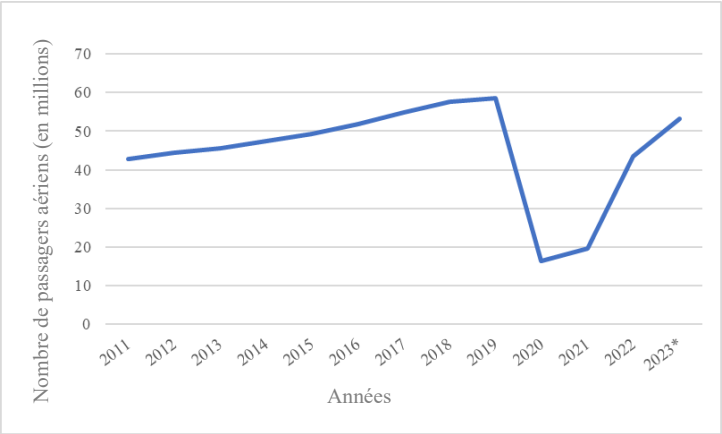
Grâce à la loi sur les données relatives aux passagers aériens, la Suisse utilisera aussi le PNR comme instrument éprouvé pour lutter contre la grande criminalité et ainsi remplir ses obligations internationales.

Les trois résolutions du Conseil de sécurité de l'ONU[26], qui enjoignent aux États membres de mettre en place un système PNR afin de lutter contre le terrorisme, sont particulièrement contraignantes à cet égard.

De plus, l'Organisation de l'aviation civile internationale (OACI) a établi, sur mandat du Conseil de sécurité de l'ONU et en collaboration avec l'Organisation mondiale des douanes (OMD), les gouvernements des États membres, les transporteurs aériens et les prestataires, des normes sur la communication des données relatives aux passagers aériens. Ces normes sont contraignantes pour tous les États membres de l'OACI, et donc aussi pour la Suisse.

Différents États, dont plusieurs partenaires économiques importants de la Suisse, demandent depuis longtemps la transmission de données PNR aux entreprises de transport aérien ayant des liaisons aériennes à destination de la Suisse. Les entreprises de transport aérien opérant des vols au départ de la Suisse peuvent aussi être obligées de communiquer des données. Depuis peu, plusieurs États envisagent de retirer les droits d'atterrissage s'ils ne reçoivent pas préalablement les données PNR. La Suisse risque donc d'être beaucoup moins incluse, à moyen et à long terme, au trafic aérien international. L'importance de ce dernier pour la Suisse se reflète dans le nombre de passagers aériens recensé chaque année dans les aéroports suisses sur des vols de ligne et charters internationaux.

26 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



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).

*2023: le nombre de passagers est provisoire.

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. ch. 1.1).

Le projet de loi sur les données relatives aux passagers aériens s'inspire de la directive PNR de l'UE et prend en compte des contenus essentiels de l'arrêt de la CJUE, dans la mesure où ils ont été demandés dans le cadre de la consultation et qu'ils ne remettent pas fondamentalement en question l'efficacité du PNR.

4.1 Réglementation proposée

Les entreprises de transport aérien collectent au moment de la réservation d'un billet d'avion les données relatives aux passagers aériens et les utilisent pour procéder aux vols. Ces données sont utilisées en aval par les États.

La loi sur les données relatives aux passagers aériens (P-LDPa) est la base légale permettant à la Confédération de traiter systématiquement les données relatives aux passagers des vols de ligne et charters au départ ou à destination de la Suisse aux fins de lutte contre la grande criminalité. Les éléments constitutifs des infractions pénales concernées figurent à l'annexe 2 de la loi.

Rattachée à fedpol, l'UIP est chargée de traiter les données relatives aux passagers aériens. Elle peut donc être considérée comme un prestataire de services de l'État dans le domaine de la sécurité.

Les art. 2 à 4 du projet de loi régissent les obligations des entreprises de transport aérien.

Au total, les entreprises de transport aérien doivent communiquer 19 catégories différentes de données relatives aux passagers aériens. Celles-ci figurent à l'annexe 1 du projet de loi et forment l'ensemble de données relatives aux passagers aériens. Les ensembles de données de *tous* les passagers sur des vols charters et de ligne en provenance de Suisse et à destination de l'étranger et inversement doivent être communiqués. Les données doivent être communiquées durant le créneau horaire prévu par la loi avant le décollage au départ ou à destination de la Suisse. Elles sont communiquées à l'UIP (art. 2) de notre pays.

Les entreprises de transport aérien doivent prendre toutes les mesures raisonnablement exigibles pour communiquer les données dans les délais et dans le respect des prescriptions techniques (art. 3).

De plus, au moment de la réservation du billet d'avion, les entreprises de transport aérien doivent informer les passagers de manière adéquate et sous une forme précise, transparente, intelligible et facilement accessible du fait que leurs données seront traitées par l'État en vertu de la présente loi (art. 4).

Si elles ne respectent pas ou que partiellement leurs obligations, elles s'exposent aux sanctions prévues à l'art. 31. Elles ne violent pas ces obligations légales si elles prouvent qu'elles ont pris toutes les mesures techniques et organisationnelles raisonnablement exigibles pour les remplir.

Les art. 5 à 11 du projet de loi régissent le traitement des données par l'UIP.

Dans l'ensemble, les données relatives aux passagers aériens que reçoit l'UIP ne sont traitées activement que lors de la comparaison automatique des données prévue à l'art. 6. Cette étape de traitement permet un tri précoce des données.

Dès que l'UIP a reçu les données relatives aux passagers aériens, elle les compare automatiquement avec les données issues des systèmes d'information de police ainsi qu'avec les profils de risque et les listes d'observation enregistrés (art. 6).

L'UIP doit ensuite vérifier manuellement les concordances ainsi obtenues. Ce n'est qu'après qu'elle peut les communiquer à une autorité compétente visée à l'art. 1, al. 2. Les concordances non confirmées lors de la vérification manuelle doivent être immédiatement supprimées (cf. art. 22).

Les résultats de la comparaison automatique des données permettent aux autorités compétentes:

- de déceler des infractions pénales visées à l'annexe 2 ne faisant pas encore l'objet d'une enquête ni d'une procédure de poursuite pénale en cours (cf. art. 5, al. 1, let. a);
- de compléter les informations liées à une enquête en cours ou à une procédure pénale pendante pour une infraction visée à l'annexe 2, ou en lien avec des infractions visées à la même annexe non encore élucidées (cf. art. 5, al. 1, let. a);
- d'interpeller voire d'arrêter des personnes qui, en raison d'une infraction pénale visée à l'annexe 2, sont recherchées au niveau national ou international (cf. art. 5, al. 1, let. a et b, ch. 1);
- de livrer des personnes à l'exécution d'une peine privative de liberté à laquelle elles ont été condamnées par un jugement entré en force pour une infraction visée à l'annexe 2 (cf. art. 5, al. 1, let. b, ch. 2).

Une fois communiquées, les données concernées font l'objet d'un marquage par l'UIP. Ces données marquées sont soumises automatiquement à une durée de conservation plus longue que les données n'ayant été ni marquées ni communiquées (cf. art. 21).

Après cette étape de traitement, les données relatives aux passagers aériens ne peuvent plus être communiquées à une autorité compétente, puis marquées:

- qu'à la demande de cette autorité conformément à l'art. 8, ou
- en même temps qu'un indice au sens de l'art. 9 reçu par l'UIP.

L'art. 11 prévoit une forme particulière de communication des données relatives aux passagers aériens *n'*entraînant *pas* le marquage des données: le Service de renseignement de la Confédération (SRC) doit recevoir les données relatives aux passagers aériens de certaines liaisons aériennes pour les traiter en toute autonomie, dans la mesure où cela sert à l'accomplissement de ses tâches prévues à l'art. 6, al. 1, let. a, ch. 1 à 5, de la loi du 25 septembre 2015 sur le renseignement (LRens)[27] et où il s'agit de lutter contre une infraction pénale visée à l'annexe 2 de la présente loi. C'est la LRens qui règle les détails relatifs au traitement par le SRC, comme le délai de conservation autorisée (cf. annexe 3, ch. 1, P-LDPa).

Distinguer les données marquées des non marquées permet de répondre à la demande formulée lors de la consultation, selon laquelle les données relatives aux passagers aériens ne présentant pas d'indices d'une infraction pénale visée à l'annexe 2 (données non marquées) ne doivent pas être conservées aussi longtemps que les données marquées.

27 RS **121**

Une autorité compétente au sens de l'art. 1, al. 2, peut se rendre compte qu'elle n'a plus besoin des données communiquées par l'UIP, par exemple lorsque les indices qui ont conduit à la communication des données n'ont pas été confirmés ou lorsque le soupçon initial portant sur une personne recherchée se révèle sans objet. Aussitôt qu'elle en est informée par l'autorité, l'UIP supprime le marquage des données concernées (art. 10). Les données sont alors à nouveau exemptes de marquage et sont soumises aux conséquences juridiques pertinentes (cf. art. 18 et 21).

Les art. 12 à 15 fixent les modalités d'utilisation des profils de risque et des listes d'observation lors de la comparaison automatique des données. Le Conseil fédéral surveille l'utilisation de ces instruments.

Le profil de risque permet de rechercher dans les données relatives aux passagers aériens des combinaisons de données qui sont fréquentes dans le cas de certaines infractions pénales visées à l'annexe 2 et notamment dans le cas du crime organisé (traite d'êtres humains) (art. 12). Étant donné que cette recherche n'est pas effectuée en rapport avec une infraction pénale visée à l'annexe 2 déjà connue des autorités, le profil de risque ne contient pas de données se rapportant à une personne physique identifiée ou identifiable et constituant par conséquent des données personnelles au sens de l'art. 5, let. a, LPD.

En revanche, les données se rapportant à une personne physique ou morale identifiée ou identifiable sont utilisées dans la liste d'observation prévue aux art. 13 et 14. Les listes d'observation permettent de rechercher dans les données relatives aux passagers aériens des éléments concrets en rapport avec une infraction pénale visée à l'annexe 2 dont les autorités ont connaissance: par exemple, le nom d'une personne recherchée ou le numéro d'une carte de crédit utilisée à plusieurs reprises par une organisation criminelle.

Dans des cas exceptionnels et uniquement si un tribunal des mesures de contrainte compétent l'a autorisé, les données de tiers peuvent également faire l'objet d'une liste d'observation (art. 14). Ces données doivent permettre de localiser à l'étranger le lieu de séjour, encore inconnu, d'une personne accusée d'une infraction pénale visée à l'annexe 2 ou condamnée par un jugement entré en force pour une telle infraction et recherchée afin qu'elle exécute sa peine privative de liberté.

L'utilisation de ces instruments doit être contrôlée par le Conseil fédéral (art. 15).

Les art. 17 à 26 concernent la protection des données, que l'UIP doit prendre en compte lorsqu'elle traite les données relatives aux passagers aériens.

En révisant totalement son droit sur la protection des données, la Suisse s'adapte aux réformes européennes dans le domaine[28]. Le présent projet de loi tient compte du nouveau droit sur la protection des données, qui est entré en vigueur le 1er septembre 2023.

Les art. 17 à 26 de la loi sur les données relatives aux passagers aériens, pour la plupart, précisent et priment la LPD. Certaines dispositions mentionnent par souci de transparence des règles de la LPD ou y renvoient.

L'art. 17 expose les bases légales en matière de protection des données applicables à l'UIP et aux autorités qui reçoivent et traitent des données en vertu du présent projet de loi.

Les données non marquées, y compris celles dont le marquage a été supprimé conformément à l'art. 10, "sont pseudonymisées un mois après avoir été communiquées à l'UIP et bénéficient ainsi d'une protection techniquement accrue (art. 18).

La période durant laquelle des données non marquées peuvent être attribuées à une personne précise se limite donc à un mois. Contrairement à l'anonymisation, la pseudonymisation peut être annulée. Cette étape du traitement nécessite néanmoins l'autorisation du Tribunal administratif fédéral (TAF) (art. 19 et 20).

Les données non marquées sont effacées automatiquement après six mois. Cette courte durée de conservation répond à une demande récurrente formulée lors de la consultation.

En revanche, les données marquées peuvent être conservées pendant cinq ans, pour autant que leur marquage n'ait pas été supprimé auparavant conformément à l'art. 10. Une fois ce délai passé, elles sont effacées automatiquement (art. 21).

Les autres données susceptibles d'être traitées par l'UIP en vertu de la présente loi sont soumises aux délais d'effacement prévus à l'art. 22.

L'art. 24 établit la nécessité de consigner tous les traitements automatiques dans un procès-verbal électronique; celui-ci permet de savoir, même a posteriori, qui a effectué quelle étape du traitement automatisé à quel moment et quelles données sont concernées. Les procès-verbaux doivent être conservés en dehors du système d'information PNR (s'agissant du lieu d'enregistrement, cf. ch. 6.1) et être accessibles uniquement aux quelques personnes qui en ont impérativement besoin pour s'acquitter de leurs tâches de sécurité, de surveillance et de contrôle.

28 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** 6565 6567

L'art. 26 confère aux passagers aériens le droit d'obtenir des informations sur les données les concernant qui sont traitées en vertu de la présente loi. Lorsque ces informations lui sont transmises, la personne concernée ne doit cependant pas pouvoir apprendre qu'une procédure à son encontre est en cours.

Ce risque existe lorsque l'accès concerne des données relatives à un vol qui date de plus de six mois, car la plupart de ces données ont alors été effacées. Seules subsistent celles qui ont été marquées et peuvent être conservées pendant cinq ans (art. 21).

En cas de demande d'accès portant sur des données relatives à un vol qui date de plus de six mois, fedpol informe *toujours* la personne requérante du report de sa réponse et de la possibilité de demander au PFPDT qu'il vérifie si les éventuelles données la concernant sont traitées licitement et si des intérêts prépondérants liés au maintien du secret justifient le report.

Tout accès concernant des données relatives à des vols qui datent de plus de six mois est régi sans restriction par la LPD.

D'autres dispositions, régies dans d'autres sections de la loi, sont aussi pertinentes du point de vue de la protection des données, notamment:

- art. 5, al. 1: finalité du traitement des données;
- art. 5, al. 2: restriction de l'UIP dans le traitement de données sensibles;
- art. 6, al. 2 et 3, et 7, ainsi que les renvois des art. 8 et 9 au 7: obligation de vérifier manuellement les résultats du traitement avant de les communiquer à une autorité compétente;
- art. 16, al. 2: accès restreint au système d'information PNR.

Peuvent être considérées comme des mesures techniques visant à garantir la protection des données (cf. art. 7, al. 2, LPD):

- la comparaison (art. 6), la pseudonymisation (art. 18) et l'effacement (art. 21) automatiques des données relatives aux passagers aériens; et
- la consignation du traitement des données dans un procès-verbal (art. 24).

Enfin, les art. 27, al. 2, et 28, al. 3, prévoient des mesures organisationnelles visant à garantir la protection des données, afin de limiter le risque d'échange informel de contenus relevant du droit sur la protection des données.

La pseudonymisation (art. 18) et l'anonymisation des données (art. 23) constituent des mesures techniques visant à garantir la sécurité des données (cf. art. 7 LPD).

Les art. 27 et 28 ont pour objet l'organisation et le personnel de l'UIP.

L'UIP est rattachée à fedpol (art. 27). Elle se compose à parts égales de collaborateurs de la Confédération et de collaborateurs détachés par les cantons. Les cantons prennent en charge les coûts relatifs au salaire de leurs collaborateurs pendant la durée de l'engagement et versent les cotisations aux assurances sociales. Cette modalité prend en compte le fait que l'UIP apporte une contribution à la lutte contre la criminalité en grande partie pour les cantons. La Confédération et les cantons fixeront les modalités du détachement du personnel à l'UIP dans une convention que le Conseil fédéral est autorisé à conclure avec les cantons (art. 28).

Les art. 31 et 32 règlent les sanctions administratives.

Les entreprises de transport aérien qui ne remplissent pas ou pas suffisamment leurs obligations en vertu des art. 3 et 4 peuvent être sanctionnées. Toutefois, si elles prouvent qu'elles ont pris toutes les mesures techniques et organisationnelles raisonnablement exigibles pour remplir leurs obligations, il n'y a pas de sanction (art. 31, al. 4).

4.2 Adéquation des moyens requis

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 dans un État de droit. Pour les victimes, punir les auteurs d'une infraction est synonyme d'un nouveau départ dans leur vie personnelle.

La sécurité est un bien crucial pour le bien-être d'une société et sa prospérité. Toutefois, la sécurité a un prix.

Ce prix n'est pas seulement pécuniaire comme on peut le constater également dans le cadre de la présente loi: bien que les contrôles contribuent de façon déterminante à la sécurité publique, ils peuvent ponctuellement restreindre nos droits de la personnalité, même lorsqu'il n'existe aucun problème sécuritaire.

Le PNR est un instrument qui a fait ses preuves au niveau international pour lutter contre la grande criminalité. En le mettant en place, la Suisse renforce la sécurité sur le plan national, mais aussi international.

Autrefois, chaque personne était contrôlée à l'entrée et à la sortie du pays. Compte tenu de l'évolution fulgurante du trafic aérien ces 30 dernières années, il a fallu réduire le nombre de contrôles systématiques de voyageurs effectués sur place selon une approche fondée sur les risques. Néanmoins, il reste indispensable, pour le maintien de la sécurité, d'identifier les personnes coupables d'avoir commis des infractions en lien avec la grande criminalité ou qui poursuivent de tels objectifs.

Le PNR permet ce maintien de la sécurité. Les succès obtenus par les États membres de l'UE le confirment. Par ailleurs, la CJUE a reconnu, dans son arrêt du 21 juin 2022, que les objectifs en matière de lutte contre la grande

criminalité visés par l'utilisation du PNR sont compatibles avec la protection des droits fondamentaux.

L'utilisation de données PNR n'entraîne pas de charge règlementaire conséquente pour les entreprises de transport aérien. La charge de travail qu'elles doivent fournir se limite à communiquer à temps les données disponibles au service de l'État responsable et à informer les voyageurs. L'utilisation du PNR n'exige donc aucun effort supplémentaire considérable de leur part.

Le PNR est non seulement efficient, mais aussi effectif, sinon comment expliquer qu'il soit utilisé depuis près de 20 ans pour lutter contre la grande criminalité dans 69 États, dont les États-Unis, le Canada, les membres de l'Union européenne, l'Australie et le Royaume-Uni. Les statistiques et les rapports de cas élaborés par certains pays le prouvent clairement.

Il est prévu que les cantons détachent la moitié des collaborateurs de l'UIP et supportent les coûts en personnel qui en découlent. Cette répartition des coûts entre la Confédération et les cantons montre que la sécurité du pays et la protection de la population contre la grande criminalité sont une tâche commune de la Confédération et des cantons. En revanche, la Confédération supporte elle seule les coûts relatifs à la mise en place de l'infrastructure technique et à l'exploitation.

4.3 Mise en œuvre

En plus des données PNR que la Confédération recevra à l'avenir en vertu de la loi sur les données relatives aux passagers aériens, 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 et commune (*single window*) doit être prévue pour la communication de données PNR et API. Elle vise à épargner du travail inutile aux entreprises de transport aérien.

Cela signifie qu'il convient de mettre à disposition cette interface unique sur le plan technique pour les données API et PNR lors de la mise en place du système PNR. L'Association suisse des aérodromes et SWISS ont salué cette solution lors de la procédure de consultation.

5 Commentaire des dispositions

Section 1 Objet

Art. 1 Objet et but

Cette disposition présente l'essentiel de la loi et le but poursuivi par celle-ci.

Al. 1

Let. a

Les entreprises de transport aérien doivent communiquer les données relatives aux passagers aériens à l'UIP pour tous les vols à destination de la Suisse ou partant de la Suisse vers l'étranger.

Pour elles, cette obligation n'a rien de totalement nouveau. Les entreprises de transport aérien la remplissent déjà depuis de nombreuses années, par exemple vis-à-vis des États-Unis, du Canada et des États membres de l'UE. Seule nouveauté: elles doivent communiquer les données relatives aux passagers aériens également à l'UIP.

Let. b

En plus des obligations des entreprises de transport aérien, la loi règle également le traitement des données relatives aux passagers aériens par les services compétents.

Les données relatives aux passagers aériens peuvent être traitées dans le but de combattre la grande criminalité (cf. al. 4).

Let. c

La présente loi définit également l'organisation du service national qui sera chargé du traitement des données relatives aux passagers aériens en Suisse. La désignation usuelle de ce service au niveau international, *unité d'information passagers, UIP* en abrégé, doit aussi être utilisée en Suisse.

L'UIP doit être rattachée à fedpol (cf. art. 27) et doit être composée de collaborateurs de la Confédération et des cantons (cf. art. 28).

Al. 2

Le but de la présente loi consiste à soutenir les autorités de la Confédération et des cantons dans la lutte contre la grande criminalité (cf. annexe 2).

Les autorités qui bénéficient des prestations de l'UIP en vertu de la présente loi sont les organes de police et les autorités de poursuite pénale de la Confédération et des cantons, les services de renseignements fédéraux, à savoir le SRC et le service de renseignement de l'armée, ainsi que les autorités d'exécution cantonales visées à l'art. 9 LRens.

Les autorités de poursuite pénale de la Confédération englobent aussi notamment le Service fédéral de sécurité (art. 4, let. b, de la loi du 19 mars 2010 sur l'organisation des autorités pénales, LOAP[29])[30].

Al. 3

Les *entreprises de transport aérien* ne sont définies nulle part dans le droit en vigueur, raison pour laquelle elles sont décrites plus en détail ici. Cette définition se fonde sur celle prévue dans le cadre de la loi du 25 septembre 2020 sur le CO_2[31] (art. 2, let. i). Est considérée comme entreprise de transport aérien toute organisation titulaire d'une autorisation d'exploitation ou d'une autre autorisation équivalente l'habilitant à transporter des personnes par aéronef à des fins commerciales.

N'est pas considérée comme entreprise de transport aérien toute 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. Sont également exclus du domaine d'application de la présente loi les vols militaires et les vols d'État, ainsi que les vols de recherche et de sauvetage.

La définition des entreprises de transport aérien est d'autant plus importante que celles-ci sont tenues de se conformer à la présente loi. Les entreprises de transport aérien suisses et étrangères ont l'obligation de communiquer les données relatives aux passagers aériens à l'UIP à temps et conformément aux prescriptions techniques (cf. art. 2 et 3). En outre, elles doivent informer leurs passagers de manière adéquate sur le traitement des données de ces derniers en vertu de la présente loi (cf. art. 4). L'art. 31 prévoit des sanctions en cas de violation de ces obligations.

Al. 4

L'annexe 1 de la présente loi spécifie les données relatives aux passagers aériens qui doivent être communiquées par les entreprises de transport aérien et traitées selon la présente loi.

Les données relatives aux passagers aériens se subdivisent en 19 catégories différentes, lesquelles forment un ensemble de données, autrement dit un dossier passager. Les catégories correspondent à la directive PNR et tiennent compte dans leur formulation de la teneur que la CJUE exige des États membres dans son arrêt du 21 juin 2022.

Les entreprises de transport aérien recueillent les données relatives aux passagers aériens au moment de la réservation des billets d'avion. Elles ont besoin de ces données pour le bon déroulement du vol. Leur traitement au sens de la présente loi se limite aux données déjà disponibles et est donc simplement décalé en aval.

29 RS **173.71**
30 Message du 10 septembre 2008 relatif à la loi fédérale sur l'organisation des autorités pénales de la Confédération (Loi sur l'organisations des autorités pénales, LOAP), FF **2008** 7371 7394
31 FF **2020** 7607 7608; rejetée en votation populaire le 13 juin 2021

Les données API constituent un cas à part, car elles doivent, pour autant qu'elles soient disponibles, être communiquées par les entreprises de transport aérien comme une partie de l'ensemble des données relatives aux passagers aériens dans la catégorie 18. Les données API ne sont pas recueillies lors de la réservation, mais doivent être relevées par les entreprises de transport aérien lorsque l'État le demande (cf. art. 104 LEI). C'est pourquoi elles doivent être communiquées à l'UIP dans la catégorie 18 du PNR seulement si elles sont *disponibles.*

La plupart des 19 catégories de données ne présentent pas de données qui permettent d'identifier une personne. Comme il ne s'agit pas de données personnelles (cf. art. 5, let. a, LPD), leur traitement n'entre pas dans le domaine d'application de la LPD révisée (cf. art. 2 LPD).

Des données personnelles figurent dans les catégories suivantes de l'ensemble de données relatives aux passagers aériens:

- *catégorie 4:* prénom(s) et nom(s) du passager;
- *catégorie 5:* adresse et coordonnées, y compris numéro de téléphone et adresse électronique du passager;
- *catégorie 6:* indications relatives à la carte de crédit utilisée et adresse de facturation;
- *catégorie 8:* programme "grands voyageurs": statut et numéro du passager;
- *catégorie 9:* nom de la personne responsable du dossier à l'agence de voyage qui a effectué la réservation du billet;
- *catégorie 12:* informations sur les personnes non accompagnées de moins de 18 ans, nom et coordonnées de la personne présente au départ et à l'arrivée, et de l'agent présent au départ et à l'arrivée;
- *catégorie 17:* nombre, prénom(s) et nom(s) des autres voyageurs figurant dans le dossier passager;
- *catégorie 18:* données API (cf. art. 104, al. 3, LEI) qui sont également des données personnelles: (a) l'identité des passagers (nom, prénom, sexe, date de naissance, nationalité); (b) le numéro, l'État émetteur, le type et la date d'échéance du document de voyage utilisé; (c) le numéro, l'État émetteur, le type et la date d'échéance du visa ou du titre de séjour utilisé, pour autant que l'entreprise de transport aérien dispose de ces données;
- *catégorie 19:* elle contient toutes les modifications du dossier passager. Cette catégorie contient des données personnelles si des données de ce type ont été modifiées postérieurement à la réservation.

Les données relatives aux passagers aériens ne peuvent être traitées au sens de la présente loi que dans le but de lutter contre la grande criminalité. On

entend par grande criminalité les infractions qui figurent dans les catégories d'infractions de l'annexe 2 de la loi indiquant les éléments constitutifs de l'infraction prévus par le code pénal (CP)[32] ou le droit pénal accessoire. L'annexe 2 les subdivise en infractions terroristes (ch. 1) et en autres infractions pénales graves (ch. 2).

Ces catégories d'infractions étaient à l'origine fondées sur celles de la directive PNR et leur attribuaient les éléments constitutifs de l'infraction déterminants prévus par l'annexe 1, élargie dans le cadre de PRÜM[33], de la loi du 12 juin 2009 sur l'échange d'informations Schengen (LEIS)[34]. Bien que l'élargissement ne soit pas encore entré en vigueur, il est néanmoins pris en compte dans la présente loi. Il en va de même pour un autre futur élargissement de l'annexe de la LEIS qui est actuellement en préparation. À la différence de l'annexe 1 LEIS, les catégories d'infractions déterminantes pour le PNR tiennent également compte des formes graves d'espionnage.

Sont considérées *terroristes* au sens de la présente loi les infractions qui tombent sous le coup du ch. 22 de l'annexe 1 LEIS. L'élément constitutif de l'infraction d'émeute (cf. art. 260, al. 1, CP) ne fait plus partie des catégories d'infractions déterminantes pour le PNR, ce qui répond aux demandes formulées par des parties consultées.

La plupart de ces infractions sont des crimes, qui sont passibles d'une peine privative de liberté de *plus* de trois ans (cf. art. 10, al. 2, CP). En revanche, les éléments constitutifs d'infraction ci-après sont des délits (cf. art. 10, al. 3, CP), qui sont passibles d'une peine privative de liberté n'excédant pas trois ans:

- Menaces alarmant la population (art. 258 CP),
- Provocation publique au crime ou à la violence (art. 259 CP).

Ne sont qualifiées de terroristes la plupart des infractions figurant dans cette catégorie que si elles sont effectivement motivées par le terrorisme (cf. annexe 2, ch. 1). Par infraction motivée par le terrorisme, on entend notamment les actions destinées à influencer ou à modifier l'ordre étatique et susceptibles d'être réalisées par des infractions graves ou la menace de telles infractions (cf. art. 23*e* de la loi fédérale du 21 mars 1997 instituant des mesures visant au maintien de la sûreté intérieure [LMSI][35]).

Sous *autres infractions pénales graves*, l'annexe 2 de la présente loi inclut:

- au ch. 2.1 les infractions déjà mentionnées de l'annexe 1 LEIS,
- ainsi qu'au ch. 2.2, les infractions en lien avec l'espionnage.

32 RS **311.0**
33 Arrêté fédéral portant approbation et mise en œuvre de l'accord entre la Suisse et l'UE concernant l'approfondissement de la coopération transfrontalière (coopération Prüm) et du Protocole Eurodac entre la Suisse, l'UE et la Principauté de Liechtenstein concernant l'accès à Eurodac à des fins répressives, FF **2021** 2332 10-16
34 RS **362.2**
35 RS **120**

La liste des autres infractions pénales graves a été considérablement raccourcie compte tenu de diverses demandes issues de la consultation en lien avec l'arrêt de la CJUE. Les infractions relevant de la compétence de poursuite pénale de l'Office fédéral de la douane et des frontières (OFDF) ont notamment été retirées, car il ne s'agit pas de grande criminalité.

Les catégories d'infractions ne comprennent désormais que les éléments constitutifs de l'infraction

a) qui présentent *explicitement* selon l'arrêt de la CJUE un "niveau de gravité incontestablement élevé" (ch. marg. 149), un "lien direct avec le transport aérien de passagers" (ch. marg. 154) en tant que grande criminalité ou sont "de nature transnationale" (ch. marg. 155);

b) pour lesquels le droit suisse prévoit une peine minimale légale qui peut être comprise comme étant une spécificité du droit national mentionnée par la CJUE et qui permet de déduire une gravité particulière de l'infraction (a contrario du ch. marg. 151 s.).

Compte tenu des changements de la situation géopolitique, trois éléments constitutifs de l'infraction en lien avec l'espionnage (ch. 2.2) ont été ajoutés aux catégories d'infractions. Ces formes graves d'espionnage sont toutes des crimes au sens de l'art. 10, al. 2, CP et prévoient une peine minimale légale.

Section 2 Obligations des entreprises de transport aérien

Art. 2 Communication des données relatives aux passagers aériens

Le fait de transmettre des données personnelles ou de les rendre accessibles est considéré comme une communication (cf. art. 5, let. e, LPD).

L'art. 2 fixe les modalités selon lesquelles les entreprises de transport aérien doivent communiquer les données relatives aux passagers aériens. La violation de ces obligations peut entraîner des sanctions (cf. art. 31).

Des parties consultées ont suggéré la création d'une disposition régissant l'utilisation et l'effacement autorisés des données par les entreprises de transport aérien. Il n'est pas possible de satisfaire cette demande, car les données relatives aux passagers aériens sont des données dont les entreprises de transport aérien ont besoin pour procéder à la réservation et au vol. Dans ce contexte, ce sont les besoins d'exploitation qui déterminent la durée de conservation de ces données auprès des entreprises de transport aérien, ainsi que les principes de protection des données que celles-ci sont tenues de respecter.

Al. 1

L'art. 2 établit que toutes les entreprises de transport aérien (cf. art. 1, al. 3) qui desservent la Suisse doivent communiquer à l'UIP les données relatives aux passagers aériens (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, en dépit du fait que l'aéroport se trouve sur un terrain situé en dehors du pays. Il en va de même pour les vols munis du code d'aéroport IATA au départ de l'Euroairport de Bâle-Mulhouse-Fribourg qui desservent un aéroport non suisse.

Il n'y a pas lieu de communiquer les données relatives aux passagers aériens sur les vols internes, même s'ils sont effectués par des entreprises de transport aérien au sens de l'art. 1, al. 3.

Al. 2

Les données relatives aux passagers aériens sont recueillies au moment de la réservation d'un billet d'avion. Si la réservation est effectuée auprès d'une entreprise de transport aérien suisse, les données correspondantes se trouvent en Suisse. Si en revanche, le billet est réservé depuis la Suisse auprès d'une entreprise de transport aérien située à l'étranger, les données relatives aux passagers aériens ne se trouvent plus en Suisse, mais dans l'État où est situé le siège de l'entreprise de transport aérien. En réservant son billet, le passager communique lui-même ses données "à l'étranger" ou accepte que celles-ci soient communiquées.

L'al. 2 s'applique donc uniquement aux entreprises de transport aérien suisses et non aux étrangères. Les entreprises de transport aérien suisses ne peuvent communiquer les données relatives aux passagers aériens à une UIP étrangère que si un traité international signé par la Suisse le prévoit (cf. art. 29).

En revanche, si le vol a été réservé depuis la Suisse auprès d'une entreprise de transport aérien étrangère, la communication transfrontalière des données par l'entreprise de transport aérien étrangère est régie par le droit (étranger) qui lui est applicable.

Le partenaire de la Suisse peut être un État étranger ou une organisation internationale. Parmi ces dernières, on mentionnera dans le présent contexte en particulier l'UE.

Si la Suisse négocie un tel traité avec un partenaire qui dispose d'une protection des données adéquate (cf. art. 16, al. 1, LPD), elle n'a pas besoin de convenir de règles spécifiques sur la protection des données communiquées depuis la Suisse. Pour la communication des données au sens de l'al. 2, il suffit d'un traité de droit international public qui se limite à la réciprocité de la communication.

Si en revanche le partenaire ne démontre pas une protection des données adéquate, le traité international doit aussi prévoir, en plus de la réciprocité de la communication des données, des dispositions qui devront être respectées pour le traitement des données relatives aux passagers aériens issues de Suisse. Le partenaire garantit ainsi que la protection des données issues de Suisse est appropriée (cf. art. 16, al. 2, let. a, LPD).

Aujourd'hui déjà, les entreprises de transport aérien suisses fournissent des données relatives aux passagers 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 constitue la base légale de la communication des données. Par ailleurs, ces deux accords garantiront la communication des données à l'UIP suisse dès que la base légale requise pour le traitement des données relatives aux passagers aériens aura été créée grâce à la présente loi.

D'autres accords sont prévus. Un mandat de négociations avec l'UE est en cours de préparation. L'accord permettra de remplacer la réglementation transitoire actuelle (cf. ch. 1.2).

Al. 3

Les données relatives aux passagers aériens sont communiquées 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'après la fin de l'embarquement. La première communication 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 est indispensable dans le cas des vols de courte distance. La communication des données immédiatement après la fin de l'embarquement permet de *mettre à jour* les données déjà enregistrées et de dresser un tableau définitif des passagers qui entrent effectivement en Suisse ou en sortent. L'UIP ne peut plus consulter les données qui lui ont été communiquées précédemment relatives aux passagers qui n'ont finalement pas embarqué sur le vol et ne peut donc plus les traiter non plus.

Cette communication échelonnée permet à l'UIP, après l'embarquement, de se concentrer sur les données qui ont été mises à jour ou qui ont été ajoutées.

Les entreprises de transport aérien procèdent elles-mêmes à la communication à l'UIP des données relatives aux passagers aériens. Cette méthode dite *push* correspond non seulement aux recommandations de l'OACI[36], mais aussi à l'art. 8 de la directive PNR de l'UE.

Al. 4

Le Conseil fédéral est compétent pour fixer les modalités à respecter pour la communication des données. Les détails *techniques* qu'il s'agit de régler comportent notamment les formats autorisés pouvant s'appliquer à la communication des données relatives aux passagers aériens.

Le Conseil fédéral s'appuie pour ce faire sur les normes de l'OACI, qui sont contraignantes pour tous les États membres, et donc pour la Suisse. Ces normes internationales garantissent que les données soient communiquées partout dans le monde selon des principes uniformes, de manière à éviter aux entreprises de transport aérien une charge de travail supplémentaire qui serait

36 OACI, Lignes directrices sur les données des dossiers passagers (PNR), ch. 2.7.3, disponibles à l'adresse https://www.icao.int/Security/FAL/ANNEX9/Documents/9944_cons_fr.pdf

due à des réglementations spécifiques à chaque pays. Si des prescriptions internationales doivent être précisées, le Conseil fédéral s'appuiera autant que possible sur les solutions de l'UE. Il remplit ainsi les exigences compréhensibles formulées par les représentants du secteur aérien lors de la consultation, c'est-à-dire renoncer à un *swiss finish* et donc à des règlementations spécifiques à la Suisse.

Art. 3 Devoir de diligence

Les entreprises de transport aérien doivent communiquer à l'UIP les données de tous les passagers à temps et conformément aux prescriptions techniques (cf. art. 2, al. 3 et 4).

Elles doivent prendre toutes les mesures raisonnablement exigibles pour remplir cette obligation. Dans le cas contraire, elles s'exposent aux sanctions prévues à l'art. 31.

Art. 4 Obligation d'informer

L'art. 4 oblige les entreprises de transport aérien à informer les passagers de manière *adéquate* du fait que leurs données communiquées au moment de la réservation du billet d'avion seront traitées non seulement dans le cadre de leur vol, mais aussi en vertu de la présente loi.

L'art. 13 de l'ordonnance du 31 août 2022 sur la protection des données (OPDo)[37] précise ce qu'est la manière "adéquate": l'information doit être communiquée de manière concise, transparente, compréhensible et facilement accessible.

Dans le rapport explicatif relatif à l'OPDo, l'Office fédéral de la justice (OFJ) précise: "en d'autres termes, cela signifie que le responsable du traitement ou le sous-traitant doivent s'assurer, lors du choix des modalités d'informations, que les informations les plus importantes sont toujours transmises dans le premier niveau de communication avec la personne concernée lors de la collecte de ses données personnelles. Par exemple, lorsque la communication se fait sur un site internet, une bonne pratique peut consister à faire en sorte que les informations essentielles soient toutes disponibles en un coup d'œil, par exemple sous la forme d'un aperçu. Pour obtenir des informations complémentaires, la personne concernée pourra ensuite cliquer sur ces premières informations et cela ouvrira une autre fenêtre contenant des détails supplémentaires Il faut néanmoins préciser que la communication par un site internet

37 RS **235.11**

n'est pas toujours suffisante: il faut que la personne concernée sache qu'elle trouvera ces informations sur un site en particulier[38]."

Pour que les passagers puissent faire valoir leurs droits, les entreprises de transport aérien doivent au moins, conformément à l'art. 4 de la présente loi, leur fournir les informations suivantes:

- le fait que les données relatives aux passagers aériens sont communiquées à fedpol;
- le titre complet de la présente loi constituant la base légale régissant le traitement des données relatives aux passagers aériens;
- l'existence du droit d'accès en vertu de l'art. 26;
- les coordonnées de fedpol;
- le nom du service étranger lorsque les données sont communiquées à l'étranger.

Si une entreprise de transport aérien ne remplit pas l'obligation d'informer visée à l'art. 4 ou la remplit de façon insuffisante, elle s'expose aux sanctions prévues à l'art. 31.

Il serait possible de renoncer à l'obligation d'informer du moment que le traitement des données relatives aux passagers aériens est déjà régi par la loi (cf. art. 19 LPD). Toutefois, le fait que l'obligation d'informer soit prévue par la loi sur les données relatives aux passagers aériens se justifie, 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 loi sur les données relatives aux passagers aériens);
- à des fins différentes (réservation du vol / lutte contre la grande criminalité);
- sous la responsabilité d'acteurs différents (entreprises de transport aérien / fedpol).

En ce qui concerne la communication automatique des liaisons aériennes au SRC régie à l'art. 11, le PFPDT aurait préféré une obligation d'informer des entreprises de transport aérien élargie. Dans ce contexte, il rappelle que la communication automatique d'informations par le biais d'un service utilisé à cet effet ne doit pas entraîner une dilution de l'obligation d'informer.

38 Rapport explicatif de l'Office fédéral de la justice du 31 août 2022 relatif à l'ordonnance sur la protection des données, p. 37, disponible sur https://www.bj.admin.ch/bj/fr/home.html > Etat & Citoyen > Protection des données > Nouveau droit de la protection des données > 1. Etapes préalables, 2022 – Adoption des nouvelles ordonnances (OPDo et OCPD)

Section 3 Traitement des données par l'UIP

Art. 5 Principes

Al. 1

L'al. 1 définit les buts du *traitement des données.*

Les données PNR doivent pouvoir servir aussi bien à la prévention qu'à la répression de la grande criminalité. La liste figurant à l'al. 1 décrit ces buts ainsi:

- *but préventif*: déceler et empêcher les infractions concernées (cf. notamment art. 6, al. 1, let. a, LRens, art. 2*a*, let. f, de la loi fédérale du 7 octobre 1994 sur les Offices centraux de police criminelle de la Confédération et les centres communs de coopération policière et douanière avec d'autres États [LOC][39], lois cantonales sur la police);
- *but répressif*: élucider les infractions concernées et rechercher des personnes prévenues (cf. notamment art. 15 à 21 du code de procédure pénale du 5 octobre 2007 [CPP][40]), ou des personnes condamnées par un jugement entré en force pour l'une des infractions pénales concernées et qui n'ont pas encore ou pas entièrement purgé leur peine.

Ces buts sont restreints lors de l'utilisation de profils de risque (art. 12) et de listes d'observation (art. 13 et 14).

Al. 2

Des données personnelles sensibles (cf. art. 5, let. c, LPD) ne se trouvent ni dans les profils de risque ni dans les listes d'observation. Les données relatives aux passagers aériens visées à l'annexe 1 ne comportent pas non plus de données personnelles sensibles.

L'UIP peut toutefois rencontrer ce type de données lorsqu'elle vérifie les concordances obtenues par la comparaison automatique (cf. art. 6, al. 2 et 3).

L'UIP ne peut traiter ces données que s'il s'agit des données visées à l'al. 2, c'est-à-dire:

- des données biométriques identifiant une personne physique, par exemple une empreinte digitale numérique, des images faciales, des images de l'iris ou des enregistrements vocaux;

39 RS **360**
40 RS **312**

- des données sur des poursuites ou sanctions pénales et administratives; sont considérées comme telles les informations sur les actes matériels de la police (mesures de sécurité et de protection)[41].

L'UIP doit effacer sans délai toutes les autres données sensibles qui peuvent être recueillies lors du traitement des données relatives aux passagers aériens (cf. art. 22, let. a).

Art. 6 Comparaison automatique des données

La comparaison automatique de toutes les données relatives aux passagers aériens est limitée dans le temps. Elle doit avoir lieu *immédiatement* après que les données sont parvenues à l'UIP et elle est déclenchée automatiquement (al. 1).

Cette comparaison sert à faire un premier tri des données relatives aux passagers aériens:

- entre celles qui n'ont pas produit de concordance et qui, sous réserve des art. 8 à 11, ne doivent pas être traitées de manière plus approfondie,
- et celles qui ont produit une concordance et doivent par conséquent être examinées plus en détail (al. 2 et 3), et peut-être communiquées à l'autorité compétente pour la suite du traitement (cf. art. 7).

Si cette vérification visée à l'al. 2 est positive, l'UIP communique la concordance et les données relatives aux passagers aériens concernées, c'est-à-dire le résultat de la comparaison automatique, à l'autorité compétente (cf. art. 7) et marque les données communiquées. L'autorité qui reçoit les données de la part de l'UIP décide ensuite des éventuelles mesures.

Les données marquées sont soumises à un délai de conservation de cinq ans. En revanche, les données non marquées sont pseudonymisées au bout d'un mois (cf. art. 18) et effacées automatiquement après cinq mois supplémentaires (cf. art. 21).

Al. 1

Les données relatives aux passagers aériens sont comparées automatiquement dès leur introduction dans le système d'information PNR de l'UIP avec:

- les données des systèmes d'information de police en vertu des art. 15 et 16 de la loi fédérale du 13 juin 2008 sur les systèmes d'information de police de la Confédération (LSIP)[42] et le système d'information de police d'INTERPOL en vertu de l'art. 351 CP[43];

41 En vertu de l'ATF 130 I 369, p. 380, on entend par acte matériel l'acte effectif et informel de l'administration. Il se caractérise notamment par le fait qu'il ne vise pas à produire des effets juridiques mais un résultat, tout en pouvant affecter le statut de particuliers (texte original en allemand).

42 RS **361**

43 RS **311.0**

- les profils de risque en vertu de l'art. 12;
- les listes d'observation en vertu des art. 13 et 14.

Si les contenus d'un ensemble de données relatives aux passagers aériens (cf. annexe 1), tels que le nom, le numéro de téléphone ou l'adresse électronique de la personne, se trouvent également dans l'un des deux systèmes d'information de police ou dans une liste d'observation, la comparaison automatique aboutit à une concordance.

Sont présentés ci-après les deux systèmes d'information de police avec lesquels les données relatives aux passagers aériens sont comparées automatiquement.

Le *système de recherches informatisées de police (RIPOL; cf. art. 15 LSIP)* contient des données sur les personnes signalées aux fins d'arrestation ou de recherche, des informations sur des infractions non élucidées ou sur des personnes impliquées dans une infraction ainsi que d'autres renseignements servant à élucider des infractions. Il aide les autorités compétentes de la Confédération et des cantons 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 visées à l'annexe 2 P-LDPa. 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 recherchées au niveau international ainsi que sur des documents d'identification dérobés ou perdus (let. d et e).

La *partie nationale du Système d'information Schengen (N-SIS; cf. art. 16 LSIP)* 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 N-SIS peut permettre aux autorités compétentes d'arrêter des personnes recherchées au niveau international lorsqu'elles entrent dans le pays ou en sortent.

Les commentaires sur les art. 12 à 14 contiennent de plus amples détails sur les profils de risque et les listes d'observation utilisés pour la comparaison automatique.

Al. 2

Il ne suffit pas d'obtenir une concordance grâce à la comparaison automatique des données dans le système d'information PNR pour qu'il soit justifié de la communiquer à l'autorité compétente et de marquer des données (cf. art. 7, al. 1).

L'UIP doit encore vérifier chaque concordance manuellement pour garantir qu'aucun résultat de traitement

- qui sortirait du cadre des buts admissibles pour le traitement des données (cf. art. 5, al. 1) ou
- qui concernerait la mauvaise personne par exemple en raison d'une erreur lors de la saisie de son nom

ne soit communiqué à une autorité compétente.

Souvent, seule une consultation manuelle des systèmes d'information de police et d'autres systèmes d'information de la Confédération permet de trouver des renseignements supplémentaires et de clarifier ces questions.

Al. 3

L'al. 3 cite les systèmes d'information auxquels l'UIP a le droit d'accéder afin de vérifier les concordances.

Let. a

Si la concordance montre effectivement l'existence d'un élément constitutif de l'infraction visé à l'annexe 2, l'UIP doit clarifier la situation en accédant manuellement aux informations de fond sur les circonstances de l'infraction dans le RIPOL et dans le N-SIS (cf. commentaire de l'art. 1) ainsi que dans les systèmes d'information suivants:

- le *Système national d'enquête* (*SNE*, art. 10 et 11 LSIP) 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. De plus, les informations relatives à la coopération entre la Police judiciaire fédérale (PJF) et les autorités de poursuite pénale, les polices judicaires cantonales ainsi que les autorités étrangères peuvent se révéler utiles dans la lutte contre la criminalité organisée au niveau international.
- le *système de traitement des données relatives à la coopération policière internationale et intercantonale* (*IPAS*, art. 12 LSIP) contient notamment des informations relatives aux enquêtes en cours menées par des autorités de police et de poursuite pénale suisses ou étrangères.
- *l'index national de police* (art. 17 LSIP): ce système comprend des informations de fond sur les signalements des cantons.
- *SIRENE-IT* (en vertu de l'art. 18 LSIP): ce système contient des informations de fond relatives aux signalements contenus dans le Système d'information Schengen dans le domaine de la criminalité organisée et du terrorisme.
- *le système d'information d'INTERPOL* (*I-24/7*, art. 350 à 352 CP): ce système de l'organisation internationale de police criminelle (INTERPOL) contient des informations permettant d'établir les motifs de signalements internationaux.

Let. b

Ce sont avant tout les indications qui ont été fournies sur la personne et sur ses informations de voyage qui sont importantes pour établir l'identité. L'UIP ne doit pas seulement se contenter du RIPOL et du N-SIS, mais doit pouvoir aussi consulter les systèmes d'information suivants:

- *le système national d'information sur les visas* (*ORBIS*, art. 109*b* 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. Une personne peut être identifiée au moyen du numéro de passeport vérifiable.
- *le système d'information central sur la migration* (*SYMIC*, loi fédérale du 20 juin 2003 sur le système d'information commun aux domaines des étrangers et de l'asile [LDEA][44]): le système d'information central sur la migration contient les données personnelles d'étrangers qui se trouvent en Suisse (par ex. nom, prénom, date de naissance) ainsi que leur statut de séjour. Il est désormais possible de consulter dans le SYMIC les données du système d'information relatif à l'établissement de documents d'identité suisses et d'autorisations de retour pour étrangers ISR (ancien art. 111, al. 1, LEI). Il est aussi possible de consulter dans le SYMIC des informations issues de documents de voyage, telles que le nom ou le lieu d'origine d'étrangers enregistrés en Suisse et possédant un document de voyage établi par la Suisse (par ex. un passeport pour réfugié).
- *le système d'information relatif aux documents d'identité* (*ISA*, art. 11 de la loi fédérale du 22 juin 2001 sur les documents d'identité [LDI][45]): ISA est exploité par fedpol et contient les données figurant sur les passeports et les cartes d'identité suisses d'une personne telles que le nom, le lieu d'origine, l'autorité d'établissement et le centre chargé de produire les documents d'identité.

Les concordances obtenues par suite de comparaison automatique qui s'avèrent négatives lors de la vérification par l'UIP doivent être effacées immédiatement (cf. art. 22, let. b). Si la concordance vérifiée est confirmée, l'UIP la transmet ainsi que les données relatives aux passagers aériens concernées à l'autorité compétente puis marque les données concernées (cf. art. 7).

Art. 7 *Communication en cas de concordance vérifiée*

Al. 1

Seules les concordances obtenues dans le cadre de la comparaison automatique qui ont été vérifiées par l'UIP en vertu de l'art. 6, al. 2, et se sont avérées positives peuvent être communiquées à l'autorité compétente visée à l'art. 1,

44 RS **142.51**
45 RS **143.1**

al. 2, accompagnées des données relatives aux passagers aériens concernées, constituant ensemble les résultats de la comparaison automatique.

La destinataire de ces résultats de traitement est l'autorité qui, selon le système d'information, est chargée du signalement déterminant pour obtenir la concordance ou fournit le profil de risque ou la liste d'observation aboutissant à la concordance.

C'est l'art. 22, let. b, qui détermine si la vérification d'une concordance entraîne d'autres suites que la communication à l'autorité compétente. Doivent être effacées immédiatement – au lieu d'être communiquées à une autorité – les concordances

- qui ne peuvent pas ou pas clairement être attribuées à une infraction pénale visée à l'annexe 2 (art. 6, al. 3, let. a) ou
- pour lesquelles l'identité se révèle inexacte (art. 6, al. 3, let. b).

Dans ces cas, la vérification des concordances obtenues par la comparaison automatique donne un résultat négatif, ce qui interdit la communication à une autorité compétente et requiert l'effacement immédiat.

Al. 2

Si c'est l'UIP qui a décidé d'établir un profil de risque (cf. art. 12, al. 2, let. b), il manque une autorité requérante. C'est également le cas si l'UIP doit transmettre des indices sur une infraction susceptible d'être commise (cf. art. 9). Il est aussi possible qu'un signalement ne mentionne exceptionnellement pas d'autorité compétente.

Dans tous ces cas, l'UIP communique les données à l'autorité visée à l'art. 1, al. 2, qui est la plus susceptible d'être compétente pour la suite du traitement. En cas de doute, l'UIP communique les données à la PJF. Si celle-ci ne s'estime pas compétente dans le cas d'espèce, elle transmet les données à l'autorité qu'elle considère compétente. Si la PJF ne trouve aucune autorité compétente, ce qui semble improbable, elle doit elle-même effacer les données. Dès que l'UIP en a pris connaissance, elle supprime le marquage des données concernées conformément à l'art. 10, al. 1.

Al. 3

L'UIP marque *techniquement* les données qui ont été communiquées à une autorité visée à l'art. 1, al. 2, qui sont dès lors considérées comme données marquées dans la présente loi.

Digression sur les données marquées

Dans son arrêt du 21 juin 2022, la CJUE précise sans équivoque que la conservation pendant six mois de toutes les données relatives à des passagers aériens peut se justifier. En revanche, la conservation au-delà de ce délai devrait se limiter au strict nécessaire aux fins d'enquête et de poursuite:

"Dans la mesure où, toutefois, sont identifiés, dans des cas particuliers, des éléments objectifs, tels que les données PNR […] ayant donné lieu à une concordance positive vérifiée, qui permettent de considérer que certains passagers pourraient présenter un risque en matière d'infractions terroristes ou de formes graves de criminalité, un stockage de leurs données PNR paraît admissible au-delà de cette période initiale"[46].

Les données que l'UIP communique à une autorité compétente en vertu de l'art. 7 sont marquées. Cette mesure technique garantit le traitement *automatique* prévu par la loi pour les données

- qui ne présentent pas d'indices de grande criminalité, ne sont par conséquent pas marquées, sont pseudonymisées automatiquement au bout d'un mois puis effacées automatiquement après cinq mois supplémentaires (art. 21, al. 1), et
- qui présentent des indices de grande criminalité, sont par conséquent communiquées à une autorité et marquées, puis sont effacées automatiquement après cinq ans (cf. art. 21, al. 2).

Un marquage est supprimé lorsque l'UIP est informée par l'autorité compétente qu'il n'y a plus besoin des données (cf. art. 10). Cela peut être le cas lorsque les indices qui ont entraîné la communication des données ne sont pas confirmés ou si le soupçon initial contre une personne signalée comme recherchée se révèle infondé. Une fois le marquage supprimé, les données doivent, en fonction de leur date, être soit pseudonymisées puis effacées, soit effacées immédiatement (cf. art. 18 et 21).

Al. 4

Tant les demandes des autorités compétentes adressées à l'UIP que les données communiquées par cette dernière à l'autorité requérante doivent pouvoir être communiquées de manière sécurisée. Le Conseil fédéral est autorisé à régler, au niveau de l'ordonnance, les modalités nécessaires pour ce faire. Il ne s'agit pas seulement de définir la manière de communiquer. Il faut également clarifier la question de savoir si les données doivent être échangées de manière standardisée entre les autorités et par le biais d'un point de contact. Dans le cas des corps de police de la Confédération et des cantons, il pourrait s'agir de la Centrale d'engagement et d'alarme.

Art. 8 Communication sur demande

Cette disposition s'applique uniquement lorsque les données relatives aux passagers aériens qui font l'objet de la demande ne sont *pas* pseudonymisées.

Si les données souhaitées sont pseudonymisées, il faut d'abord demander la levée de la pseudonymisation (cf. art. 19 ou 20).

Al. 1

46 Affaire C-817/19, EU:C:2022:491; ch. marg. 248 à 262

La communication de données visée à l'art. 8 doit être suffisamment concrète et précise. Les demandes d'ordre général qui ne sont pas spécifiques et peuvent produire une pléthore de résultats divers ne sont en revanche pas admises. Cette nuance est apportée par le terme "au cas par cas".

De plus, la demande doit exposer de manière concluante les raisons pour lesquelles les données sollicitées sont nécessaires pour combattre une infraction visée à l'annexe 2 de la présente loi.

Al. 2

L'UIP doit examiner, sur la base de la demande et éventuellement par des renseignements complémentaires recueillis auprès de l'autorité requérante, si les données relatives aux passagers aériens sollicitées sont effectivement en lien avec une infraction visée à l'annexe 2 (cf. art. 7, al. 1).

Les données relatives aux passagers aériens communiquées à la demande d'une autorité compétente doivent être marquées (cf. art. 7, al. 3).

Art. 9 Transmission d'indices

Al. 1

L'UIP peut recevoir de la part d'une UIP étrangère des indices du risque imminent qu'une infraction visée à l'annexe 2 soit commise (cf. art. 30).

L'UIP doit communiquer ces indices à l'autorité compétente (cf. art. 1, al. 2), de sorte que cette dernière puisse effectuer des clarifications plus approfondies et éventuellement mettre en place les mesures indiquées pour prévenir cette infraction.

Al. 2

Parmi les autres informations que l'UIP communique à l'autorité compétente à sa demande se trouvent le dossier passager de la personne concernée par l'indice ainsi que les éventuelles concordances vérifiées obtenues par une comparaison des données de ce dossier en vertu de l'art. 6, al. 1.

Al. 3

En cas d'urgence, l'UIP peut communiquer les informations visées à l'al. 2 immédiatement et sans attendre une demande de l'autorité compétente.

Al. 4

Par analogie avec l'art. 7, l'UIP vérifie notamment si l'indice transmis a effectivement un lien avec une infraction visée à l'annexe 2 (cf. art. 7, al. 1).

Si l'UIP ne peut pas déterminer avec certitude quelle autorité est compétente pour procéder à des clarifications, elle transmet l'indice à la PJF, qui détermine la compétence (cf. art. 7, al. 2).

Une fois les données transmises à l'autorité compétente, c'est l'UIP qui doit procéder à leur marquage (cf. art. 7, al. 3).

Art. 10 Suppression des marquages

L'autorité compétente est en mesure d'examiner le soupçon dont les données communiquées font l'objet dans un cadre bien plus large que l'UIP. Elle peut parvenir à la conclusion que les indices qui ont conduit à la communication des données ne sont pas confirmés ou que le soupçon initial contre une personne signalée comme recherchée se révèle infondé.

Dans ce cas, l'autorité compétente doit informer l'UIP qu'elle n'a plus besoin des données communiquées.

Dès que l'UIP a pris connaissance de cette information, elle doit supprimer le marquage des données concernées. Ces données sont ensuite soumises aux règles s'appliquant aux données non marquées (cf. art. 18 et 21).

Il faudra déterminer au niveau de l'ordonnance une procédure permettant de rappeler aux autorités compétentes leur obligation d'informer prévue à l'art. 10 à intervalles réguliers. Si elles confirment dans un délai fixé par l'UIP (par ex. 10 jours) que la personne concernée fait toujours l'objet de soupçons de grande criminalité, les données restent marquées. En revanche, si l'UIP ne reçoit aucune confirmation, elle supprime le marquage et pseudonymise ou efface les données redevenues non marquées (en fonction de leur date de saisie dans le système). Cette procédure permet d'empêcher que des données soient marquées de manière injustifiée et restent ainsi soumises au délai de conservation de cinq ans.

Art. 11 Communication au SRC

Le SRC joue un rôle particulier dans la lutte contre les infractions terroristes et les autres infractions pénales graves. Sa collecte d'informations précède généralement l'enquête de police et la poursuite pénale, et sert à anticiper et à prévenir les menaces pour la sécurité intérieure ou extérieure.

C'est pourquoi le SRC doit avoir accès aux données brutes relatives à certaines liaisons aériennes en vue de leur traitement, contrairement au service de renseignement de l'armée et aux autorités d'exécution cantonales visés à l'art. 9 LRens, qui n'ont pas ce droit.

Le traitement par le SRC des données relatives aux passagers aériens est régi par la LRens, qui est complétée en conséquence (cf. annexe 3, ch. 1). La loi sur les données relatives aux passagers aériens ne régit que la communication des données et le but du traitement admissible.

Al. 1

L'al. 1 spécifie simplement que le SRC reçoit les données relatives aux passagers aériens sur certaines liaisons aériennes prédéfinies. Ces données lui sont communiquées automatiquement. Cette communication n'entraîne pas de marquage des données concernées.

Al. 2

Le SRC doit pouvoir traiter les données relatives aux passagers aériens en toute autonomie afin d'accomplir ses tâches conformément à l'art. 6, al. 1, let. a, LRens. Il n'est toutefois pas prévu que le SRC se voie octroyer un accès direct au système d'information PNR. Les données lui sont communiquées automatiquement et concernent uniquement les liaisons aériennes prédéfinies par le Conseil fédéral (cf. al. 3).

Le SRC se heurte à une autre restriction pour traiter les données relatives aux passagers aériens conformément à la présente loi: il ne peut traiter ces données que pour lutter contre les infractions pénales visées à l'annexe 2 qui comptent parmi ses tâches prévues à l'art. 6, al. 1, let. a, LRens.

Le nouvel art. 16*a* LRens renvoie explicitement à cette finalité prévue par la présente loi.

L'avant-projet de loi sur les données relatives aux passagers aériens anticipait déjà cette disposition de finalité, qui correspond aussi à l'arrêt de la CJUE (cf. ch. marg. 235). Cette dernière tire encore une autre conclusion:

"Par ailleurs, le caractère exhaustif des finalités […] de la directive PNR implique également que les données PNR ne sauraient être conservées dans une base de données unique pouvant être consultée aux fins de la poursuite tant de ces finalités que d'autres finalités. En effet, la conservation de ces données dans une telle base de données comporterait le risque que lesdites données soient utilisées à des fins autres que celles visées […]".

Il découle de la finalité spécifiée à l'al. 2 qu'il n'est pas non plus possible pour le SRC d'élargir le but du traitement sur le plan technique. Une réglementation supplémentaire n'est donc pas nécessaire dans la loi sur les données relatives aux passagers aériens.

Section 4 Profils de risque et listes d'observation

Art. 12 Profils de risque

Cet article fournit la base légale permettant d'établir un profil de risque et de l'utiliser et contient également une définition de celui-ci.

L'expérience professionnelle éprouvée et l'intuition des collaborateurs des autorités de contrôle permettent aujourd'hui encore de repérer, dans le flux des personnes entrant en Suisse et quittant le pays, certains individus aux antécédents criminels jusqu'alors inconnus des autorités compétentes et de les examiner de plus près, voire de les interroger ou de les arrêter. Toutefois, il convient de considérer ces impressions personnelles lors des contrôles sous un angle critique, d'autant plus que leur motivation est subjective et qu'elles peuvent être inconsciemment une "porte d'entrée" à des discriminations. Par conséquent, et compte tenu du fait que le nombre de personnes passant les points de contrôle a fortement augmenté ces dernières années, il faut à présent davantage recourir à des outils électroniques.

Les profils de risque dans le cadre du PNR sont l'un de ces outils. Tout comme les listes d'observation, ils sont utilisés dans la comparaison automatique visée à l'art. 6 et permettent d'attirer l'attention sur des dossiers passagers présentant des combinaisons de données observées fréquemment en lien avec la grande criminalité.

Dans le cadre du PNR, un profil de risque ne correspond *pas* à un profilage (cf. art. 5, let. f et g, LPD). En effet, la comparaison de données relatives aux passagers aériens avec le profil de risque ne comprend ni une analyse de la personne concernée ni l'anticipation de son comportement.

Les profils de risque sont utilisés pour rechercher certaines données qui se trouvent combinées dans un dossier passager. Une concordance obtenue dans le cadre d'une comparaison confirme uniquement que le dossier passager concerné par cette concordance contient bien la combinaison recherchée au moyen du profil de risque.

En pratique, le développement de profils de risque représente un défi de taille. Les profils de risque ne sont opérants que si, lors de leur conception, un savoir-faire criminalistique est combiné à une expérience éprouvée dans le domaine de la consultation des données.

Toutes les étapes de traitement automatiques doivent être consignées dans un procès-verbal électronique, l'utilisation de profils de risque également (cf. art. 24).

Les profils de risque doivent être effacés lorsqu'ils ne sont plus nécessaires (cf. art. 22, let. d).

L'utilisation de profils de risque est vérifiée par le Conseil fédéral (cf. art. 15).

Al. 1

Certains crimes se traduisent par des combinaisons de données typiques dans les dossiers passagers, par exemple la criminalité organisée et en particulier la traite d'êtres humains. L'utilisation de profils de risque permet de rechercher systématiquement de telles combinaisons dans les dossiers passagers, afin d'obtenir des indices objectifs d'une infraction visée à l'annexe 2 encore inconnue des autorités.

Plusieurs participants à la consultation craignent que les profils de risque puissent présenter des contenus discriminatoires. Cette crainte est infondée. En effet, un profil de risque *n'est pas* composé de données qui se réfèrent à une personne physique identifiée ou identifiable et, par conséquent, il ne contient pas de données personnelles au sens de l'art. 5, let. e, LPD. De même, un profil de risque ne peut en aucun cas contenir des données personnelles sensibles (cf. art. 5, let. c, LPD).

Al. 2

Les profils de risque sont toujours établis par l'UIP.

Un profil de risque peut avoir comme point de départ une demande écrite d'une autorité compétente visée à l'art. 1, al. 2. Celle-ci doit exposer dans sa demande quelles données doivent être intégrées dans le profil de risque et dans quel but.

L'UIP peut toutefois aussi établir des profils de risque sans une telle demande. Dans ce cas, elle se fonde sur les renseignements qu'elle a recueillis au cours du travail quotidien des autorités de police et de poursuite pénale en Suisse et à l'étranger.

Dans les deux cas, l'UIP doit examiner si les contenus demandés sont conformes à la finalité du traitement et suffisamment concrets. Si elle constate que les informations de l'autorité requérante ne sont pas suffisamment concrètes, elle le lui signale puis l'aide à préciser davantage le profil de risque souhaité.

Al. 3

L'établissement de profils de risque pose de grandes exigences techniques. Les expériences faites à l'étranger montrent que les profils de risque débouchent souvent sur un trop grand nombre de concordances.

Cela provient du fait que ces profils ne sont pas suffisamment précis. Dans l'idéal, ils devraient contenir aussi bien des données à charge que des données à décharge.

Obtenir une multitude de concordances qui ne sont pas pertinentes ne devrait pas être le but des profils de risque, que ce soit pour des raisons de protection de données (cf. art. 7, al. 3, LPD) ou pour des raisons d'économie de procédure.

Par conséquent, les profils de risque doivent impérativement être testés avant d'être utilisés. Ces tests sont menés exclusivement au moyen de données générées artificiellement par des simulations.

Al. 4

Seule l'UIP, c'est-à-dire des personnes physiques, peut modifier les données intégrées dans un profil de risque.

Art. 13 Liste d'observation

Cet article fournit la base légale permettant d'établir et d'utiliser une liste d'observation et contient également une définition de celle-ci.

Tout comme les profils de risque, les listes d'observation sont utilisées dans la comparaison automatique de toutes les données relatives aux passagers aériens nouvellement reçues (cf. art. 6, al. 1).

Toutes les étapes de traitement automatiques doivent être consignées dans un procès-verbal électronique, l'utilisation d'une liste d'observation également (cf. art. 24).

L'effacement du contenu d'une liste d'observation visée à l'art. 13 est régi à l'art. 22, let. d.

L'utilisation d'une liste d'observation est vérifiée par le Conseil fédéral (cf. art. 15).

Al. 1

Les listes d'observation visées à l'art. 13 permettent de rechercher de façon directe et ciblée des contenus dans les données relatives aux passagers aériens qui ont un rapport avec des infractions visées à l'annexe 2 déjà *commises* et connues des autorités.

Contrairement aux profils de risque, une liste d'observation est composée uniquement de données qui se réfèrent à une personne physique ou morale identifiée ou identifiable. Cette définition reprend la définition des données personnelles qui était en vigueur en Suisse jusqu'à l'abrogation de la loi fédérale du 19 juin 1992 sur la protection des données[47]. Cet élargissement permet de garantir qu'il est par exemple aussi possible de rechercher des numéros de carte de crédit spécifiques lorsque la carte de crédit appartient à une personne morale plutôt qu'à une personne physique.

La liste d'observation ne contient pas de données personnelles sensibles, car même les données biométriques inscrites dans les documents d'identité ne font pas partie d'un dossier passager au sens de l'annexe 1 (cf. catégorie 18).

Al. 2

Cet alinéa spécifie qui peut solliciter une liste d'observation et quels buts du traitement définis à l'art. 5, al. 1, doivent être respectés pour l'établissement et l'utilisation de la liste d'observation.

Contrairement aux profils de risque, l'UIP n'a le droit d'établir et d'utiliser des listes d'observation qu'à la demande écrite d'une autorité visée à l'art. 1, al. 2, let. a. La tâche de l'UIP se limite à vérifier si les contenus sollicités sont conformes à la finalité du traitement et suffisamment concrets.

La liste d'observation visée à l'art. 13 ne peut être établie et utilisé qu'aux fins suivantes:

- élucider une infraction terroriste ou toute autre infraction pénale grave visée à l'annexe 2 *connue des autorités*, qui fait l'objet d'une procédure d'enquête ou de poursuite pénale en cours (let. a) ou
- rechercher une personne *identifiée* qui est prévenue dans le cadre d'une procédure pénale en cours en lien avec une infraction visée à l'annexe 2 (let. b) ou qui a été condamnée par un jugement entré en force et tente de se soustraire à l'exécution d'une peine privative de liberté (let. c).

Al. 3

Seule l'UIP, c'est-à-dire des personnes physiques, peut établir des listes d'observation et modifier les données utilisées.

47 RO **2022** 491

Art. 14 Intégration de données de tiers dans la liste d'observation

Cet article établit une règle spéciale permettant d'intégrer des données dans une liste d'observation visée à l'art. 13. L'inclusion de données de tiers qui n'ont aucun lien avec une infraction visée à l'annexe 2 permet de rechercher *indirectement* des personnes identifiées qui sont connues des autorités.

Les données de tiers doivent permettre de déterminer le lieu de séjour d'une personne recherchée en lien avec une infraction pénale visée à l'annexe 2. Il doit s'agir d'une personne qui est prévenue dans le cadre d'une procédure pénale en cours ou qui a été condamnée par un jugement entré en force et doit être livrée à une peine privative de liberté pour une infraction visée à l'annexe 2.

L'art. 270 CPP fixe une règle similaire qui autorise la surveillance de la correspondance par poste et télécommunication d'un tiers. Cette mesure représente toutefois une atteinte bien plus forte aux droits de la personnalité des tiers concernés que la mesure prévue au présent article, qui devrait par ailleurs se révéler bien moins coûteuse à mettre en œuvre qu'une mesure en vertu de l'art. 270 CPP. Des tiers peuvent aussi être touchés par une observation en vertu de l'art. 282 CPP.

L'effacement du contenu d'une liste d'observation visée à l'art. 14 est régi par l'art. 22, let. e.

L'utilisation d'une liste d'observation est vérifiée par le Conseil fédéral (cf. art. 15).

Al. 1

La liste d'observation peut intégrer pour une durée limitée les données d'un tiers qui n'a aucun lien direct avec une infraction terroriste ou une autre infraction pénale grave visée à l'annexe 2.

Seule une autorité visée à l'art. 1, al. 2, let. a, peut demander par écrit une liste d'observation en vertu de l'art. 14.

Mais dans le cas présent, la demande doit être adressée au tribunal des mesures de contrainte compétent pour l'autorité requérante. En effet, il n'est possible d'inclure les données d'un tiers dans une liste d'observation que si le tribunal des mesures de contrainte compétent l'approuve.

La liste d'observation a pour but de permettre aux autorités de déterminer, à l'aide du dossier passager d'un tiers, le lieu de séjour d'une personne recherchée en lien avec une infraction pénale visée à l'annexe 2 qui est soit prévenue, soit condamnée par un jugement entré en force et tente de se soustraire à l'exécution d'une peine privative de liberté (art. 13, al. 2, let. b et c).

On entend par tiers au sens de l'art. 14 une personne suffisamment proche de la personne recherchée, que ce soit au plan professionnel ou au plan privé, pour qu'il soit probable qu'elle rende visite à la personne recherchée à son lieu de séjour.

Il faut garder à l'esprit qu'une liste d'observation incluant des contenus visés à l'art. 14 ne peut être opérante que si le tiers et la personne recherchée sont en contact sur place et que le tiers *ou* la personne recherchée se trouve en Suisse. Si les deux personnes se trouvent en Suisse, elles n'ont pas besoin de prendre l'avion et de traverser les frontières pour entretenir le contact. Et si les deux se trouvent à l'étranger, les données du tiers dans une liste d'observation ne servent à rien, car l'UIP suisse ne dispose normalement que des dossiers passagers des vols à destination ou en provenance de la Suisse.

Al. 2

L'inclusion de telles données dans une liste d'observation est soumise à une durée limitée, qui doit également être fixée par le tribunal des mesures de contrainte.

Pour fixer cette durée autorisée, le tribunal des mesures de contrainte adoptera probablement des critères semblables au type de mesures en vertu du CPP.

L'UIP doit effacer les contenus de la liste d'observation à l'expiration de la durée fixée par le tribunal (cf. art. 22, let. e).

Al. 3

Le tribunal des mesures de contrainte communique sa décision à l'autorité requérante et à l'UIP.

Art. 15 Vérification des profils de risque et des listes d'observation

Les profils de risque et les listes d'observation sont des instruments essentiels du PRN. Ils permettent d'obtenir rapidement et sans grand effort des informations qui peuvent être importantes dans la lutte contre la grande criminalité.

Il est ressorti de la consultation qu'il faudrait vérifier l'utilisation de ces deux instruments. Cette vérification portant essentiellement sur la fonctionnalité de ces instruments essentiels du PRN, cette tâche doit être confiée au Conseil fédéral.

Al. 1

L'art. 15 spécifie que l'utilisation de profils de risque et de listes d'observation doit être vérifiée par le Conseil fédéral.

Pour être utilisés, il est impératif que ces instruments soient établis de sorte qu'ils permettent d'atteindre les buts définis par la loi.

Les profils de risque qui génèrent une multitude de concordances inutiles font perdre de vue l'essentiel, en plus de mobiliser beaucoup de ressources inutilement. Les profils de risque insuffisamment précis ne peuvent pas être justifiés par la nécessité.

Il en va de même pour les profils de risque qui ne sont pas fondés sur les schémas de comportement actuels, car ceux-ci changent sans cesse. Si les profils de risque ne sont plus actuels, il n'est plus nécessaire de les utiliser et leur contenu doit être effacé (cf. art. 22, let. d).

L'utilisation de listes d'observation est moins problématique, même si celles-ci peuvent aussi générer beaucoup de concordances inutiles, par exemple lorsque des noms de famille courants sont intégrés sans autres critères permettant de définir la personne recherchée avec plus de précision.

La raison principale pour laquelle des listes d'observation ne sont plus nécessaires pourrait résider dans le fait que la personne recherchée a été retrouvée. L'UIP doit effacer le contenu d'une liste d'observation qui n'est plus nécessaire (cf. art. 22, let. d et e).

Al. 2

Les détails de cette vérification doivent être fixés au niveau de l'ordonnance. La publication d'un rapport, comme certains participants à la consultation l'ont souhaité, n'est toutefois pas considérée comme indiquée. Pour des raisons de protection de la personnalité et des considérations de sécurité, il est préférable de ne pas publier un rapport à forte portée informative.

Section 5 Système d'information PNR

Art. 16

Al. 1

Le traitement des données relatives aux passagers aériens est effectué dans le système d'information PNR. De plus amples détails se trouvent au ch. 6.1.

Al. 2

En tant qu'exploitant du système d'information PNR, fedpol endosse le rôle de responsable du traitement au sens de l'art. 5, let. j, LPD.

fedpol est notamment chargé:

- de concevoir, par des mesures techniques et organisationnelles, le traitement des données de manière à ce qu'il respecte les prescriptions de protection des données (art. 7, al. 1, LPD);
- de garantir, par le biais de préréglages appropriés, que le traitement des données personnelles soit limité au minimum requis pour la finalité poursuivie (art. 7, al. 3, LPD);
- d'assurer, par des mesures organisationnelles et techniques appropriées, une sécurité adéquate des données personnelles par rapport au risque encouru (art. 8, al. 1, LPD);
- de tenir un registre des activités de traitement (Art. 12 LPD);
- de procéder à une analyse d'impact relative à la protection des données personnelles, pour autant que les conditions permettant d'établir une telle analyse soient réunies (art. 22 LPD);
- d'annoncer dans les meilleurs délais au PFPDT les cas de violation de la sécurité des données entraînant vraisemblablement un risque

élevé pour la personnalité ou les droits fondamentaux de la personne concernée (art. 24, al. 1, LPD);

- d'informer la personne concernée de tout cas de violation de la sécurité des données lorsque cela est nécessaire à sa protection ou lorsque le PFPDT l'exige (art. 24, al. 4, LPD).

Par ailleurs, fedpol est tenu:

- d'informer toute personne qui le demande si des données personnelles la concernant sont traitées (art. 25 LPD, sous réserve des restrictions visées à l'art. 26 de la présente loi);
- de remettre à toute personne qui le demande, sous réserve des restrictions prévues à l'art. 29 LPD, les données personnelles traitées de manière automatisée qui la concernent (art. 28 LPD);
- de traiter l'opposition d'une personne concernée à ce que ses données personnelles soient communiquées (art. 37 LPD);
- de traiter les demandes d'une personne concernée en vertu de l'art. 41 LPD.

Les art. 17 à 26 P-LDPa contiennent des dispositions qui précisent en partie ces prescriptions et priment les dispositions générales de la LPD.

Al. 3 et 4

L'accès aux données relatives aux passagers aériens et aux résultats de traitement de ces données est réservé aux collaborateurs qui en ont impérativement besoin pour l'accomplissement de leurs tâches. Le droit d'accès est accordé en premier lieu aux collaborateurs de l'UIP (let. a). Le conseiller à la protection des données de fedpol doit aussi disposer d'un droit d'accès afin d'accomplir ses tâches conformément à la LPD (let. b).

Les personnes qui sont chargées du développement ou de la maintenance du système d'information PNR ou qui apportent un soutien technique doivent également avoir un droit d'accès (let. c). Cette nécessité découle du fait que le traitement de données est défini de manière très large.

En effet, on entend par traitement toute opération relative à des données personnelles, quels que soient les moyens et procédés utilisés (cf. art. 5, let. d, LPD). Le support des utilisateurs peut par conséquent déjà donner lieu à un traitement de données. S'agissant des questions techniques, seuls les prestataires qui ont obtenu le marché public dans le cadre de l'appel d'offres OMC Alpin 2.0 interviennent dans le traitement PNR. Alpin 2.0 garantit un pool de prestations en faveur de toute l'administration fédérale en matière de projets clés TIC, de grands projets TIC ou de projets complexes et stratégiques. Les mandats concrets sont attribués aux adjudicataires par des processus électroniques mini-tenders (mise au concours). Tous les prestataires choisis pour intervenir doivent en outre passer avec succès le contrôle de sécurité relatif aux personnes de la Confédération.

L'exploitation et la maintenance du système d'information PNR relèvent de la responsabilité du Centre de services informatiques du DFJP (CSI-DFJP) et de ses collaborateurs. Il n'est pas fait appel à des prestataires externes pour l'exploitation et la maintenance de la solution.

Enfin, selon la let. d, les autorités compétentes (cf. art. 1, al. 2) doivent aussi pouvoir accéder au système d'information PNR afin de recevoir et de traiter les données qui leur sont communiquées par l'UIP. L'accès est limité au "prélèvement" de ces données.

Section 6 Protection des données

Art. 17 Principes

Les données relatives aux passagers aériens sont traitées non seulement par l'UIP, mais aussi par les autorités de la Confédération et des cantons auxquelles ces données sont communiquées.

La consultation a souligné la nécessité de préciser dans la loi que le traitement des données est régi par des bases légales de protection des données différentes selon l'autorité compétente.

Une première étape consiste à déterminer s'il s'agit d'une autorité de la Confédération ou d'un canton et, par conséquent, si c'est le droit fédéral ou le droit cantonal qui s'applique. Les autorités de poursuite pénale constituent cependant un cas à part (cf. commentaire de l'al. 2).

La deuxième étape consiste à vérifier s'il existe des dispositions particulières fédérales ou cantonales s'appliquant à l'autorité concernée qui priment le droit général de la protection des données fédéral ou cantonal.

Al. 1

Dans son 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[48], le Conseil fédéral expose:

"Pour le reste, le P-LPD reste, à l'instar de la LPD, une législation générale sur la protection des données. Par conséquent, si des traitements de données personnelles sont régis par des dispositions de protection des données prévues dans d'autres lois fédérales, celles-ci sont en principe applicables en vertu du principe de la priorité des dispositions spéciales sur les dispositions générales."

L'UIP étant une autorité de la Confédération, elle est tenue de respecter la LPD lors du traitement des données pour autant que la présente loi ne prévoie pas de dispositions particulières. Or, les dispositions de la présente loi relatives à la protection des données, notamment les art. 17 à 26, s'apparentent à des dispositions spéciales et priment donc la LPD.

48 FF **2017** 6565 6631

Al. 2

Les dispositions en matière de protection des données prévues dans le P-LDPa ne s'appliquent pas aux autorités qui reçoivent des données de l'UIP au sens de la présente loi. Selon l'autorité concernée, les dispositions de la LPD ne s'appliquent pas non plus.

Autorités de poursuite pénale fédérales et cantonales: dans les procédures pendantes, la protection des données devant être garantie est définie par le droit de procédure applicable et notamment par les art. 95 à 103 CPP. Le droit fédéral et cantonal sur la protection des données s'applique à nouveau seulement une fois que la procédure est clôturée (cf. art. 99, al. 1, CPP). Il s'applique également aux procédures administratives de première instance (cf. art. 2, al. 3, LPD). Dans son message précité, le Conseil fédéral précise à ce sujet[49]:

"Aux termes de l'art. 2, al. 3, P-LPD, les traitements de données personnelles effectués dans le cadre de procédures devant des tribunaux ou dans le cadre de procédures régies par les dispositions de la procédure fédérale, ainsi que les droits des personnes concernées, obéissent au droit de procédure applicable. La norme règle le rapport entre la LPD et le droit de procédure, et fixe comme principe général que seul le droit de procédure applicable détermine d'une part la manière dont les données personnelles sont traitées dans les procédures et d'autre part les droits des personnes concernées. Le droit de procédure garantit également la protection de la personnalité et des droits fondamentaux de toutes les personnes impliquées, offrant ainsi une protection équivalente à celle de la LPD. Si la LPD s'appliquait dans ce domaine, on serait confronté à un risque de conflits de normes et de contradictions, qui pourrait perturber le la bonne application des règles de procédure."

Autorités de police de la Confédération en dehors d'une procédure de poursuite pénale: la protection des données est déterminée par la LPD, pour autant que le droit fédéral ne prévoie pas de dispositions spéciales. De telles dispositions sont présentes dans la LSIP, la LMSI et l'ordonnance du 30 novembre 2001 concernant l'exécution de tâches de police judiciaire au sein de l'Office fédéral de la police[50].

Autorités de police des cantons en dehors d'une procédure de poursuite pénale: la protection des données est déterminée par la loi cantonale sur la protection des données pour autant que des dispositions spéciales cantonales ne priment pas.

SRC: les art. 44 à 67 LRens priment les dispositions de la LPD.

Organes d'exécution cantonaux visés à l'art. 9 LRens: lorsque ces autorités cantonales travaillent comme des autorités d'exécution cantonales au sens de l'art. 46, al. 1, LRens, elles sont soumises au droit fédéral de protection des données, pour autant que des dispositions particulières de la LRens ne priment pas. En revanche, lorsque les services de renseignement cantonaux travaillent

49 FF **2017** 6565 6633 s.
50 RS **360.1**

dans leur propre domaine de compétence cantonal, la protection des données à garantir est celle définie dans le droit cantonal.

Art. 18 Pseudonymisation des données relatives aux passagers aériens

Lors de la pseudonymisation, les données qui permettent d'identifier une personne concrète sont remplacées par des indications neutres (pseudonyme). Un tableau de concordances spécifie le pseudonyme correspondant aux données d'identification. Ce tableau doit être enregistré ailleurs que dans le système d'information PNR. Aussi longtemps que ce tableau existe et qu'il est accessible aux personnes autorisées, la pseudonymisation peut être annulée (cf. art. 19 et 20).

Dans le cadre de la consultation, plusieurs participants se sont référés à l'arrêt de la CJUE pour demander de raccourcir considérablement la durée de conservation des données qu'il n'est pas nécessaire de garder plus longtemps.

Ainsi, il est demandé implicitement que dans tout le champ d'application du PNR, une distinction soit faite entre les données qui contiennent des éléments objectifs indiquant que certaines personnes pourraient représenter un danger dans le domaine des infractions terroristes ou de la grande criminalité ("données marquées"), et les données ne contenant pas de tels éléments (autres données relatives aux passagers aériens). La présente loi prévoit d'appliquer des règles différentes aux unes et aux autres.

L'une de ces règles est la pseudonymisation. Doivent être pseudonymisées au sens de l'art. 18 uniquement les données qui n'ont pas été communiquées à une autorité compétente et ne sont par conséquent pas marquées en vertu de l'art. 7, al. 3. De même, les données dont le marquage a été supprimé par la suite (cf. art. 11) doivent être pseudonymisées un mois après leur introduction dans le système d'information PNR.

Selon le message relatif à la nouvelle loi sur la protection des données précité, la pseudonymisation est considérée comme une mesure technique appropriée pour assurer la sécurité des données personnelles (cf. art. 8 LPD)[51]. 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."

La pseudonymisation consiste à attribuer un pseudonyme aux données d'un dossier passager qui donnent des renseignements sur la personne physique concernée. Une fois pseudonymisées, les données concernées ne peuvent plus

51 FF **2017** 6650

être associées à une personne identifiée ou identifiable, si bien qu'elles perdent leur statut de données personnelles.

Dans son message, le Conseil fédéral écrit encore que pseudonymiser les données est l'une des mesures techniques devant permettre "d'éviter toute violation de la sécurité des données, soit toute violation de la sécurité entraînant la perte de données personnelles, leur modification, leur effacement ou leur destruction, leur divulgation ou un accès non autorisé à ces données, et ce indépendamment de la question de savoir si la violation est intentionnelle ou non, licite ou illicite"[52].

Un dossier passager contient les données personnelles au sens de l'art. 5, let. a, LPD (cf. annexe 1 de la présente loi) suivantes:

- prénom(s) et nom(s) du passager ainsi que prénom(s) et nom(s) des autres voyageurs figurant dans le dossier passager (catégories 4 et 17);
- adresse et coordonnées (catégorie 5);
- détails sur les cartes de crédit utilisées et adresse de facturation du billet d'avion (catégorie 6);
- programme "grands voyageurs" (catégorie 8);
- nom de la personne responsable du dossier à l'agence de voyage qui a effectué la réservation du billet d'avion (catégorie 9);
- toutes les informations disponibles sur les personnes non accompagnées de moins de 18 ans, telles que le nom, le sexe, l'âge, les langues parlées, le nom et les coordonnées de la personne présente au départ et son lien avec la personne mineure, le nom et les coordonnées de la personne présente à l'arrivée et son lien avec la personne mineure, l'agent présent au départ et l'agent présent à l'arrivée (catégorie 12);
- les données API (cf. art. 104, al. 3, LEI), qui sont aussi des données personnelles: (a) l'identité des passagers (nom, prénom, sexe, date de naissance, nationalité); (b) le numéro, l'État émetteur, le type et la date d'échéance du document de voyage utilisé; (c) le numéro, l'État émetteur, le type et la date d'échéance du visa ou du titre de séjour utilisé, pour autant que l'entreprise de transport aérien dispose de ces données (catégorie 18);
- modifications ultérieures des données personnelles figurant dans le dossier passager.

Les données personnelles faisant partie de ces catégories de données doivent être pseudonymisées.

52 FF **2017** 6650

Contrairement à l'anonymisation, la pseudonymisation peut être levée à certaines conditions.

Les données qui présentent des indices objectifs de grande criminalité, qui ont été communiquées à une autorité compétente au sens de l'art. 1, al. 2, en vue de clarifications et qui ont par conséquent été marquées par l'UIP (cf. art.7) ne doivent en revanche *pas* être pseudonymisées.

Al. 1

Les données relatives aux passagers aériens qui ne livrent *pas* d'indice de grande criminalité et qui n'ont par conséquent pas été communiquées à une autorité visée à l'art. 1, al. 2, n'ont pas de marquage (cf. art. 7, al. 3). Elles sont pseudonymisées automatiquement un mois après leur introduction dans le système d'information PNR et ne peuvent donc plus être attribuées au passager aérien concerné.

Les données marquées ne sont en revanche pas pseudonymisées.

Al. 2

Si l'autorité compétente constate qu'elle n'a plus besoin des données pour sa procédure, elle doit en informer l'UIP, qui supprime alors le marquage des données concernées (cf. art. 10, al. 2).

Une fois le marquage supprimé, ces données

- *doivent être pseudonymisées* par l'UIP, pour autant que le vol associé aux données ait eu lieu entre un et six mois auparavant;
- *doivent être effacées* par l'UIP, pour autant que le vol ait eu lieu plus de six mois auparavant (cf. art. 21, al. 2).

Art. 19 Levée ordinaire de la pseudonymisation

Seules les données personnelles d'un dossier passager non marquées ou dont le marquage a été supprimé par la suite sont pseudonymisées (cf. art. 18, al. 2).

Malgré la comparaison automatique des données relatives aux passagers aériens prévue à l'art. 6 et la vérification manuelle qui s'ensuit, le délai d'un mois avant la pseudonymisation s'avère toutefois très court. Il doit donc être possible de consulter la base de données du système d'information PNR même si les données datent de plus d'un mois et que, n'étant pas marquées, elles ont été pseudonymisées. Compte tenu de ces requêtes effectuées dans l'historique, il faut que la pseudonymisation puisse être levée en cas de besoin.

Cet article établit que la pseudonymisation peut être levée seulement si le TAF considère que les conditions légales pour ce faire sont remplies et qu'il approuve cette étape de traitement.

Du point de vue technique, il a été fait en sorte que la levée de la pseudonymisation approuvée par le tribunal ne peut être exécutée que si:

- l'opération est effectuée par une personne habilitée à le faire, *et*
- l'arrêt du TAF est mentionné ou suffisamment référencé d'une autre manière.

Cette étape est inscrite au procès-verbal, de sorte qu'il est possible de vérifier ultérieurement si la pseudonymisation a été levée conformément au droit (cf. art. 24).

Conformément aux art. 19 et 20, la pseudonymisation doit être levée lorsqu'une autorité compétente le demande.

Si une demande d'accès de la personne concernée au sens de l'art. 26, al. 1, nécessite une levée de la pseudonymisation, cette étape peut être effectuée *non pas* en vertu des dispositions susmentionnées ni sur la base d'un arrêt du TAF, mais conformément à l'art. 25, al. 2, let. b, LPD, qui dispose que la personne concernée doit recevoir "les données personnelles traitées en tant que telles" dans l'accès octroyé.

Toutefois, la levée de la pseudonymisation doit également être consignée dans un procès-verbal sur la base de la demande d'accès (cf. art. 24). Celle-ci doit être mentionnée ou suffisamment référencée d'une autre manière dans le procès-verbal. Les modalités seront réglées en détail au niveau de l'ordonnance.

Al. 1

Les autorités visées à l'art. 1, al. 2, peuvent demander à l'UIP la levée de la pseudonymisation.

Al. 2 et 3

Dans un premier temps, l'UIP vérifie si la demande est suffisamment motivée.

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 précise. Dans des cas exceptionnels et dûment motivés, il peut également s'agir d'un vol dans son intégralité;
- s'il est rendu vraisemblable que la levée de la pseudonymisation fournit des informations déterminantes à des fins de lutte contre une infraction spécifique visée à l'annexe 2 de la loi sur les données relatives aux passagers aériens. Les informations requises doivent être décrites avec la plus grande précision possible.

Si la demande n'est pas motivée ou ne l'est pas suffisamment, l'UIP en informe l'autorité requérante, qui a la possibilité de compléter sa demande (al. 3).

L'UIP recommande la levée de la pseudonymisation lorsque cela permet d'obtenir sur le plan technique les informations recherchées. Il n'est pas possible d'obtenir sur le plan technique des informations ne pouvant pas figurer dans un dossier passager, ni des données datant de plus de six mois. De telles

données ont déjà été effacées (car non marquées) ou n'ont pas été pseudonymisées (car marquées).

Si la demande est suffisamment fondée, l'UIP la transmet au TAF assortie de sa recommandation.

Al. 4 et 5

Le TAF statue sur l'éventuelle levée de la pseudonymisation. Les droits allemand[53] et autrichien[54] prévoient eux aussi 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. Ce délai maximum ne dispense pas pour autant le tribunal de statuer aussi rapidement que possible en fonction de la gravité du soupçon.

La décision est définitive. Les recours auprès du Tribunal fédéral contre les décisions concernant la sûreté intérieure ou extérieure de la Suisse sont irrecevables conformément à l'art. 83, let. a, de la loi du 17 juin 2005 sur le Tribunal fédéral[55].

Al. 6

Le TAF notifie son arrêt aussi bien à l'UIP qu'à l'autorité requérante.

Art. 20 Levée de la pseudonymisation en cas d'urgence

Cette procédure en cas d'urgence démontrée se fonde sur l'art. 31 LRens.

Dans un cas d'urgence, le directeur de fedpol doit pouvoir ordonner provisoirement la levée de la pseudonymisation. Il en informe ensuite *sans délai* le chef du DFJP, qui peut faire suspendre la levée de la pseudonymisation (cf. art. 31, al. 1, LRens).

Le chef du DFJP peut être amené à le faire uniquement si l'urgence est discutable. La décision de suspension exige d'annuler toutes les étapes visant à lever la pseudonymisation déjà effectuées et d'attendre que le TAF rende son arrêt.

Le TAF statue sur la demande du directeur de fedpol dans un délai de trois jours ouvrables (cf. art. 31, al. 2 et 3, LRens).

Si le TAF rend une décision négative, toutes les étapes effectuées par suite de la décision provisoire ordonnée par le directeur de fedpol doivent être entièrement annulées.

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

54 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

55 RS **173.110**

Art. 21 *Durée de conservation et effacement des données relatives aux passagers aériens*

Cet article ne concerne que les données relatives aux passagers aériens et règle leur effacement et donc indirectement leur durée de conservation.

L'effacement de toutes les autres données résultant du traitement effectué par l'UIP ou liées à ce traitement est régi par l'art. 22. L'effacement des procès-verbaux constitue une exception (cf. art. 24, al. 4).

Sont effacées au sens de la présente loi les données et les informations qui ont été effacées irrévocablement et ne peuvent plus être rétablies. Il s'agit d'une procédure automatique par laquelle l'espace de stockage est écrasé plusieurs fois de suite.

Dans son arrêt du 21 juin 2022, la CJUE précise sans équivoque que la conservation pendant six mois de toutes les données relatives à des passagers aériens *peut se justifier*.

En revanche, la conservation au-delà de ce délai devrait se limiter au strict nécessaire aux fins d'enquête et de poursuite:

"Dans la mesure où, toutefois, sont identifiés, dans des cas particuliers, des éléments objectifs, tels que les données PNR […] ayant donné lieu à une concordance positive vérifiée, qui permettent de considérer que certains passagers pourraient présenter un risque en matière d'infractions terroristes ou de formes graves de criminalité, un stockage de leurs données PNR paraît admissible au-delà de cette période initiale"[56].

Plusieurs participants à la consultation se sont ralliés à ce point de vue, invoquant parfois l'arrêt cité dans leurs prises de position.

L'art. 21 prévoit ainsi différentes durées de conservation en fonction des données:

- pour les données non marquées: six mois;
- pour les données marquées qui ont plus de six mois: jusqu'à la suppression du marquage et cinq ans au maximum après leur introduction dans le système d'information PNR.

Cette règlementation indirecte permet également d'établir que les durées de conservation autorisées sont des délais absolus.

Al. 1

Une durée de conservation de six mois s'applique à toutes les données relatives à des passagers aériens qui ne sont pas marquées. Celles-ci sont ensuite effacées automatiquement au bout de six mois.

Al. 2

56 Affaire C-817/19, EU:C:2022:491; ch. marg. 259

Les données relatives à des passagers aériens marquées peuvent être conservées pendant cinq ans, puis sont ensuite également effacées automatiquement.

Si le marquage est supprimé avant l'expiration du délai de conservation autorisé pour les données marquées, l'UIP doit alors, en fonction de leur date d'introduction dans le système d'information PNR, pseudonymiser ou effacer immédiatement ces données qui deviennent à nouveau des données non marquées (cf. commentaire de l'art. 18, al. 2).

Art. 22 Effacement de données supplémentaires

Contrairement à l'art. 21, qui règle l'effacement des données relatives aux passagers aériens, l'art. 22 vise les données supplémentaires susceptibles d'être générées lors du traitement des données relatives aux passagers aériens conformément à la présente loi.

L'effacement a lieu "sans délai" 'après prise de connaissance des circonstances qui en sont la cause.

Sont effacées au sens de la présente loi les données et les informations qui ont été effacées irrévocablement et ne peuvent plus être rétablies. Il s'agit d'une procédure automatique par laquelle l'espace de stockage est écrasé plusieurs fois de suite.

Let. a

En vertu de l'art. 5, al. 2, l'UIP ne peut traiter que les données biométriques et les données sur les poursuites ou sanctions pénales ou administratives. Elle doit effacer sans délai toute autre donnée sensible.

Let. b

Toute concordance obtenue par suite de la comparaison automatique des données doit être vérifiée manuellement avant d'être communiquée à une autorité compétente (cf. art. 6, al. 2).

La let. b définit les conditions auxquelles les concordances vérifiées ne doivent pas être communiquées, mais effacées sans délai.

D'une part, la concordance obtenue doit être effacée si elle ne peut pas clairement être attribuée à une infraction pénale visée à l'annexe 2 (cf. ch. 1). D'autre part, elle doit être effacée si la personne recherchée et le passager aérien ne sont pas identiques (cf. ch. 2).

Let. c

Les données relatives aux passagers aériens qui ont été communiquées à une autorité conformément à l'art. 1, al. 2, et ont donc été marquées, sont effacées automatiquement après un délai de cinq ans, à moins que leur marquage n'ait été supprimé de façon anticipée (cf. art. 21, al. 2).

La let. c établit que les données ayant été communiquées à l'autorité compétente en même temps que les données relatives aux passagers aériens doivent être effacées dès lors que ces dernières ont été supprimées.

Let. d

Les profils de risque et les listes d'observation contiennent des données qui ne sont pas effacées en vertu de l'art. 21. Celles-ci doivent être effacées conformément à l'art. 22, let. d, dès qu'elles ne sont plus nécessaires.

Let. e

Les données saisies dans une liste d'observation conformément à l'art. 14 constituent un cas particulier. Elles doivent être effacées après l'expiration du délai fixé par le tribunal des mesures de contrainte (cf. art. 14, al. 2). Si elles ne sont plus nécessaires avant ce délai, ces données doivent être effacées comme prévu à la let. d.

Art. 23 Traitement de données anonymisées

Les données sont considérées comme anonymisées lorsqu'elles ne peuvent plus être attribuées à une personne identifiée ou identifiable et que cette perte du statut de données personnelles est irrévocable.

L'anonymisation fait *irrévocablement* perdre aux données leur statut de données personnelles (cf. art. 5, let. a, LPD). Ce caractère irrévocable est ce qui distingue l'anonymisation de la pseudonymisation. Cette dernière peut être levée à certaines conditions (cf. art. 19 et 20), si bien que les données peuvent à nouveau être attribuées à une personne identifiée ou identifiable.

L'UIP peut traiter des données anonymisées à des fins statistiques. Elle peut également les proposer aux Archives fédérales (cf. art. 6 de la loi fédérale du 26 juin 1998 sur l'archivage[57]).

Art. 24 Journalisation du traitement de données

Al. 1

Les étapes de traitement qui doivent impérativement être consignées dans un procès-verbal sont définies à l'art. 4, al. 2, OPDo: "lors du traitement automatisé de données personnelles, [il convient de journaliser] au moins l'enregistrement, la modification, la lecture, la communication, l'effacement et la destruction des données".

Le droit suisse de la protection des données ne fournit pas de définition juridique du terme *automatisé*. Selon les informations écrites transmises par l'OFJ le 23 novembre 2022, *automatisé* peut être décrit comme la contrepartie de *manuel*. "Alors que le traitement manuel des données implique l'action d'une personne, le traitement automatisé est effectué par un *automate*". Il s'agit là d'une "machine dont la commande mécanique ou électronique a pour effet que les opérations qu'elle exécute de façon autonome produisent un résultat qui dépend d'une tâche préalable [traduction libre de l'allemand]".

57 RS **152.1**

L'OFJ souligne toutefois que l'obligation de journaliser le traitement des données s'applique également "lorsque certaines étapes de travail sont effectuées manuellement". Il précise que la journalisation devrait avoir lieu notamment "lorsqu'il n'est pas possible d'établir a posteriori si les données ont été traitées dans le but pour lequel elles avaient été collectées ou communiquées".

En vertu de l'art. 4, al. 4, OPDo, les procès-verbaux doivent fournir des informations sur:

- l'identité de la personne qui a effectué le traitement;
- la nature du traitement;
- la date et l'heure du traitement;
- l'identité du destinataire des données.

Ces procès-verbaux permettent ainsi de vérifier ultérieurement tout traitement de données personnelles.

Al. 2 et 3

L'al. 2 fixe les buts poursuivis par la journalisation[58]. L'énumération exhaustive exclut l'utilisation de la journalisation pour surveiller des collaborateurs. Les autorisations d'accès octroyées à l'al. 3 vont également dans ce sens.

Al. 4

Les procès-verbaux sont établis automatiquement et doivent être conservés en dehors du système d'information PNR. Il s'agit ainsi de garantir que les procès-verbaux ne soient pas manipulés et restent en sécurité, même en cas de cyberattaque. Il est prévu d'enregistrer les procès-verbaux sur l'infrastructure du CSI-DFJP.

Il est précisé dans le rapport explicatif susmentionné concernant l'OPDo que les procès-verbaux devront être conservés durant un an (cf. art. 4, al. 5, OPDo). "Cette durée minimale ne permet cependant pas de conserver les procès-verbaux pendant une durée excessive. La durée de conservation doit en effet être proportionnée à la finalité de sécurité des données[59].

La présente loi prévoit que les procès-verbaux portant sur le traitement automatisé des données relatives aux passagers aériens sont disponibles un an de plus que les données dont le traitement a été consigné dans ces procès-verbaux. Ils doivent ensuite être effacés.

Jusqu'à leur effacement, les procès-verbaux sont disponibles à des fins de contrôle et de surveillance, mais toutefois pas pour l'UIP.

58 Rapport explicatif de l'Office fédéral de la justice du 31 août 2022 relatif à l'ordonnance sur la protection des données, p. 27, disponible sur https://www.bj.admin.ch/bj/fr/home.html > Etat & Citoyen > Protection des données > Nouveau droit de la protection des données > 1. Etapes préalables, 2022 – Adoption des nouvelles ordonnances (OPDo et OCPD)

59 Ibid., pp. 27 et 28

Art. 25 Surveillance

Le conseiller à la protection des données de fedpol veille, de façon indépendante et sans être soumis à aucun pouvoir d'instruction, au respect des dispositions en matière de protection des données au sein de l'office (cf. art. 26, al. 1 et 2, OPDo). Il exerce également cette tâche vis-à-vis de l'UIP.

Le conseiller à la protection des données est en outre l'interlocuteur du PFPDT (art. 28 OPDo).

fedpol a les obligations ci-après à l'égard du conseiller à la protection des données: lui fournir l'accès à tous les renseignements, documents, registres des activités de traitement et données personnelles dont il a besoin pour accomplir ses tâches et lui annoncer les éventuelles violations de la sécurité des données.

Malgré la fonction de soutien et de contrôle[60] qui revient au conseiller à la protection des données, c'est le PFPDT qui est chargé effectivement de la surveillance.

Ni le conseiller à la protection des données ni le PFPDT ne sont responsables de la conformité du traitement des données personnelles aux règles de la protection des données. Cette responsabilité n'incombe qu'à fedpol, selon le message concernant la nouvelle loi sur la protection des données[61].

Art. 26 Droit d'accès

Les entreprises de transport aérien doivent informer les passagers, lors de la réservation de leur billet d'avion, du traitement de leur données conformément à la présente loi (cf. art. 4).

Grâce aux informations fournies par les entreprises de transport aérien, les personnes concernées peuvent exercer leur droit d'accès en vertu de l'art. 26. Elles peuvent adresser à fedpol une demande d'accès.

Il convient de distinguer deux types de droits d'accès:

- *le droit d'accès direct* (al. 1), qui s'applique aux données ne datant pas de plus de six mois et découle des art. 25 à 28 LPD;
- *le droit d'accès indirect* (al. 2), qui s'applique aux données datant de plus de six mois et est régi par analogie par l'art. 8 LSIP.

Cette double approche selon la date des données s'explique par le fait qu'après six mois, seules sont conservées les données relatives aux passagers aériens marquées, qui se trouvent en cours de traitement auprès de l'autorité compétente. Pouvoir accéder aux données d'un vol en cours de traitement alors

60 Rapport explicatif de l'Office fédéral de la justice du 31 août 2022 relatif à l'ordonnance sur la protection des données, p. 18, ch. 4.7, disponible sur https://www.bj.admin.ch/bj/fr/home.html > Etat & Citoyen > Protection des données > Nouveau droit de la protection des données > 1. Etapes préalables, 2022 – Adoption des nouvelles ordonnances (OPDo et OCPD)

61 FF **2017** 6565 6652

qu'elles datent de plus de six mois indique au requérant qu'une procédure est en cours et que des soupçons pèsent sur sa personne.

Fournir cette information peut nuire considérablement aux procédures préliminaires et aux procédures d'enquête en cours.

L'art. 26, al. 2, let. b, LPD prévoit certes, dans de tels cas, la possibilité de refuser, de restreindre ou de différer la communication des renseignements. Selon cette même loi, un autre renseignement devrait en revanche être fourni à la grande majorité des passagers du même vol, à savoir que leurs données ne sont pas ou plus traitées, car elles ont déjà été effacées en vertu de l'art. 21, al. 1.

S'agissant des données relatives aux passagers aériens, le fait de refuser, restreindre ou différer la communication des renseignements en vertu de l'art. 26, al. 2, let. b, LPD signifie que les données en question sont encore traitées après l'expiration du délai de six mois. La personne concernée pourrait l'en déduire. En effet, les données relatives aux passagers aériens ne peuvent être traitées au-delà de six mois que si elles ont été marquées et donc communiquées par une autorité compétente.

Afin d'éviter cette information indésirable, la loi sur les données relatives aux passagers aériens renvoie au droit d'accès indirect prévu à l'art. 8 LSIP.

Dans de tels cas, qu'il dispose ou non de données, fedpol donne toujours la même réponse: l'obligation de renseigner est reportée. Le requérant peut toutefois exiger du PFPDT qu'il vérifie si les éventuelles données le concernant sont traitées licitement.

Le PFPDT procède à la vérification si des indices suffisants font penser qu'un traitement des données pourrait être contraire à des dispositions de protection des données (art. 49, al. 1, LPD). Il informe ensuite le requérant des démarches entreprises et du résultat d'une éventuelle enquête.

Cette information, élémentaire pour le requérant, n'est refusée à personne, même dans le cadre du droit d'accès indirect prévu à l'art. 8 LSIP, donc pas non plus aux passagers dont les données sont marquées auprès de l'UIP et traitées par une autorité compétente au sens de l'art. 1, al. 2.

Indépendamment de cela, fedpol doit accorder l'accès au requérant une fois que les intérêts au maintien du secret ne sont plus d'actualité et au plus tard après expiration de la durée maximale de conservation autorisée de cinq ans. Les personnes au sujet desquelles aucune donnée n'a été traitée en sont informées par fedpol trois ans après réception de leur demande (cf. art. 8, al. 6, LSIP).

Section 7 Organisation et personnel de l'UIP

Art. 27 Organisation

Al.1

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 aura indubitablement une répercussion positive sur la mise en place et l'exploitation du système d'information PNR.

Al. 2

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. Il est également indiqué explicitement que le personnel doit être distinct, ce qui exclut que des collaborateurs puissent travailler simultanément au sein de l'UIP et d'une autorité chargée d'enquêtes ou de poursuites pénales.

Cela permet d'éviter que ces autorités obtiennent de façon informelle un accès privilégié à des informations détenues par l'UIP. Toutes les autorités compétentes visées à l'art. 1, al. 2, qu'elles soient fédérales ou cantonales, sont ainsi soumises aux mêmes conditions pour obtenir des données de l'UIP.

S'agissant du PNR, l'UIP, rattachée à fedpol, doit être le point de contact unique (*single point of contact*) tant pour les entreprises de transport aérien que pour les UIP étrangères.

L'UIP pourra si nécessaire assurer un service permanent, afin de pouvoir vérifier à temps également les données relatives aux passagers aériens arrivant pendant les heures creuses.

Art. 28 Personnel

L'UIP doit se composer à parts égales de collaborateurs de la Confédération et des cantons. C'est en détachant des collaborateurs que les cantons participent aux frais de l'UIP. Il n'est pas prévu qu'ils apportent une participation supplémentaire.

Étant donné que les collaborateurs cantonaux sont intégrés *temporairement* dans l'exploitation de l'UIP sans qu'il soit mis fin à leur rapport de travail auprès du canton, ce modèle de collaboration se rapproche le plus d'une véritable mise à disposition de travailleurs à titre principal (travail en régie), qui est un type de location de services. Le Conseil fédéral écrit à ce sujet dans le message du 27 novembre 1985 concernant la révision de la loi fédérale sur le service de l'emploi et la location de services[62]:

"Le travailleur n'exécute pas la prestation due dans l'entreprise de son employeur, mais le fait au dehors, dans une entreprise tierce. Cela a pour conséquence une division des fonctions d'employeur: le droit de donner des instructions d'ordre technique touchant des objectifs visés, ou concernant le comportement du travailleur[,] passe à l'entreprise tierce; c'est également le cas du droit à la sauvegarde des intérêts et du secret, de même que, cela va

62 FF **1985** III 524 533 s.

sans dire, du devoir d'assistance sociale incombant à l'employeur. Les autres droits et obligations découlant du contrat de travail continuent d'être assumés par le bailleur de services, notamment l'obligation de payer le salaire et le devoir général d'assistance sociale."

Ces considérations s'appliquent par analogie également au détachement de collaborateurs auprès de l'UIP.

La Confédération et les cantons doivent régler les détails du détachement par convention.

Le commentaire bâlois de la Constitution fédérale (Cst.)[63] 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 sont 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 [traduction libre][64]".

L'art. 28 constitue la base légale de la convention que la Confédération et les cantons doivent conclure et définit notamment:

- le but et l'étendue du détachement (al. 1);
- le financement (al. 2); et
- les dispositions spéciales importantes en matière de droit du personnel (al. 3 et 4).

L'al. 5 s'entend comme une norme de délégation et habilite le Conseil fédéral à régler les détails susmentionnés dans la convention avec les cantons.

Demeure pour l'instant ouverte la question de savoir si les cantons règlent entre eux leur participation respective dans le cadre d'un concordat ou d'une autre façon. Elle n'a pas besoin d'être réglée par le droit fédéral.

Al. 1

Compte tenu du système fédéral de la Suisse, le travail de police et la poursuite pénale relèvent généralement de la compétence première des cantons. En revanche, la Confédération assume la poursuite de certaines infractions pénales graves, telles que le terrorisme ou le crime organisé, et 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[65], sur la transplantation[66] ou sur les armes[67].

63 RS **101**
64 Waldmann Bernhard / Belser Eva Maria / Epiney Astrid (Hrsg.), Basler Kommentar Bundesverfassung, Basel 2015, art. 48 N 37
65 Loi du 21 mars 2003 sur l'énergie nucléaire; RS **732.1**
66 Loi du 8 octobre 2004 sur la transplantation; RS **810.21**
67 Loi du 20 juin 1997 sur les armes; RS **514.54**

Dans ce contexte, la lutte contre la grande criminalité se veut être une tâche commune de la Confédération et des cantons, chacun ayant ses spécificités. En traitant les données relatives aux passagers aériens, l'UIP appuie à la fois la Confédération et les cantons dans l'accomplissement de cette tâche commune.

C'est la raison pour laquelle l'UIP doit se composer à parts égales de collaborateurs de la Confédération et des cantons.

Al. 2

L'engagement des collaborateurs cantonaux au sein de l'UIP n'entraîne pas la suppression du rapport de travail existant, mais seulement une division du rôle de l'employeur, comme en cas de location de services[68].

Le droit de donner des instructions sur des questions techniques et opérationnelles, qui inclut notamment le droit de fixer les horaires de travail, est transféré à fedpol pendant l'engagement auprès de l'UIP. En revanche, le droit de donner des instructions sur le plan disciplinaire reste une compétence de l'autorité qui détache son personnel.

Les autres droits et obligations découlant du contrat de travail, notamment l'obligation de payer le salaire et de verser les cotisations de l'employeur prévues par le droit des assurances sociales, restent du ressort de l'autorité mettant des collaborateurs à la disposition de l'UIP.

La Confédération supporte à elle seule les coûts relatifs à l'infrastructure des places de travail au sein de l'UIP ainsi que ceux relatifs à la mise en place et à l'exploitation du système d'information PNR.

Il convient de noter que la Confédération n'est pas seulement responsable de ses collaborateurs, mais aussi de ceux détachés par les cantons et engagés auprès de l'UIP, au sens de l'art. 1, al. 1, let. f, de la loi du 14 mars 1958 sur la responsabilité[69].

Al. 3

Les al. 3 et 4 prévoient des dispositions spéciales en matière de droit du travail qui s'appliquent pendant l'engagement auprès de l'UIP. Ces dispositions spéciales nécessitent une base légale.

Les dispositions spéciales concernent en particulier:

- le droit partagé de donner des instructions (al. 3);
- le devoir des collaborateurs de respecter le secret professionnel (al. 4), également vis-à-vis de leur employeur contractuel.

Le droit de donner des instructions est considéré comme partagé, car il est exercé aussi bien par l'employeur qui détache son personnel que par fedpol ou

68 Loi fédérale du 6 octobre 1989 sur le service de l'emploi et la location de services; RS **823.11**
69 RS **170.32**

l'UIP. Celle-ci exerce le droit de donner des instructions techniques et opérationnelles, ce qui englobe tout ce qui ne relève pas du droit de donner des instructions disciplinaires, lequel reste du ressort de l'employeur contractuel.

Si, lors de son engagement au sein de l'UIP, une personne détachée a un comportement susceptible de justifier des mesures disciplinaires, fedpol devra chercher le dialogue avec l'employeur contractuel. Celui-ci examinera alors quelles mesures disciplinaires sont indiquées. Dans la grande majorité des cas, des instructions suffiront. Dans des cas exceptionnels, il faudra, à des fins disciplinaires, prononcer le licenciement immédiat. Cette possibilité reste également du ressort de l'employeur contractuel et n'est pas affectée par le détachement.

Al. 4

Selon cet alinéa, il est interdit aux collaborateurs de l'UIP de disposer librement en dehors de l'UIP des éléments dont ils ont connaissance durant leur engagement. Cette disposition s'applique également une fois leur engagement terminé. Par conséquent, l'échange informel de données personnelles notamment 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 connaissances de l'UIP aux autorités qui détachent leurs collaborateurs.

Al. 5

Il convient de fixer les modalités relatives au détachement dans la convention que le Conseil fédéral et les cantons doivent conclure.

Il s'agit ainsi de convenir, outre du nombre de collaborateurs cantonaux détachés, des qualifications souhaitées et de viser tout particulièrement les collaborateurs cantonaux qui s'intéressent vivement aux processus numériques. Les autres prétentions financières des personnes détachées, qui doivent également faire l'objet de la convention, concernent notamment les frais. L'employeur contractuel ou le canton qui détache ces personnes est tenu de les indemniser.

Section 8 Conclusion de traités et de conventions et assistance administrative

Art. 29 Conclusion de traités et de conventions

Soixante-neuf États utilisent déjà le PNR. Ils demandent au minimum les données relatives aux passagers aériens sur les vols à destination de leur territoire.

L'art. 2 de la présente loi prévoit une règle analogue à celle de la directive PNR de l'UE: les entreprises de transport aérien doivent communiquer à l'UIP de la Suisse les données relatives aux passagers aériens qui entrent dans notre pays ou en sortent.

Toutefois, les entreprises de transport aérien suisses ne peuvent communiquer leurs données relatives aux passagers aériens à un service compétent étranger que si un traité international signé par la Suisse le prévoit (cf. art. 2, al. 2).

Grâce à l'art. 29, qui autorise le Conseil fédéral à conclure ces traités, l'approbation parlementaire prévue à l'art. 166, al. 2, Cst. n'est pas nécessaire, pour autant que la teneur du contrat soit conforme à la norme de délégation prévue à l'al. 2 de la présente loi.

Un tel traité devra être conclu notamment avec l'UE ("organisation internationale"). Il remplacera la solution transitoire élaborée avec le concours du PFPDT qui permet actuellement aux entreprises de transport aérien suisses de communiquer des données à l'UE (cf. ch. 1.2 ci avant).

Près de 72 % des passagers enregistrés dans les aéroports suisses s'envolent à destination de l'UE ou proviennent de l'UE et se rendent en Suisse. Si ce pourcentage certes élevé ne permet pas de déduire directement quel est le volume de données provenant de l'UE, il montre que le trafic aérien entre l'UE et la Suisse est significatif. Par conséquent, un traité international régissant la communication réciproque des données relatives aux passagers aériens est essentiel tant pour la Suisse que pour l'UE. Le Conseil fédéral a octroyé un mandat de négociations ad hoc le 1er novembre 2023.

D'autres traités sont prévus, entre autres avec la Norvège et le Royaume-Uni.

Al. 1

Les États qui garantissent un niveau de protection adéquat sont inscrits sur la liste de l'annexe 1 de l'OPDo. La Suisse peut leur communiquer des données personnelles sans devoir conclure de traité international. Néanmoins, la présente loi prévoit tout de même de conclure des traités avec eux. Il s'agit ainsi de garantir la communication *réciproque* de données. Si les deux États signataires estiment que le niveau de protection des données qu'ils s'octroient réciproquement est adéquat (cf. art. 16, al. 1, LPD), le traité se limitera aux modalités relatives à la communication réciproque des données.

Dans son rapport explicatif du 31 août 2022 relatif à l'ordonnance sur la protection des données, l'OFJ explique que la liste des États figurant à l'annexe 1 de l'ordonnance "sera revue périodiquement afin de prendre en compte d'une part la pratique d'autres États et d'autre part les développements au niveau international, en particulier les ratifications de la Convention STE 108. La

liste n'est donc pas définitive et pourrait encore être modifiée avant l'entrée en vigueur de l'ordonnance[70].

Dans le 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, le Conseil fédéral a précisé ce qu'on entend par traité international: "non seulement une convention internationale en matière de protection des données à laquelle l'État destinataire serait partie, telle que la convention STE 108[71] et son protocole additionnel dont les exigences ont été transposées par l'État partie dans son droit interne, mais aussi tout autre accord international qui prévoit un échange de données entre États parties et qui répond en substance aux exigences de la convention STE 108. Il peut également s'agir d'un traité international conclu par le Conseil fédéral en vertu de l'art. 61, let. b, P-LPD [qui correspond à l'art. 67, let. b, LPD][72]".

Al. 2

Étant donné que la Suisse n'a pas repris toutes les prescriptions de la CJUE, il n'est pas exclu que l'accord avec l'UE prévoie ponctuellement des règles plus strictes en matière de protection des données qui s'écartent de la présente loi. L'al. 2 tient compte de cette éventualité dans la mesure où le Conseil fédéral, si nécessaire, est habilité à convenir dans un traité des traitements moins étendus pour les données provenant de l'UE.

Al. 3

Cet alinéa vise à octroyer 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.

En revanche, le Conseil fédéral doit toujours fixer dans un traité, conformément à l'al. 1, les questions fondamentales relatives à la protection des données, notamment celles concernant les droits et obligations des autorités.

Art. 30 Assistance administrative

Dans le cas des données PNR aussi, l'assistance administrative doit être fournie par les autorités compétentes (cf. art. 1, al. 2) conformément au droit régissant ces dernières.

L'UIP ne doit fournir une assistance administrative qu'en cas d'urgence; à savoir, comme cela est exprimé à l'al. 2, s'il existe un "risque imminent" qu'une infraction pénale visée à l'annexe 2 soit commise à l'étranger. Les dispositions dérogatoires d'un traité international sont toutefois réservées.

70 https://www.bj.admin.ch/bj/fr/home.html > Etat & Citoyen > Protection des données > Nouveau droit de la protection des données > 1. Etapes préalables, 2022 – Adoption des nouvelles ordonnances (OPDo et OCPD)

71 Convention du 5 juin 1997 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, RS **0.235.1**

72 FF **2017** 6565 6658

L'assistance administrative que l'UIP octroie à une UIP étrangère se limite ainsi à des cas exceptionnels dûment justifiés, qui légitiment l'action de l'UIP – en lieu et place d'une autorité compétente visée à l'art. 1, al. 2.

Dans le cadre de l'assistance administrative, l'UIP ne communique des données relatives aux passagers aériens à une UIP étrangère que si la demande de cette dernière est dûment motivée et indique au moins:

- les données souhaitées, désignées précisément;
- en quoi ces données sont nécessaires pour prévenir une infraction imminente visée à l'annexe 2.

L'UIP n'est autorisée à communiquer des données qu'à une UIP étrangère rattachée à l'administration d'un État qui:

- conformément à l'annexe 1 de l'OPDo, garantit un niveau de protection adéquat (cf. art. 16, al. 1, LPD); ou
- sur la base de règles spécifiques prévues dans un traité international conclu avec la Suisse, garantit un niveau de protection approprié (art. 16, al. 2, let. a, LPD).

Si aucune de ces conditions n'est remplie, l'UIP renonce à communiquer des données relatives aux passagers aériens.

Si les données demandées sont pseudonymisées ou sensibles, l'assistance administrative de l'UIP est également exclue.

Section 9 Sanctions administratives

Art. 31 Sanctions en cas de violation des obligations des entreprises de transport aérien

Les sanctions prévues à l'art. 31 constituent des sanctions administratives pécuniaires. En se fondant sur les règles en vigueur du droit fédéral, le Conseil fédéral a décrit ces sanctions dans son rapport du 1er novembre 2018[73] comme suit: "[p]our simplifier, on entend par [sanction administrative pécuniaire] une réaction des autorités à une violation passée d'une prescription de droit administratif, consistant à faire payer un montant à la partie dans le cadre d'une procédure administrative."

Al. 1

La violation du devoir de diligence et de l'obligation d'informer prévus aux art. 3 et 4 est sanctionnée indépendamment du fait que la Confédération prouve ou non que l'entreprise en question est en faute, en application depuis le 1er octobre 2015 de l'art. 122*b* LEI relatif à la violation de l'obligation de communiquer des entreprises de transport aérien. Le Conseil fédéral a justifié qu'on ait autrefois renoncé à fournir une telle preuve par les recherches

73 Sanctions administratives pécuniaires. Rapport du Conseil fédéral donnant suite au postulat 18.4100 de la CIP-N du 1er novembre 2018, FF **2022** 776, ch. 2.1

d'envergure qui en résultaient, également à l'étranger, ce qui rendait l'obtention de la preuve quasiment impossible en pratique[74].

Al. 2

La violation d'une obligation au sens de l'art. 3 de la présente loi est légalement présumée lorsque l'entreprise de transport aérien:

- omet de communiquer les données relatives aux passagers aériens ou les communique trop tard;
- ne respecte pas les prescriptions techniques en communiquant les données relatives aux passagers aériens;
- ne communique pas toutes les données des passagers.

Il en va de même lorsqu'une entreprise de transport aérien n'a pas informé ses passagers du traitement des données prévu à l'art. 4 de la présente loi (cf. commentaire de l'art. 4).

L'UIP doit apporter la preuve que l'entreprise de transport aérien n'a pas communiqué les données conformément aux exigences légales ou n'a pas informé, ou du moins pas de façon adéquate, les passagers du traitement de leurs données en vertu de la présente loi.

Al. 3

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

En revanche, la violation du devoir de diligence est considérée comme grave lorsqu'elle est constatée à plusieurs reprises ou lorsque l'ensemble des données d'un vol n'est pas fourni.

Al. 4

Dans le rapport susmentionné, le Conseil fédéral a précisé le concept de sanction administrative pécuniaire indépendante de la faute prévu par le législateur: "L'autorité administrative doit donc [pouvoir] prouver au moins une faute dans l'organisation (violation objective d'un devoir de prudence). L'entreprise peut aussi être sanctionnée en cas de comportement fautif d'une personne responsable. Cette voie médiane a fait ses preuves dans la pratique en droit des cartels et peut être transposée aux autres dispositions consacrant des sanctions administratives pécuniaires. Dans l'ensemble, il n'est pas nécessaire d'apporter des adaptations sur le plan législatif en ce qui concerne la faute du destinataire de la sanction."[75]

74 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

75 Sanctions administratives pécuniaires. Rapport du Conseil fédéral donnant suite au postulat 18.4100 de la CIP-N du 1er novembre 2018, FF **2022** 776, ch. 4.3.3

Il n'y a pas de sanction, malgré une éventuelle contestation, lorsque l'entreprise de transport aérien prouve qu'elle a pris toutes les précautions 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 communication des données.

Al. 5

L'al. 5 garantit que les violations de l'obligation de diligence survenues à l'étranger puissent également faire l'objet d'une sanction. C'est notamment le cas lorsqu'une entreprise de transport aérien ne communique pas, pas à temps ou de façon incomplète à l'UIP de la Suisse les données relatives aux passagers aériens en partance pour notre pays.

Art. 32 Procédure

Al. 1

fedpol prononce les sanctions prévues à l'art. 31.

Al. 2

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 n'est pas sanctionnée une nouvelle fois en vertu de la loi sur les données relatives aux passagers aériens. Cependant, la sanction de la violation de l'obligation d'informer prévue à l'art. 4 est réservée.

Al. 3

Le délai de deux ans ne peut pas être prolongé.

Section 10 Dispositions finales

Art. 33 Exécution

Les présentes dispositions d'exécution sont des prescriptions subordonnées ou de détail qui servent à l'exécution de la présente loi. La compétence du Conseil fédéral d'édicter de telles dispositions repose sur l'art. 182, al. 2, Cst.

Art. 34 Modification d'autres actes

L'annexe 3 indique les modifications qui doivent être apportées à d'autres lois en lien avec la présente loi. Sont concernées: la LRens, la LEI, la LDEA, la loi du 17 juin 2005 sur le Tribunal administratif fédéral (LTAF)[76], la LSIP et la LA.

L'art. 351, al. 1, CP est la base légale permettant à fedpol d'accéder au système d'information d'INTERPOL (I-24/7). Étant rattachée à fedpol, l'UIP n'a pas besoin d'une base légale supplémentaire pour y accéder.

76 RS **173.32**

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, mais séparées.

On parle de *partage de code* (ch. 15) lorsqu'une autre entreprise de transport aérien achète des places à celle responsable du vol. Si un passager réserve un tel siège, il vole avec les codes des deux entreprises de transport aérien.

Des précisions sur les ensembles de données relatives aux passagers aériens sont fournies également dans le commentaire de l'art. 1, al. 4.

Annexe 2 Catégories d'infractions

Les catégories d'infractions comprennent des infractions terroristes (ch. 1) et d'autres infractions pénales graves (ch. 2); la lutte contre ces dernières autorise le traitement des données relatives aux passagers aériens en vertu de la présente loi.

À l'origine, elles s'inspiraient des catégories d'infractions de la directive PNR de l'UE et y associaient les éléments constitutifs d'infraction déterminants prévus à l'annexe 1 LEIS, élargie dans le cadre de PRÜM[77]. Bien que cet élargissement ne soit pas encore en vigueur, il est déjà pris en compte dans le présent message. Il en va de même pour un autre complément à l'annexe de la LEIS, qui est en cours de préparation.

Sont en outre prises en compte de nouvelles formes graves d'espionnage. Ce complément résulte de l'évolution de la situation géopolitique.

Dans le tableau ci-dessous figurent les infractions qui ont été ajoutées à la suite de la consultation.

1.7	Atteintes à l'ordre constitutionnel (art. 275 CP)
2.1.14.1	Contrainte sexuelle (art. 189, al. 1, CP)
2.1.14.3	Actes d'ordre sexuel commis sur une personne incapable de discernement ou de résistance (art. 191 CP)
2.1.11.5	Disparition forcée (art. 185bis et 260bis, al. 1, let. f^{bis}, et 3, CP)

77 Arrêté fédéral portant approbation et mise en œuvre de l'accord entre la Suisse et l'UE concernant l'approfondissement de la coopération transfrontalière (coopération Prüm) et du Protocole Eurodac entre la Suisse, l'UE et la Principauté de Liechtenstein concernant l'accès à Eurodac à des fins répressives, FF **2021** 2332 10-16

2.2.1.1	Service de renseignements politiques (art. 272, ch. 2, CP)
2.2.1.2	Service de renseignements économiques (art. 273, al. 3, CP)
2.2.1.3	Service de renseignements militaires (art. 274, ch. 1, al. 4, CP)

À la suite de la consultation et compte tenu des explications de la CJUE, les catégories d'infractions ont à l'inverse été nettement condensées. Désormais, elles ne comprennent plus que les éléments constitutifs d'infractions:

a. qui présentent selon l'arrêt de la CJUE un "niveau de gravité incontestablement élevé" (ch. marg. 149), un "lien direct avec le transport aérien de passagers" (ch. marg. 154) en tant que grande criminalité ou sont du moins "de nature transnationale" (ch. marg. 155);

b. pour lesquels le droit suisse prévoit une peine minimale légale qui peut être comprise comme étant une spécificité du droit national mentionnée par la CJUE et qui permet de déduire une gravité particulière de l'infraction (a contrario du ch. marg. 151 s.).

Les éléments constitutifs de l'infraction en lien avec l'espionnage ajoutés aux catégories d'infractions prévoient aussi une peine minimale légale.

Le commentaire de l'art. 1, al. 4, fournit des explications supplémentaires sur les éléments constitutifs de l'infraction visés à l'annexe 2.

Annexe 3 Modification d'autres actes

1. Loi fédérale du 25 septembre 2015 sur le renseignement[78]

Le SRC dispose d'un statut particulier dans la lutte contre les infractions terroristes et les autres infractions pénales graves. Il recherche des informations le plus souvent en amont de l'enquête policière et de la poursuite pénale afin de détecter de façon précoce et de prévenir les menaces pesant sur la sécurité intérieure et extérieure.

Il compare les données relatives aux passagers aériens après leur réception avec celles des systèmes d'information IASA SRC et IASA-EXTR SRC et traite les éventuelles concordances dans le système où elles ont été obtenues.

L'art. 21 de l'ordonnance du 16 août 2017 sur les systèmes d'information et les systèmes de stockage de données du Service de renseignement de la Confédération (OSIS-SRC)[79] prévoit un délai de conservation de 30 à 45 ans pour

78 RS **121**
79 RS **121.2**

les données d'IASA SRC selon le domaine concerné. Les concordances obtenues dans IASA-EXTR SRC sont effacées après quinze ans au plus tard (cf. art. 28, al. 1, OSIS-SRC).

Les données relatives aux passagers aériens n'ayant pas abouti à une concordance restent dans le système de stockage des données résiduelles jusqu'à leur effacement au bout d'un mois.

Art. 16a Données relatives aux passagers aériens

Le SRC est la seule autorité compétente qui reçoit des données relatives aux passagers aériens de la part de l'UIP pour les traiter en toute autonomie. La communication des données relatives aux passagers aériens n'est autorisée que pour les liaisons que le Conseil fédéral détermine au préalable dans une liste non publique. La formulation de cet article s'inspire de celle de l'art. 20, al. 4, LRens.

Le SRC est tenu de respecter la finalité définie à l'art. 11, al. 2, P-LDPa lors du traitement des données relatives aux passagers aériens: il ne peut les traiter et les comparer avec ses propres données dans le cadre de l'art. 6, al. 1, let. a, ch. 1 à 5, LRens que dans la mesure où cela est nécessaire afin de prévenir les infractions visées à l'annexe 2 du P-LDPa (al. 2).

Selon l'al. 3, les données n'ayant pas eu pour résultat une concordance par suite de la comparaison automatisée dans les deux systèmes d'information du SRC susmentionnés doivent être effacées automatiquement un mois après leur transmission au SRC.

2. Loi fédérale du 16 décembre 2005 sur les étrangers et l'intégration[80]

L'art. 109*b* LEI constitue la base légale du système national d'information sur les visas (ORBIS). Celui-ci fournit des informations sur les demandes de visa et répertorie toutes les personnes qui disposent d'un visa pour l'espace Schengen. Une personne peut être identifiée grâce à son numéro de passeport vérifiable.

Art. 109c, let. i Consultation du système national d'informations sur les visas

L'UIP est ainsi autorisée à accéder aux données enregistrées dans ORBIS pour la vérification de l'identité des passagers aériens (cf. art. 6, al. 3, let. b, P-LDPa).

80 RS **142.20**

3. Loi fédérale du 20 juin 2003 sur le système d'information commun aux domaines des étrangers et de l'asile[81]

La LDEA règle le système d'information utilisé dans le domaine des étrangers et de l'asile (SYMIC). Celui-ci contient des données personnelles sur les étrangers en Suisse (par ex. nom, prénom, date de naissance) et leur statut de séjour. Désormais, le SYMIC permet également de consulter les données du système d'information en vue de l'établissement des documents de voyage suisses et des autorisations de retour pour étrangers. Peuvent donc y être également consultées les données des documents de voyage comme le nom et le lieu d'origine des étrangers enregistrés en Suisse et titulaires d'un document de voyage délivré par notre pays (par ex. passeport pour réfugié).

Art. 9, al. 1, let. q

L'UIP est ainsi autorisée à accéder aux données enregistrées dans le SYMIC pour la vérification de l'identité des passagers aériens (cf. art. 6, al. 3, let. b, P-LDPa).

4. Loi du 17 juin 2005 sur le Tribunal administratif fédéral[82]

Conformément aux art. 19 et 20 P-LDPa, le Tribunal administratif fédéral décide de la levée de la pseudonymisation. Cela nécessite les modifications proposées.

5. Loi fédérale du 13 juin 2008 sur les systèmes d'information de police de la Confédération[83]

La LSIP contient les bases légales relatives aux systèmes d'information de police avec les données desquels les données relatives aux passagers aériens sont comparées automatiquement (cf. art. 6, al. 1, let. a). En outre, l'UIP doit pouvoir accéder manuellement aux données des différents systèmes d'information de police, afin de vérifier la conformité au but légal des concordances obtenues automatiquement (cf. art. 6, al. 3, let. a).

Il n'est pas nécessaire de prévoir explicitement l'accès manuel de l'UIP au système de gestion des affaires et des dossiers prévu à l'art. 18 LSIP afin de vérifier la conformité au but légal des concordances obtenues automatiquement (cf. art. 6, al. 3, let. a), étant donné que l'art. 18, al.7, prévoit déjà l'accès des collaborateurs de fedpol.

Pour vérifier l'identité, l'UIP doit pouvoir accéder également au RIPOL et au N-SIS (cf. art. 6, al. 3, let. b).

81 RS **142.51**
82 RS **173.32**
83 RS **361**

Art. 10, al. 4, let. a^{bis} *Système d'appui aux enquêtes de police judiciaire de la Confédération*

Art. 11, al. 5, let. b^{bis} *Système de traitement des données relatives aux infractions fédérales*

Ces deux modifications visent à autoriser l'UIP à accéder manuellement aux données du Système national d'enquête (SNE) afin de vérifier la conformité au but légal des concordances obtenues automatiquement conformément à l'art. 6, al. 3, let. a.

Art. 12, al. 6, let. b^{bis} *Système de traitement des données relatives à la coopération policière internationale et intercantonale*

Cette modification vise à autoriser l'UIP à accéder manuellement au système de traitement des données relatives à la coopération policière internationale et intercantonale (IPAS) afin de vérifier la conformité au but légal des concordances obtenues automatiquement conformément à l'art. 6, al. 3, let. a.

Art. 15, al. 4, let. a^{bis} *Système de recherches informatisées de police*

Cette modification vise à autoriser l'UIP à comparer automatiquement les données relatives aux passagers aériens avec les données du système de recherches informatisées de police (RIPOL), en vertu de l'art. 6, al. 1, let. a, P-LDPa, et à y accéder manuellement afin de vérifier la conformité au but légal des concordances obtenues automatiquement conformément à l'art. 6, al. 3, let. a, P-LDPa.

Art. 16, al. 2, let. k^{bis} *Partie nationale du Système d'information Schengen*

Cette modification vise à autoriser l'UIP à comparer automatiquement les données relatives aux passagers aériens avec les données de la partie nationale du Système d'information Schengen (N-SIS), en vertu de l'art. 6, al. 1, let. a, P-LDPa, et à y accéder manuellement afin de vérifier la conformité au but légal des concordances obtenues automatiquement conformément à l'art. 6, al. 3, let. a, P-LDPa.

Art. 17, al. 4, let. a^{bis} *Index national de police*

Cette modification vise à autoriser l'UIP à accéder manuellement à l'Index national de police afin de vérifier la conformité au but légal des concordances obtenues automatiquement conformément à l'art. 6, al. 3, let. a, P-LDPa.

6. Loi fédérale du 21 décembre 1948 sur l'aviation[84]

Art. 29, al. 5

Il ne faut pas que les entreprises de transport aérien puissent 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. 31 de la loi sur les données relatives aux passagers aériens.

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 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[85]).

Cette règle doit non seulement s'appliquer aux sanctions prévues par la loi sur les données relatives aux passagers aériens, mais aussi à celles prévues par la LEI, laquelle prévoit des dispositions analogues relatives à la sanction des entreprises de transport aérien (art. 122*a* et 122*b*).

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

- une sanction en vertu de l'art. 31 P-LDPa ou des art. 122*a* et 122*b* LEI 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, les autres circonstances indirectement liées aux impayés doivent toutes avoir été prises en considération. Par conséquent, l'obligation légale de retirer l'autorisation d'exploitation est abandonnée.

6 Conséquences

6.1 Conséquences pour la Confédération

L'utilisation du PNR nécessite un système d'information et la mise en place de l'unité responsable (UIP) à fedpol.

Système d'information PNR

À l'image de plusieurs États, la Suisse devrait aussi utiliser le système *goTravel* de l'ONU.

goTravel est un dérivé de *TRIP*, le système d'information PNR que les Pays-Bas ont développé et mis à la disposition de l'ONU.

84 RS **748.0**
85 RS **281.1**

Depuis plusieurs années maintenant, celle-ci le fournit à ses États membres et soutient ces derniers dans le cadre de son *Programme de lutte contre le terrorisme axé sur les déplacements* en lien avec le PNR. En Europe, la Belgique utilise *TRIP*, alors que *goTravel* est utilisé par le Luxembourg et, depuis 2022, par la Norvège.

Compte tenu de son utilisation par plusieurs États, *goTravel* est développé en continu. L'ONU rend accessibles les résultats de ces développements aux autres États membres qui utilisent ce système d'information PNR.

Toutefois, *goTravel* nécessitera des adaptations techniques avant d'être utilisé en Suisse. Elles seront instaurées par la Suisse et mises en œuvre par l'ONU.

C'est seulement par la suite que la version de *goTravel* adaptée à l'utilisation suisse sera intégrée dans l'environnement informatique du CSI-DFJP, lequel vérifiera, avec le concours de fedpol, si elle fonctionne et est sûre.

Lors des tests, aucune donnée de production ne sera utilisée. Il sera uniquement fait usage de données "synthétiques". Il s'agit de données établies artificiellement. Tous les tests seront effectués en interne; aucune donnée de test ne quittera l'environnement de test et donc le CSI-DFJP. Si l'examen se révèle concluant, *goTravel* sera validé pour l'utilisation productive.

Dans le cadre de sa collaboration avec la Suisse, l'ONU n'entre jamais en possession de données PNR ni de résultats de leur traitement effectué en Suisse. Ces données sont exclusivement enregistrées en Suisse, en l'occurrence dans l'environnement informatique du CSI-DFJP, à moins d'être communiquées à une autorité légalement compétente (cf. art. 7 à 11 et 30).

Il ne sera pas possible de réaliser le projet sur le plan technique à fedpol sans le soutien de prestataires externes. S'agissant des aspects techniques, seuls les prestataires ayant obtenu une adjudication principalement dans le cadre de l'appel d'offres OMC ALPIN 2.0 sont éligibles. ALPIN 2.0 fournit un pool de services pour les projets informatiques clés, les grands projets informatiques et les projets complexes et stratégiques de l'ensemble de l'administration fédérale. Les mandats concrets seront attribués aux adjudicataires au moyen d'une procédure de mini-tender électronique (concours). Par ailleurs, toutes les personnes affectées à la fourniture de prestations devront réussir le contrôle de sécurité élargi de la Confédération.

La responsabilité liée à l'exploitation et à la maintenance de la version de *goTravel* utilisée par la Suisse incombe au CSI-DFJP. Aucun prestataire externe ne sera impliqué pour ce faire.

Voir le ch. 7.7 relatif à la protection des données devant être garantie grâce à des mesures techniques et organisationnelles.

Coûts

La Confédération prend entièrement à sa charge les coûts de projet et d'exploitation du système d'information PNR ainsi que les coûts d'exploitation de l'UIP. Le personnel de l'UIP se compose à parts égales de collaborateurs de la

Confédération et des cantons. L'effectif devrait s'élever à 30 équivalents plein temps (EPT) pour que l'UIP soit pleinement opérationnelle (24 heures sur 24, 7 jours sur 7). Une mise en place progressive est néanmoins prévue afin de faire de premières expériences dans l'utilisation des données PNR. La phase initiale prévoit donc un effectif inférieur permettant de fournir les prestations de base de l'UIP.

a) Coûts de projet

Dans le cadre du projet "PNR Suisse", fedpol crée les bases légales et les conditions techniques et organisationnelles relatives au traitement des données relatives aux passagers aériens.

Lors de la phase d'initialisation du projet, il a été examiné si le système d'information PNR devait être acheté sur le marché ou si le CSI-DFJP devait lui-même le développer. Comme le développement en interne a été jugé très complexe et onéreux, il a été décidé, dans le cadre d'une preuve de concept, d'évaluer si le système *goTravel* de l'ONU remplissait les exigences et pouvait être intégré à l'environnement informatique du CSI-DFJP. En juin 2022, les responsables du projet PNR ont opté pour *goTravel*.

Si la mise en œuvre de *goTravel* en Suisse n'occasionne pas d'adaptations majeures, les coûts de projet devraient s'élever à environ 11,5 millions de francs (dont 6,82 millions de francs de dépenses avec incidences financières) pour la période 2020-2026. Dans le détail, ces coûts sont budgétisés comme suit:

	Coûts de projet de 2020 à 2026 ***(en mio. de francs)***
Coûts pour les prestations externes et les conventions avec le fournisseur de prestations CSI-DFJP	6,82
Coûts en personnel internes à fedpol	4,69
Coûts totaux	**11,51**

Une deuxième preuve de concept plus approfondie est en cours pour examiner plus en détail la manière dont les nouvelles exigences légales suisses peuvent être mises en œuvre dans *goTravel* sur le plan technique. Les adaptations et les développements éventuellement nécessaires et considérables sur le plan financier ne devraient toutefois être mis en œuvre que dans le cadre d'un développement ultérieur à partir de 2026.

b) Coûts d'exploitation du système d'information PNR et de l'UIP dès 2026 (sans les coûts en personnel)

L'exploitation du système d'information PNR et la maintenance de la structure informatique (matériel, logiciels, réseaux, etc.) auprès du CSI-DFJP engendreront des coûts annuels de maximum 1,65 million de francs dès la mise en service opérationnelle en 2026.

Sont inclus dans ce calcul

- l'infrastructure du serveur pour l'exploitation de *goTravel* et de tous les composants logiciels nécessaires ainsi que pour l'enregistrement des données PNR;
- l'enregistrement des procès-verbaux de journalisation (cf. art. 24).

Le DFJP est en train de sonder le marché pour clarifier les coûts escomptés qu'occasionneraient l'achat et l'exploitation de la passerelle de données. Il est également en train de clarifier la création de synergies avec le SEM, qui pourrait utiliser la même passerelle de données à l'avenir pour recevoir les données API.

Selon la planification actuelle, l'UIP sera mise en place au siège de fedpol à Berne. Des locaux y sont déjà disponibles, ce qui ne devraient donc pas occasionner de coûts supplémentaires conséquents. D'autres coûts seront occasionnés pour les postes de travail selon la stratégie usuelle de l'administration fédérale.

Les coûts concrets relatifs à l'infrastructure et à l'exploitation seront analysés plus en détail dans la suite du projet.

c) Coûts en personnel

Les besoins en personnel de l'UIP dépendent des heures d'exploitation de cette dernière, des données à traiter et du nombre de routes aériennes prises en compte. Une mise en place progressive est prévue. Dans une première phase, il conviendra de permettre l'utilisation des données PNR grâce à des prestations de base et de faire de premières expériences. L'UIP débutera avec un effectif réduit et son exploitation sera limitée (s'agissant des heures d'exploitation et de l'étendue des prestations). Trente EPT devraient être nécessaires à la pleine exploitation de l'UIP (24 heures sur 24, 7 jours sur 7 et prestations complètes).

Du côté de la Confédération, le DFJP (fedpol) et le Département fédéral des finances (OFDF) mettront leurs collaborateurs à disposition. L'OFDF s'est dit prêt à collaborer au sein de l'UIP à hauteur de un à deux EPT tant qu'il assume une tâche déléguée dans le contrôle des personnes aux aéroports de Bâle et de Genève. Contrairement aux collaborateurs de l'OFDF, ceux de fedpol seront engagés à l'UIP à long terme, garantissant ainsi la continuité du travail de l'UIP et la "mémoire opérationnelle" de cette unité organisationnelle. On peut notamment penser à la direction de l'UIP, aux personnes responsables de l'encadrement des entreprises de transport aérien et à la représentation de l'UIP au sein des organismes internationaux.

6.2 Conséquences pour les cantons et les communes, ainsi que pour les centres urbains, les agglomérations et les régions de montagne

De nombreux éléments constitutifs de l'infraction qui seront également combattus grâce aux données PNR relèvent de la compétence des cantons en matière de poursuite pénale. Grâce au PNR, les autorités cantonales de police et de poursuite pénale accèdent plus simplement, plus rapidement et plus précisément aux informations issues du trafic aérien qui sont importantes pour l'accomplissement de leurs tâches.

Les données PNR permettent aux autorités cantonales de poursuite pénale de recevoir des informations sur des personnes recherchées au niveau national ou international qui sont sur le point d'atterrir en Suisse ou de quitter le pays par voie aérienne. Ainsi, les cantons (éventuellement en coopération avec d'autres autorités) peuvent prendre à temps les mesures qui s'imposent. De plus, l'utilisation du 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. Elle pourrait aussi fournir des renseignements utiles sur des infractions non élucidées.

Comme le montrent les expériences faites à l'étranger, le PNR, et bientôt la loi sur les données relatives aux passagers aériens, contribuent considérablement à renforcer l'efficience et l'efficacité de la poursuite pénale et de la prévention de la criminalité. Les cantons en profitent grandement.

Étant donné qu'une majorité des mesures devant être prises sur la base du PNR le seront à l'arrivée des personnes à l'aéroport, le traitement 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.

Coûts en personnel

La Confédération et les cantons détachent chacun la moitié des collaborateurs de l'UIP et en assument le coût. Les 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 se sont prononcées, dans le cadre de la consultation, en faveur de la participation des cantons au personnel de l'UIP. Une convention en ce sens est en cours d'élaboration avec les cantons.

Les collaborateurs détachés par les cantons seront engagés à l'UIP pendant une durée déterminée. Ils assumeront en priorité les tâches centrales de l'UIP, notamment la surveillance de la communication de données par les entreprises de transport aérien à l'UIP ainsi que la vérification des concordances obtenues par suite de la comparaison automatique des données relatives aux passagers aériens avec celles issues des systèmes d'information, les profils de risque et

les listes d'observation. Cette manière de procéder garantit le transfert de connaissances de la Confédération aux cantons et permet à ces derniers de tirer le meilleur profit du PNR.

Il serait judicieux que les cantons désignent au moins une personne de contact pour l'UIP. Il serait souhaitable qu'ils forment également des spécialistes disposant du savoir requis pour déposer des demandes ciblées à l'UIP et coopérer étroitement avec celle-ci au cas par cas.

La loi sur les données relatives aux passagers aériens n'a pas de conséquences directes pour les communes et les régions de montagne.

6.3 Conséquences économiques

La loi sur les données relatives aux passagers aériens 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 69 États. Pour les entreprises de transport aérien, qui sont tenues de communiquer des données au service compétent de l'État, cette tâche n'a donc plus rien de nouveau.

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. Ce constat est également ressorti des prises de position remises dans le cadre de la consultation qui a eu lieu du 13 avril au 31 juillet 2022.

Il convient également de noter que la communication de données PNR par les entreprises de transport aérien est de plus en plus une condition préalable aux vols à destination de certains pays. Si la Suisse n'élaborait pas la loi sur les données relatives aux passagers aériens et, partant, ne mettait pas un système PNR en place, les entreprises de transport aérien helvétiques pourraient être désavantagées et la Suisse pourrait perdre son excellente inclusion actuelle au trafic aérien international, ce qu'il faut absolument éviter d'un point de vue économique.

Les États-Unis ont en outre fait du PNR une condition au maintien de la Suisse dans le VWP. Ce programme permet aux Suisses de se rendre et de séjourner aux États-Unis sans visa à des fins professionnelles ou touristiques pendant 90 jours au plus. Une exclusion de la Suisse de ce programme aurait des répercussions négatives sur les différents domaines économiques suisses.

6.4 Conséquences sociales

Généralités

La grande criminalité déstabilise la société et mine la confiance en l'État de droit. Les instruments pouvant être utilisés pour lutter contre ces infractions sont une condition essentielle au maintien de la sécurité publique et au développement positif de la société.

Par ailleurs, la prise en compte des prescriptions en matière de protection des données garantit que les données personnelles soient traitées dans le respect des principes de licéité et de proportionnalité. De plus, les personnes concernées ont le droit d'être informées du traitement de leurs données et, le cas échéant, de faire vérifier la licéité de ce traitement.

Les enfants font aussi partie des victimes de la grande criminalité. Ils ont besoin d'une protection particulière. Les expériences faites par les États étrangers montrent que le PNR est un instrument efficace pour protéger les enfants contre la criminalité organisée (par ex. la traite des êtres humains) ou la pédophilie.

Digression: le PNR et les enfants

En règle générale, les enfants se déplacent accompagnés par au moins un de leurs parents, surtout lorsqu'ils voyagent en avion. Dans ce cas, tant qu'ils n'ont pas douze ans, ils figurent en tant qu'autres voyageurs avec indication de leur date de naissance dans l'ensemble de données relatives aux passagers aériens de leur(s) parent(s). Si les parents réservent un billet d'avion séparément pour leur enfant, ce qui est autorisé dès l'âge de cinq ans, celui-ci dispose de son propre ensemble de données relatives aux passagers aériens. Dès qu'ils atteignent l'âge de douze ans, les enfants sont considérés comme des adultes dans l'aviation et ont leur propre PNR.

Il se peut aussi que des enfants voyagent seuls, ce qui est autorisé chez SWISS et Lufthansa à partir de cinq ans. Dans ce cas, un collaborateur du service d'assistance de l'entreprise de transport aérien doit accompagner l'enfant durant toute la durée du vol. Lufthansa recense à elle seule près de 70 000 enfants qui bénéficient de ce service chaque année.

Dans ce cas, la catégorie 12 de l'ensemble de données relatives aux passagers aériens fournit les informations suivantes:

- le nom, le sexe, l'âge et les langues parlées des personnes non accompagnées de moins de 18 ans;
- le nom et les coordonnées de la personne présente au départ et son lien avec la personne mineure;
- le nom et les coordonnées de la personne présente à l'arrivée et son lien avec la personne mineure;
- le nom et les coordonnées de l'agent présent au départ et de l'agent présent à l'arrivée.

7 Aspects juridiques

7.1 Constitutionnalité

La loi sur les données relatives aux passagers aériens impose de nouvelles obligations aux entreprises de transport aérien. La Constitution attribue à la Confédération la compétence de légiférer en matière de transport aérien (cf. art. 87 Cst.).

La loi sur les données relatives aux passagers aériens 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, à savoir la lutte contre les infractions terroristes et les autres infractions pénales graves. Il s'agit de tâches de sécurité que le CPP attribue partiellement à la Confédération en vertu de l'art. 123, al. 1, Cst. (lutte contre les infractions terroristes et les autres infractions pénales graves soumises à la juridiction fédérale). Ces compétences préexistantes de la Confédération sont importantes et les aspects relevant de la sécurité réglés par la loi sur les données relatives aux passagers aériens nécessitent une coordination sous la direction de la Confédération, d'après cette dernière. Par conséquent, la loi sur les données relatives aux passagers aériens peut aussi s'appuyer sur l'art. 57, al. 2, Cst.[86].

7.2 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 (cf. note de bas de page 1). En même temps, elle met en application les normes de l'OACI que l'aviation suisse doit respecter et s'assure de rester dans le VWP des États-Unis. Ce statut important n'est que provisoire pour l'instant (cf. ch. 1.1).

L'avant-projet de loi sur les données relatives aux passagers aériens s'appuyait largement sur la directive PNR de l'UE, même si cela n'était pas obligatoire. L'arrêt de la CJUE a partiellement modifié l'interprétation de cette directive. Il n'a aucun effet contraignant pour la Suisse. Toutefois, certains aspects centraux de cet arrêt ont été pris en compte dans le présent projet de loi, notamment la réduction à six mois du délai de conservation des données ne présentant aucun indice de grande criminalité ainsi que le retrait de certaines catégories d'infractions pour ne garder que celles relevant de la grande criminalité.

86 Rapport du Conseil fédéral donnant suite au postulat Malama 10.3045 du 3 mars 2010. Sécurité intérieure. Clarification des compétences, FF **2012** 4161 4187

Le présent projet de loi se base sur les résultats de la consultation et prend en compte des éléments importants de l'arrêt de la CJUE, dans la mesure où les prises de position reçues dans le cadre de la consultation se réfèrent à ces aspects centraux de l'arrêt et que ces derniers n'ont pas remis fondamentalement en question l'efficacité et l'efficience du PNR.

L'accord du 21 juin 1999 entre la Confédération suisse et la Communauté européenne sur le transport aérien[87] n'est pas concerné par le projet de loi.

7.3 Forme de l'acte à adopter

La nécessité de disposer d'une loi fédérale est principalement justifiée par la nouvelle tâche incombant à la Confédération de par la mise en œuvre de la loi sur les données relatives aux passagers aériens (art. 164, al. 1, let. e, Cst.).

De plus, le traitement des données 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.).

Enfin, la nécessité de régler le traitement des données relatives aux passagers aériens dans une loi au sens formel résulte de la LPD.

7.4 Frein aux dépenses

Le projet ne prévoit pas de nouvelle disposition en matière de subventions, ni de nouveaux crédits d'engagement ou plafonds de dépenses. Il n'est donc pas soumis au frein aux dépenses (cf. art. 159, al. 3, let. b, Cst.).

7.5 Conformité aux principes de subsidiarité et d'équivalence fiscale

Subsidiarité

La Confédération doit assumer une nouvelle tâche, en l'occurrence le traitement de données relatives aux passagers aériens en vue de les communiquer aux autorités fédérales et cantonales compétentes pour lutter contre la grande criminalité.

Le principe de subsidiarité (cf. art. 5*a* Cst.) exige une justification lorsque la Confédération doit se charger d'une tâche.

Le caractère international de la tâche plaide en faveur d'un traitement des données relatives aux passagers aériens effectué par la Confédération:

- cette tâche permet à la Suisse de remplir plusieurs de ses obligations internationales (cf. ch. 1.1);

87 RS **0.748.127.192.68**

- les États-Unis font de la mise en place rapide du PNR une condition au maintien de la Suisse dans le VWP;
- l'échange de données relatives aux passagers aériens avec l'étranger nécessite la conclusion de traités internationaux avec de nombreux États pour garantir la réciprocité avec tous les États et une protection des données appropriée. La Confédération est compétente pour conclure ces traités.

Compte tenu de la compétence constitutionnelle qu'a la Confédération de légiférer en matière de transport aérien, il convient également de lui attribuer cette nouvelle tâche (cf. art. 87 Cst.). En effet, l'utilisation du PNR implique que l'UIP dispose de données que les entreprises de transport aérien lui communiquent. La présente loi prévoit non seulement l'obligation pour les entreprises de transport aérien de communiquer ces données à l'UIP, mais aussi des sanctions si elles ne le font pas à temps ou si les données sont incomplètes. Seule la Confédération dispose de la compétence normative correspondante.

Équivalence fiscale

L'équivalence fiscale découle de l'art. 43*a* Cst. Elle prévoit un rapport équilibré entre l'unité qui bénéficie d'une prestation, celle qui assume les coûts et celle qui prend la décision.

On peut considérer que l'UIP, qui est compétente en matière de traitement des données relatives aux passagers aériens, est un fournisseur de prestations. Elle met les résultats du traitement des données relatives aux passagers aériens à la disposition tant de la Confédération que des cantons, qui sont tous deux les bénéficiaires de cette nouvelle tâche.

Comme la compétence en matière de sécurité intérieure, notamment dans le domaine de la police, incombe principalement aux cantons en vertu de la Constitution, on peut supposer que le PNR est bénéfique essentiellement pour les cantons. Le retrait de certaines catégories d'infractions effectué après la consultation ne change pas fondamentalement la donne. Ce sont surtout des éléments constitutifs de l'infraction prévus par le droit pénal accessoire fédéral qui ont été supprimés, et ils ne concernent les cantons que marginalement. Dans ce contexte, il est justifié que ces derniers mettent à disposition la moitié des collaborateurs de l'UIP et assument les charges financières associées.

La Confédération met à disposition l'autre moitié des collaborateurs de l'UIP et assume les charges financières associées. De plus, elle supporte les coûts relatifs au projet, à l'infrastructure nécessaire et à l'exploitation de l'UIP.

Dans l'ensemble, les cantons ont ainsi à leur charge bien moins de la moitié des coûts liés à la mise en place d'un système PNR en Suisse.

Dans le cadre de la consultation, plusieurs cantons ont demandé que la Confédération prenne à sa charge l'intégralité des coûts, ce qui est en contradiction totale avec le principe d'équivalence fiscale prévu de manière contraignante par le droit constitutionnel. Par conséquent, il n'est pas possible d'entrer en matière sur la demande de ces cantons.

7.6 Délégation de compétences législatives

L'*art. 2, al. 4* confère au Conseil fédéral la compétence de régler par voie d'ordonnance les modalités techniques que les entreprises de transport aérien doivent respecter lorsqu'elles communiquent les données relatives aux passagers aériens à l'UIP. Pour ce faire, le Conseil fédéral s'appuie sur les normes internationales de l'OACI, de l'OMD et de l'IATA, qu'il peut préciser au besoin.

L'*art. 7, al. 4* confère au Conseil fédéral la compétence de régler les modalités relatives à la communication sécurisée des données entre l'UIP et les autorités compétentes. Il ne s'agit pas seulement de définir la manière de communiquer. Il faut également clarifier la question de savoir si les données doivent être échangées de manière standardisée entre les autorités et par le biais de points de contact uniques. Dans le cas des corps de police de la Confédération et des cantons, il pourrait s'agir de la Centrale d'engagement et d'alarme.

L'*art. 15, al. 2* confère au Conseil fédéral la compétence de définir les modalités relatives à la vérification des profils de risque et des listes d'observation. De plus, il doit régler la rédaction du rapport sur les résultats de la vérification.

L'*art. 29, 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 et des organisations internationales (UE) qui garantissent un niveau adéquat ou approprié de protection des données provenant de Suisse au moyen de dispositions contractuelles spécifiques. De plus, les traités doivent garantir la réciprocité de la communication des données.

7.7 Protection des données

La loi sur les données relatives aux passagers aériens s'inscrit dans le droit fil de la nouvelle LPD, qui est entrée en vigueur le 1er septembre 2023. Cela est d'autant plus important que cette protection joue un rôle central dans le traitement des données au sens de la loi sur les données relatives aux passagers aériens. Ce point est aussi ressorti de la consultation qui s'est déroulée durant le premier semestre 2022. Plusieurs prises de position reçues se fondent sur l'arrêt de la CJUE. Le projet de loi prend en compte des éléments clés de cet arrêt bien que ce dernier n'ait aucun effet contraignant pour la Suisse. Par exemple, la loi sur les données relatives aux passagers aériens prévoit la réduction à six mois du délai de conservation des données ne présentant aucun indice de grande criminalité ainsi que le retrait de certaines catégories d'infractions pour ne garder que celles relevant effectivement de la grande criminalité. En revanche, les contenus de l'arrêt qui auraient considérablement altéré l'efficacité et l'efficience du PNR n'ont pas été retenus.

Données personnelles

L'ensemble de données relatives aux passagers aériens comprend différentes catégories. Celles qui relèvent de la protection des données sont uniquement les données personnelles (art. 2, al. 1, let. b, LPD). Il s'agit des données concernant une personne physique identifiée ou identifiable (art. 5, let. a, LPD). La loi sur les données relatives aux passagers aériens prévoit ces données aux catégories 4 à 6, 8, 9, 12, 17 et 18; la catégorie 19 *peut* contenir des données personnelles (cf. annexe 1 du P-LDPa). Sont notamment concernés le nom, le numéro de téléphone, l'adresse de domicile et l'adresse électronique d'un passager aérien.

Les données relatives aux passagers aériens qui ne présentent aucun indice d'infraction pénale visée à l'annexe 2 et qui ne sont donc pas marquées sont automatiquement pseudonymisées un mois après avoir été saisies dans le système d'information PNR (cf. art. 18). Grâce à cette pseudonymisation, il n'est plus possible d'attribuer les données à une certaine personne. Elles perdent alors leur statut de données personnelles. Contrairement à l'anonymisation, processus par lequel les données perdent irrévocablement leur statut de données personnelles, la pseudonymisation peut être annulée (cf. art. 19 et 20). Le TAF doit autoriser cette étape de traitement. Sur le plan technique, il est prévu que seules les personnes autorisées puissent exécuter cette décision en se référant à l'arrêt en question.

Dans son message du 15 septembre 2017 sur la révision totale de la LPD[88], le Conseil fédéral souligne que la pseudonymisation est une mesure technique appropriée pour garantir la sécurité des données (cf. art. 8 LPD). Il 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 […]. Cette dernière règle vaut aussi pour les données pseudonymisées"[89].

Données sensibles

La loi autorise uniquement le traitement des données sensibles visées à l'art. 5, al. 2. Il se peut que l'UIP entre en possession de ces données lorsqu'elle vérifie manuellement les concordances obtenues par suite de la comparaison automatique (cf. art. 6, al. 3, P-LDPa).

Le projet de loi prend en compte les réserves de la CJUE concernant la description des différentes catégories de données (cf. annexe 1 du P-LDPa)[90]. Il est donc légalement exclu que l'UIP puisse entrer en possession de données sensibles par le biais des données relatives aux passagers aériens. Néanmoins, l'art. 22, let. a prévoit, à titre préventif, que l'UIP doit effacer sans délai toutes les données sensibles qui ne sont pas visées à l'art. 5, al. 2.

88 FF **2017** 6650
89 FF **2017** 6640
90 Affaire C-817/19, ECLI:EU:C:2022:491, ch. marg. 130 à 140

Durée de conservation

Le projet de loi sur les données relatives aux passagers aériens prévoit que les données non marquées sont effacées automatiquement six mois après leur introduction dans le système d'information PNR (cf. art. 21, al. 1). En ce sens, il reprend l'arrêt de la CJUE, qui explique les éléments suivants à ce sujet:

"Ainsi, eu égard aux finalités de la directive PNR et aux besoins des enquêtes et des poursuites en matière d'infractions terroristes et de formes graves de criminalité, il y a lieu de considérer que la conservation, au cours de la période initiale de six mois, des données PNR de l'ensemble des passagers aériens soumis au système instauré par cette directive, sans qu'il existe la moindre indication de leur implication dans des infractions terroristes ou des formes graves de criminalité, ne paraît pas, par principe, excéder les limites du strict nécessaire, dans la mesure où elle permet les recherches nécessaires aux fins d'identifier des personnes qui n'étaient pas soupçonnées de participation à des infractions terroristes ou à des formes graves de criminalité.[91]"

En revanche, les données marquées (cf. art. 7, al. 3) doivent être enregistrées pendant une période de cinq ans si leur marquage n'a pas été supprimé avant (cf. art. 21, al. 2). La CJUE considère que cette durée de conservation est justifiée. Voici ce qu'elle dit à ce propos:

"Dans la mesure où, toutefois, sont identifiés, dans des cas particuliers, des éléments objectifs, tels que les données PNR des passagers ayant donné lieu à une concordance positive vérifiée, qui permettent de considérer que certains passagers pourraient présenter un risque en matière d'infractions terroristes ou de formes graves de criminalité, un stockage de leurs données PNR paraît admissible au-delà de cette période initiale […]. En effet, l'identification de ces éléments objectifs serait de nature à établir un rapport avec les objectifs poursuivis par les traitements au titre de la directive PNR, de sorte que la conservation des données PNR relatives à ces passagers serait justifiée pendant le délai maximal admis par ladite directive, à savoir pendant cinq ans.[92]"

Les données ne peuvent être marquées et donc soumises à la durée de conservation de cinq ans que dans la mesure du nécessaire. Cette durée de conservation devient inutile dès lors que l'autorité compétente constate qu'elle n'a plus besoin des données. C'est par exemple le cas lorsqu'une procédure d'enquête ou de poursuite pénale en cours révèle que des éléments objectifs ne sont pas soutenables. La loi sur les données relatives aux passagers aériens prévoit pour ce genre de cas que l'autorité doit en informer l'UIP. Celle-ci supprime alors le marquage. Les données concernées sont à nouveau non marquées et soumises aux dispositions en la matière.

91 Affaire C-817/19, ECLI:EU:C:2022:491, ch. marg. 255
92 Affaire C-817/19, ECLI:EU:C:2022:491, ch. marg. 259 et 260

Les données ne peuvent être traitées que dans le but prévu par la loi (art. 6, al. 4, LPD).

Conformément à l'art. 5, al. 1, les données relatives aux passagers aériens ne peuvent être traitées que dans le but de lutter contre la grande criminalité. Les éléments constitutifs de l'infraction admis figurent à l'annexe 2 de la loi. Les profils de risque et les listes d'observation ne peuvent être utilisés qu'à des fins supplémentaires restreintes (cf. art. 12 à 14).

L'UIP doit vérifier que le but légal du traitement des données est respectée avant toute communication de concordances obtenues par suite de la comparaison automatique des données (cf. art. 6, al. 3, let. a). Elle doit effacer sans délai les concordances qui ne remplissent pas ce but (cf. art. 22, let. b, ch. 1).

Cette obligation de vérification s'applique par analogie à la communication des autres données à une autorité compétente (cf. art. 8, al. 2, et 9, al. 3).

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 chacune des concordances obtenues par la comparaison automatique des données et, le cas échéant, par un accès à des systèmes d'information supplémentaires. Elle doit notamment vérifier l'identité du passager aérien concerné (cf. art. 6, al. 3, let. b). Si ce dernier ne correspond pas à la personne recherchée, l'UIP doit effacer sans délai la concordance (cf. art. 22, let. b, ch. 2). Cette obligation de vérification s'applique par analogie aux autres résultats de traitement avant d'être communiqués à une autorité compétente (cf. art. 8, al 2, et 9, al. 3).

La protection des données doit être garantie au moyen de mesures techniques appropriées (art. 7 LPD).

La protection des données est mise en œuvre sur le plan technique grâce aux automatismes que prévoit la loi sur les données relatives aux passagers aériens pour les nombreuses étapes de traitement (pseudonymisation des données non marquées [cf. art. 18, al. 1], effacement de ces données après six mois, effacement des données marquées après cinq ans). Ces étapes importantes de traitement doivent être effectuées en continu et en temps utile, raison pour laquelle elles sont automatiques (cf. art. 18, al. 1, et 22).

L'établissement de profils de risque pose des exigences techniques élevées. Ces derniers ne doivent en effet livrer que quelques concordances ou celles effectivement nécessaires. C'est pourquoi les profils de risque doivent être obligatoirement testés avant d'être utilisés. Ces tests sont exclusivement effectués au moyen de données synthétiques. En complément à cette disposition, le Conseil fédéral vérifie l'utilisation des profils de risque. Cette surveillance est une mesure supplémentaire qui garantit que la structure des profils de risque soit à jour et pertinente et que leur utilisation se limite au strict nécessaire (cf. art. 15).

Des mesures organisationnelles doivent également être prises pour protéger les données (art. 7 LPD).

Le fait que l'organisation et le personnel de l'UIP soient distincts de ceux des unités potentiellement destinataires de résultats de traitement de l'UIP est, sur le plan légal, une mesure organisationnelle (cf. art. 27, al. 2). Ainsi, et compte tenu du devoir de discrétion auquel sont soumis les collaborateurs de l'UIP (cf. art. 28, al. 4), les risques d'échanges informels d'individu à individu sont réduits au maximum sur les plans organisationnel et légal.

Dans deux domaines, la présente loi dispose en outre que l'UIP ne peut pas décider en toute autonomie, mais qu'elle dépend de la décision rendue par une instance judiciaire, à savoir:

- le tribunal des mesures de contrainte compétent, qui décide si une liste d'observation contenant les données d'un tiers (cf. art. 14) peut être utilisée;
- le TAF, qui décide si les conditions permettant la levée de la pseudonymisation de certaines données sont remplies (cf. art. 19 et 20).

Des mesures techniques assurent également une sécurité adéquate des données relatives aux passagers aériens (art. 8 LPD).

La protection des données individuelles n'est possible que si, dans le même temps, des mesures techniques générales sont prises en matière de sécurité des données. Celle-ci vise les données disponibles et comprend le cadre technique et organisationnel général du traitement des données. Conformément à l'art. 8 LPD, fedpol doit prévoir une architecture sécuritaire appropriée pour le système d'information PNR de sorte que les données relatives aux passagers aériens et les résultats du traitement soient sécurisés.

Les données relatives aux passagers aériens et les résultats de leur traitement sont enregistrés au sein de l'administration fédérale auprès du CSI-DFJP. Il en va de même pour les procès-verbaux de journalisation, qui doivent toutefois être enregistrés séparément des données opérationnelles.

Comme le mentionne le Conseil fédéral dans son 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, la pseudonymisation constitue une telle mesure[93]. La loi sur les données relatives aux passagers aériens prévoit la pseudonymisation (cf. art. 18) des données relatives aux passagers aériens non marquées. Font également partie de ces données non marquées celles dont le marquage a été supprimé a posteriori et qui datent d'au moins un mois, mais pas de plus de six mois (cf. art. 18). La pseudonymisation consiste à attribuer un pseudonyme aux données d'un dossier passager qui donnent des renseignements sur la personne physique concernée.

Il est certes possible d'annuler la pseudonymisation, contrairement à l'anonymisation, mais uniquement si le TAF l'autorise (cf. art. 19 et 20). Sur le plan

93 FF **2017** 6565 6650

technique, seule la direction de l'UIP est habilitée à mettre en œuvre une telle décision prise par le TAF. Elle peut alors accéder au tableau des concordances pour lever la pseudonymisation dans le cadre autorisé. Ce faisant, la personne habilitée doit également présenter l'arrêt du TAF légitimant cette étape.

Toutes ces mesures expliquent le passage suivant du message susmentionné du Conseil fédéral: "la loi [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."

Analyse du besoin de protection et analyse d'impact relative à la protection des données personnelles

L'administration fédérale procède à une analyse préalable du besoin de protection pour chaque projet informatique. Le moment auquel cette analyse est menée est régi par le modèle de gestion de projet HERMES. L'analyse doit être établie pendant la phase d'initialisation, ce qui garantit une prise en compte de la sécurité informatique dès le début du projet.

Pour le projet PNR Suisse, une analyse du besoin de protection a été établie dans le cadre de HERMES. Elle a été examinée par le préposé à la sécurité de fedpol puis signée en mars 2021.

Sur la base de la LPD, les risques en matière de protection des données liés aux données personnelles saisies par les compagnies aériennes et communiquées à la police ont été identifiés et des mesures ont été définies en conséquence dans une analyse d'impact relative à la protection des données personnelles (AIPD) en tenant compte de l'analyse du besoin de protection.

L'AIPD présentait 14 risques potentiels de violation des droits fondamentaux ("risques bruts"), prévenus au moyen de 22 mesures organisationnelles, juridiques et techniques. Ces mesures ont permis de faire passer les risques bruts, dont certains se situaient au niveau "élevé", aux niveaux "moyen" voire "faible" s'agissant de la probabilité de leur survenance et de l'étendue des dommages. Ainsi, l'AIPD ne présente plus aucun risque résiduel potentiellement élevé.

Comme le projet législatif ne demande pas aux compagnies aériennes de saisir des données personnelles supplémentaires, il n'existe aucun risque de plus que les risques résiduels indiqués dans l'AIPD pour la personnalité et les droits fondamentaux des personnes concernées.

Dans sa prise de position du 5 avril 2024 sur l'AIPD, le PFPDT souligne que l'analyse a été soigneusement établie et que la probabilité que des dommages importants surviennent pour une partie des risques résiduels est faible. Le service spécialisé responsable du traitement estime donc que les risques résiduels identifiés sont globalement raisonnables. Le PFPDT n'a pas jugé nécessaire de formuler des objections compte tenu de la clarté de l'AIPD élaborée dans les règles de l'art, d'autant plus que sa marge d'appréciation ne remplace pas

sans nécessité celle qui revient aux services spécialisés dans l'évaluation des risques.

Annexe (projet d'acte)