Conseil de
l'Union européenne

Bruxelles, le 14 décembre 2022
(OR. en)

15719/22

Dossier interinstitutionnel:
2022/0425(COD)

IXIM 292
ENFOPOL 639
AVIATION 319
DATAPROTECT 363
JAI 1678
CODEC 2012
IA 223

PROPOSITION

Origine:	Pour la secrétaire générale de la Commission européenne, Madame Martine DEPREZ, directrice
Date de réception:	14 décembre 2022
Destinataire:	Madame Thérèse BLANCHET, secrétaire générale du Conseil de l'Union européenne
N° doc. Cion:	COM(2022) 731 final
Objet:	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

Les délégations trouveront ci-joint le document COM(2022) 731 final.

p.j.: COM(2022) 731 final

COMMISSION
EUROPÉENNE

Strasbourg, le 13.12.2022
COM(2022) 731 final

2022/0425 (COD)

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

{SWD(2022) 424 final}

EXPOSÉ DES MOTIFS

1. CONTEXTE DE LA PROPOSITION

• Justification et objectifs de la proposition

Ces dix dernières années, l'Union européenne et d'autres régions du monde ont vu une augmentation des formes graves de criminalité et de la criminalité organisée. Selon l'évaluation de la menace que représente la grande criminalité organisée, réalisée par Europol, dans la plupart des cas, la criminalité organisée implique des voyages internationaux, qui visent généralement à faire entrer illégalement des personnes, des drogues ou d'autres produits illicites dans l'Union. Les criminels utilisent ainsi fréquemment les grands aéroports de l'Union ainsi que les aéroports régionaux de plus petite taille qui accueillent les compagnies aériennes à bas coûts[1]. De même, le rapport d'Europol sur la situation et les tendances du terrorisme indique que la menace terroriste dans l'Union demeure réelle et sérieuse[2]. Il souligne que la plupart des campagnes terroristes sont de nature transnationale et se caractérisent par des contacts transnationaux ou des voyages en dehors de l'Union. Dans ce contexte, les informations sur les voyageurs aériens constituent un outil important pour permettre aux autorités répressives de lutter contre les formes graves de criminalité et le terrorisme au sein de l'Union.

Les données des voyageurs aériens comprennent les informations préalables sur les passagers (API) et les dossiers passagers (PNR) qui, lorsqu'ils sont utilisés ensemble, offrent un moyen particulièrement efficace d'identifier les voyageurs à haut risque et de confirmer les habitudes de voyage de personnes suspectes. Lorsqu'un passager achète un billet auprès d'un transporteur aérien, les systèmes de réservation des transporteurs aériens génèrent un PNR aux fins de leurs activités. Ce PNR inclut des données sur l'itinéraire complet, les détails du paiement, les coordonnées de contact et les demandes spéciales du passager. Lorsqu'il existe une obligation en ce sens, les données de ce dossier passager sont envoyées à l'unité d'informations passagers (UIP) du pays de destination et, souvent, du pays d'origine.

Dans l'Union, la directive PNR[3] a été adoptée en 2016 afin que tous les États membres appliquent les règles en matière de collecte des données PNR auprès des transporteurs aériens aux fins de la prévention et de la détection des infractions terroristes et des formes graves de criminalité, ainsi que des enquêtes et des poursuites en la matière, sans remettre en cause les règles de l'Union existantes imposant aux transporteurs aériens de recueillir des données API, énoncées dans la directive API[4]. Conformément à la directive PNR, les États membres doivent adopter les mesures nécessaires pour que les transporteurs aériens transfèrent les données PNR, pour autant qu'ils aient déjà recueilli de telles données dans le cadre normal de leurs activités. La directive PNR permet le traitement conjoint des données API et des données PNR, puisque sa définition de ces dernières englobe «toute information préalable sur

---

1 Europol, Serious and Organised Crime Threat Assessment (SOCTA), 2021, https://www.europol.europa.eu/cms/sites/default/files/documents/socta2021_1.pdf.

2 Europol, Terrorism Situation and Trend Report (Te-SAT), 2021, https://www.europol.europa.eu/cms/sites/default/files/documents/tesat_2021_0.pdf.

3 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.

4 Directive 2004/82/CE du Conseil du 29 avril 2004 concernant l'obligation pour les transporteurs de communiquer les données relatives aux passagers.

les passagers (données API) qui a été recueillie»[5]. Elle n'oblige toutefois pas les transporteurs aériens à recueillir des données en dehors du cadre normal de leurs activités. Par conséquent, la directive PNR ne permet pas la collecte de l'ensemble complet des données API, les transporteurs aériens n'ayant pas d'intérêt commercial à recueillir ces données dans le cadre normal de leurs activités.

Ce n'est que lorsqu'il existe une obligation en ce sens que le transporteur aérien recueille des données API lors de l'enregistrement du passager (enregistrement en ligne et à l'aéroport). Elles sont ensuite envoyées aux autorités frontalières compétentes sous la forme d'un «manifeste des passagers» mentionnant tous les passagers présents à bord au moment du départ de l'avion. Alors que les données API sont considérées comme des informations «vérifiées», puisqu'elles correspondent aux voyageurs qui ont effectivement embarqué dans l'aéronef, et peuvent être utilisées par les autorités répressives pour identifier des suspects et des personnes recherchées, les données PNR, elles, sont des informations «non vérifiées» fournies par les passagers. Les données PNR d'un passager particulier ne contiennent généralement pas tous les éléments PNR potentiels, mais uniquement ceux fournis par le passager et/ou nécessaires à la réservation, et donc à l'exercice des activités du transporteur aérien.

Depuis l'adoption de la directive API en 2004, il est généralement admis que les données API constituent non seulement un instrument essentiel à la gestion des frontières, mais aussi un précieux outil à des fins répressives, notamment pour lutter contre les formes graves de criminalité et le terrorisme. C'est pourquoi au niveau international, depuis 2014, les résolutions du Conseil de sécurité des Nations unies ont appelé à maintes reprises à la mise en place et au déploiement mondial de systèmes API et PNR à des fins répressives[6]. En outre, l'engagement pris par les États participants de l'Organisation pour la sécurité et la coopération en Europe (OSCE) à mettre en place des systèmes API confirme l'importance de l'exploitation de ces données dans la lutte contre le terrorisme et la criminalité transnationale.[7]

Comme l'indique le rapport de la Commission sur le réexamen de la directive PNR, le traitement conjoint des données API et PNR par les autorités répressives compétentes – ce qui signifie que les données PNR recueillies par les transporteurs aériens dans le cadre normal de leurs activités et transférées aux autorités répressives compétentes sont complétées par l'obligation imposée aux transporteurs aériens de recueillir et de transférer les données API – augmente sensiblement l'efficacité de la lutte contre les formes graves de criminalité et le terrorisme au sein de l'Union[8]. L'utilisation combinée des données API et des données PNR permet aux autorités nationales compétentes de confirmer l'identité des passagers et d'améliorer considérablement la fiabilité des données PNR. Cette utilisation combinée avant l'arrivée des passagers permet aussi aux autorités répressives de procéder à une évaluation et de ne contrôler étroitement que les personnes les plus susceptibles de représenter une menace pour la sécurité, sur la base de critères d'évaluation et de pratiques objectifs et conformément

---

5 Voir annexe 1, point 18, de la directive (UE) 2016/681.

6 Résolutions 2178(2014), 2309(2016), 2396(2017) et 2482(2019) du Conseil de sécurité des Nations unies, et décision 6/16 du Conseil ministériel de l'OSCE du 9 décembre 2016 sur le renforcement de l'utilisation des renseignements préalables concernant les voyageurs.

7 Décision 6/16 du Conseil ministériel de l'OSCE du 9 décembre 2016 sur le renforcement de l'utilisation des renseignements préalables concernant les voyageurs.

8 Commission européenne, «Staff Working Document Accompanying the Report on the review of Directive 2016/681», SWD(2020)128 final.

au droit applicable. Cette pratique facilite le déplacement de tous les autres passagers et réduit le risque qu'ils soient soumis, à leur arrivée, à un contrôle des autorités compétentes fondé sur des éléments discrétionnaires, tels que la race ou l'origine ethnique, que les autorités répressives peuvent, à tort, associer à des risques pour la sécurité.

Cependant, le cadre juridique actuel de l'Union régit uniquement l'utilisation des données PNR pour lutter contre les formes graves de criminalité et le terrorisme, mais pas celle des données API, qui ne peuvent être réclamées que pour les vols en provenance de pays tiers, ce qui crée une faille de sécurité, notamment en ce qui concerne les vols intra-UE pour lesquels les États membres demandent aux transporteurs aériens de transférer des données PNR. Les unités d'informations passagers (UIP) obtiennent les résultats opérationnels les plus efficaces sur les vols pour lesquels tant des données API que des données PNR sont recueillies. Les autorités répressives compétentes ne peuvent donc bénéficier des résultats du traitement conjoint des données API et des données PNR sur les vols intra-UE, pour lesquels seules des données PNR sont transférées.

Pour remédier à cette faille, dans sa stratégie pour un espace Schengen pleinement opérationnel et résilient, publiée en juin 2021, la Commission a préconisé une utilisation accrue des données API combinées aux données PNR sur les vols intra-UE, afin d'améliorer sensiblement la sécurité intérieure, dans le respect du droit fondamental à la protection des données à caractère personnel et du droit fondamental à la liberté de circulation[9].

La proposition de règlement vise dès lors à établir de meilleures règles en matière de collecte et de transfert des données API par les transporteurs aériens aux fins de la prévention et de la détection des infractions terroristes et des formes graves de criminalité, ainsi que des enquêtes et des poursuites en la matière. Afin de garantir le respect des droits fondamentaux pertinents inscrits dans la charte des droits fondamentaux de l'Union européenne (ci-après, la «charte»), en particulier le respect de la vie privée et la protection des données à caractère personnel, et des exigences de nécessité et de proportionnalité qui en découlent, la proposition est, comme il est expliqué ci-après, rigoureusement limitée dans son champ d'application et contient des limites strictes et des garanties en matière de protection des données à caractère personnel.

- **Cohérence avec les dispositions existantes dans le domaine d'action**

Les règles proposées en matière de collecte et de transfert des données API aux fins de la prévention et de la détection des infractions terroristes et des formes graves de criminalité, ainsi que des enquêtes et des poursuites en la matière, sont alignées sur les règles applicables en matière de traitement des données PNR, établies dans la directive PNR[10]. Elles tiennent compte des interprétations données par la Cour de justice de l'Union européenne dans sa jurisprudence récente, notamment au sujet du traitement des données PNR sur les vols intra-UE, à savoir que le transfert des données PNR aux autorités compétentes des États membres sur les vols intra-UE doit être sélectif et ne peut être systématique, à moins d'être justifié par une menace terroriste réelle et actuelle ou prévisible[11].

---

9 COM(2021) 277 final du 2.6.2021.

10 La directive PNR fixe les conditions du traitement de ces données, telles que les autorités compétentes concernées (article 7), la période de conservation des données (article 12) et la protection des données à caractère personnel (article 13).

11 Arrêt de la CJUE dans l'affaire C-817/19, Ligue des droits humains.

Dans la mesure où il existe une possibilité de chevauchement entre la proposition de règlement et les dispositions de la directive PNR, étant donné que – comme il a été précisé ci-dessus – dans ladite directive, la définition des «données PNR» inclut «toute information préalable sur les passagers (données API) qui a été recueillie», les dispositions de la proposition de règlement priment, car ce dernier est à la fois lex specialis et lex posterior. Si, conformément à la directive PNR, les États membres doivent adopter les mesures nécessaires pour que les transporteurs aériens transfèrent les données PNR, pour autant qu'ils aient déjà recueilli de telles données dans le cadre normal de leurs activités, le règlement proposé impose quant à lui aux transporteurs aériens de recueillir des données API dans certaines situations et de les transférer d'une manière bien précise. Le règlement proposé complète donc la directive PNR, puisqu'il fait en sorte que, dans tous les cas dans lesquels les autorités répressives compétentes –à savoir les UIP – reçoivent des données PNR au titre de la directive PNR, les transporteurs aériens soient tenus de recueillir et de transférer également des données API auxdites autorités.

Après la transmission des données API aux UIP établies par la directive PNR, outre les exigences limitées à cet égard définies dans la proposition de règlement, les règles régissant le traitement ultérieur des données API par les UIP sont celles définies dans la directive PNR. Comme il a été mentionné , la directive PNR permet le traitement conjoint des données API et des données PNR, puisque sa définition de ces dernières inclut «toute information préalable sur les passagers (données API) qui a été recueillie», y compris, par conséquent, les données API reçues par les UIP en application du règlement proposé. Par conséquent, les règles de l'article 6 et des articles 9 et suivants de la directive PNR s'appliquent, en ce qui concerne des aspects tels que les finalités précises du traitement, les périodes de conservation, l'effacement, l'échange d'informations, le transfert par les États membres à des pays tiers et les dispositions particulières concernant la protection de ces données à caractère personnel.

En outre, les actes du droit de l'Union généralement applicables s'appliqueront conformément aux conditions qui y sont stipulées. En ce qui concerne le traitement des données à caractère personnel, c'est, notamment, le cas du règlement général sur la protection des données (RGPD)[12], de la directive en matière de protection des données dans le domaine répressif[13], et du règlement relatif à la protection à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union[14]. Ces actes ne sont pas affectés par la présente proposition.

L'applicabilité des actes du droit de l'Union susvisés au traitement des données API reçues au titre du présent règlement signifie que les États membres appliquent le droit de l'Union au sens de l'article 51, paragraphe 1, de la charte des droits fondamentaux de l'Union européenne (ci-après, la «charte»), et donc que les règles de la charte s'appliquent également.

---

12 Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

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

14 Règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) nº 45/2001 et la décision nº 1247/2002/CE (JO L 295 du 21.11.2018, p. 39).

En particulier, les dispositions de ces actes du droit de l'Union doivent être interprétées à la lumière de la charte.

Afin de garantir la cohérence avec les règles établies dans la proposition de règlement concernant la collecte et le transfert des données API aux fins du contrôle aux frontières et de garantir l'efficience de la transmission des données API, la présente proposition prévoit l'obligation pour les transporteurs aériens de recueillir le même ensemble de données API et de le transférer au même routeur mis en place par cet autre règlement proposé.

La collecte des données API contenues dans les documents de voyage est également cohérente avec les lignes directrices de l'OACI sur les documents de voyage lisibles à la machine[15], qui sont transposées dans le règlement (UE) 2019/1157 relatif au renforcement de la sécurité des cartes d'identité des citoyens de l'Union, dans la directive 2019/997 du Conseil sur les titres de voyage provisoires de l'Union européenne, et dans le règlement (CE) nº 2252/2004 établissant des normes pour les éléments de sécurité et les éléments biométriques intégrés dans les passeports. Ces règlements sont les précurseurs devant permettre une extraction automatisée de données complètes et de grande qualité à partir des documents de voyage.

2. BASE JURIDIQUE, SUBSIDIARITÉ ET PROPORTIONNALITÉ

• Base juridique

Pour la présente proposition de règlement relatif à la collecte et au transfert des données API 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, au vu de son objectif et des mesures prévues, la base juridique appropriée est l'article 82, paragraphe 1, point d), et l'article 87, paragraphe 2, point a), du traité sur le fonctionnement de l'Union européenne (TFUE).

L'article 82, paragraphe 1, point d), du TFUE confère à l'Union le pouvoir d'adopter des mesures visant à faciliter la coopération entre les autorités judiciaires ou équivalentes des États membres dans le cadre des poursuites pénales et de l'exécution des décisions. L'article 87, paragraphe 2, point a), du TFUE confère à l'Union le pouvoir d'adopter des mesures portant sur la collecte, le stockage, le traitement, l'analyse et l'échange d'informations pertinentes aux fins de la coopération policière au sein de l'Union.

Par conséquent, la base juridique retenue pour la présente proposition est la même que celle de la directive PNR, ce qui est approprié, étant donné non seulement que la proposition de règlement poursuit le même objectif, mais aussi qu'elle vise à compléter la directive PNR.

• Subsidiarité

Les autorités répressives doivent être dotées d'outils efficaces pour lutter contre le terrorisme et les formes graves de criminalité. Comme les formes de criminalité les plus graves et les actes terroristes impliquent des voyages internationaux, souvent aériens, les données PNR se sont avérées un moyen très efficient de protéger la sécurité intérieure de l'Union. Par ailleurs, les enquêtes aux fins de la prévention et de la détection des infractions terroristes et des formes graves de criminalité, ainsi que des enquêtes et des poursuites en la matière, menées

[15] OACI, Document 9303, Documents de voyage lisibles à la machine, Huitième édition, 2021, disponible à l'adresse suivante: https://www.icao.int/publications/documents/9303_p1_cons_fr.pdf.

par les autorités compétentes des États membres dépendent dans une large mesure de la coopération internationale et transfrontière.

Dans un espace exempt de contrôles aux frontières intérieures, la collecte, le traitement et l'échange de données sur les passagers, dont les données PNR et API, par les États membres constituent également des mesures compensatoires efficientes. Grâce à une action cohérente au niveau de l'Union, la proposition contribuera à renforcer la sécurité des États membres et, par extension, de l'Union dans son ensemble.

La directive API fait partie de l'acquis de Schengen relatif au franchissement des frontières extérieures. Elle ne régit donc pas la collecte et le transfert des données API sur les vols intra-UE. En l'absence de données API pour compléter les données PNR pour ces vols, les États membres ont mis en œuvre toute une série de mesures différentes qui visent à compenser le manque de données d'identité sur les passagers. Parmi celles-ci, des contrôles de conformité physiques destinés à vérifier les données d'identité entre le document de voyage et la carte d'embarquement, qui génèrent de nouveaux problèmes sans résoudre le problème sous-jacent de l'absence de données API.

Une action au niveau de l'Union permettra l'application de dispositions harmonisées en matière de protection des droits fondamentaux, en particulier la protection des données à caractère personnel, dans les États membres. Les divers systèmes des États membres qui ont déjà mis en place des mécanismes similaires, ou qui le feront à l'avenir, peuvent avoir des conséquences négatives pour les transporteurs aériens, qui pourraient devoir se conformer à plusieurs exigences nationales divergentes, par exemple en ce qui concerne les types d'informations à transférer et les conditions auxquelles ces informations doivent être fournies aux États membres. Ces divergences nuisent à une coopération efficace entre les États membres aux fins de la prévention et de la détection des infractions terroristes et des formes graves de criminalité, ainsi que des enquêtes et des poursuites en la matière. De telles règles harmonisées ne peuvent être fixées qu'au niveau de l'Union.

Étant donné que les objectifs de la présente proposition ne peuvent pas être atteints de manière suffisante par les États membres mais peuvent l'être mieux au niveau de l'Union, il peut être conclu que l'Union est à la fois en droit d'agir et mieux placée pour le faire que les États membres agissant de manière indépendante. La proposition est donc conforme au principe de subsidiarité consacré à l'article 5 du traité sur l'Union européenne.

- **Proportionnalité**

En vertu du principe de proportionnalité établi à l'article 5, paragraphe 4, du traité sur l'Union européenne, la nature et l'intensité d'une mesure donnée doivent correspondre au problème détecté. Tous les problèmes abordés dans la présente initiative législative nécessitent, d'une manière ou d'une autre, une action législative à l'échelle de l'Union pour que les États membres puissent y répondre efficacement.

Les règles proposées en matière de collecte et de transfert des données API, soumises à des limitations strictes et à des garanties, amélioreront la prévention et la détection des infractions terroristes et des formes graves de criminalités, ainsi que les enquêtes et les poursuites en la matière. Par conséquent, les règles proposées correspondent à un besoin constaté de renforcer la sécurité intérieure, répondant ainsi efficacement au problème découlant de l'absence de traitement conjoint des données API et des données PNR, y compris sur les vols intra-UE pour lesquels les États membres reçoivent des données PNR.

Le champ d'application de la proposition est limité au strict nécessaire, autrement dit, les éléments qui nécessitent une approche harmonisée au niveau de l'Union, à savoir les finalités pour lesquelles les données API peuvent être utilisées par les unités d'informations passagers,

les éléments de données qui doivent être recueillis, et les moyens par lesquels les données API doivent être recueillies auprès des voyageurs et transférées. Le transfert des données API au routeur permet aux transporteurs aériens de gérer plus facilement les connexions avec les unités d'informations passagers et d'introduire des économies d'échelle, tout en réduisant les risques d'erreurs et d'utilisation abusive. La finalité couvre uniquement les infractions terroristes et les formes graves de criminalité, telles que définies dans la proposition, au vu de leur gravité et de leur dimension transnationale.

Afin de limiter l'ingérence dans les droits des passagers au strict nécessaire, la proposition prévoit plusieurs garanties. Plus précisément, le traitement des données API au titre de la proposition de règlement est limité à une liste fermée et restreinte de données API. Au-delà de celles-ci, aucune donnée d'identité supplémentaire ne sera recueillie. En outre, la proposition de règlement se contente de prévoir des règles en matière de collecte et de transfert des données API aux UIP au moyen du routeur à des fins limitées précisées dans ladite proposition de règlement et ne régit pas le traitement ultérieur des données API par les UIP, étant donné que, comme expliqué ci-dessus, celui-ci est couvert par d'autres actes du droit de l'Union (la directive PNR, la législation en matière de protection des données, la charte). Les fonctionnalités du routeur et, en particulier, sa capacité à recueillir et à fournir des informations statistiques complètes, facilitent également le suivi de la mise en œuvre du présent règlement par les transporteurs aériens et par les unités d'informations passagers. Certaines garanties particulières sont également prévues, telles que des règles concernant la tenue de registres, la protection des données à caractère personnel et la sécurité.

Afin de garantir la nécessité et la proportionnalité du traitement des données au titre de la proposition de règlement, et plus précisément en ce qui concerne la collecte et le transfert des données API sur les vols intra-UE, les États membres ne recevront des données API que pour les vols intra-UE qu'ils ont sélectionnés conformément à la jurisprudence de la CJUE susvisée. En outre, le traitement ultérieur des données API par les UIP sera soumis aux limites et aux garanties établies dans la directive PNR, telle qu'interprétée par la CJUE dans l'affaire Ligue des droits humains[16] à la lumière de la charte.

- **Choix de l'instrument**

L'instrument proposé est un règlement. Compte tenu de la nécessité que les mesures proposées soient directement applicables et appliquées uniformément dans tous les États membres, le règlement est l'instrument juridique approprié.

3. RÉSULTATS DES ÉVALUATIONS EX POST, DES CONSULTATIONS DES PARTIES INTÉRESSÉES ET DES ANALYSES D'IMPACT

- **Évaluation ex post de la législation existante**

La directive API n'empêche pas le traitement des données API à des fins répressives tel qu'il est prévu dans la législation nationale et conformément aux exigences en matière de protection des données à caractère personnel. Cependant, le recours à cette possibilité dans les États membres est problématique, comme l'a conclu l'évaluation de la directive API, car il

[16] Arrêt de la CJUE du 21 juin 2022 dans l'affaire C-817/19, Ligue des droits humains.

crée des failles de sécurité en l'absence de critères définis au niveau de l'Union en matière de collecte et de transfert des données API à des fins répressives[17]:

– Dans le droit national de certains États membres, la finalité répressive est interprétée dans un sens large, allant d'infractions administratives à la lutte contre le terrorisme et la protection des intérêts nationaux de sécurité, en passant par le renforcement de la sécurité intérieure et de l'ordre public. L'évaluation de la directive API indiquait aussi qu'une utilisation efficace des données API à des fins répressives nécessiterait un instrument juridique spécialement dédié à cet effet[18].

– Les multiples finalités pour lesquelles des données API sont recueillies accroissent la difficulté de faire respecter le cadre de protection des données à caractère personnel institué par l'Union. L'obligation d'effacer les données API dans un délai de 24 heures est applicable uniquement dans le cas où ces données sont utilisées dans l'objectif principal de la directive API, à savoir la gestion des frontières extérieures. La directive n'indique pas clairement si cette obligation s'applique également aux traitements à des fins répressives.

– L'ensemble de données API qui peut être réclamé aux transporteurs aériens à des fins répressives, en plus de la pratique de certains États membres consistant à demander des données API en dehors de la liste non exhaustive figurant dans la directive API, crée un obstacle supplémentaire au respect des différentes exigences par les transporteurs aériens lorsqu'ils transportent des passagers vers l'Union.

– De même, la directive API ne donne aucune indication quant aux vols pour lesquels des données API peuvent être réclamées ni quant aux autorités auxquelles les données API devraient être transférées ou aux conditions d'accès à ces données à des fins répressives.

• **Consultation des parties intéressées**

La préparation de la présente proposition s'est accompagnée de toute une série de consultations des parties concernées, dont les autorités des États membres (autorités frontalières compétentes, unités d'informations passagers), les représentants du secteur des transports, et les différents transporteurs. Les agences de l'Union – telles que l'Agence européenne de garde-frontières et de garde-côtes (Frontex), l'Agence de l'Union européenne pour la coopération des services répressifs (Europol), l'Agence de l'Union européenne pour la gestion opérationnelle des systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice (eu-LISA), et l'Agence des droits fondamentaux de l'Union européenne (FRA), ont aussi apporté leur contribution. La présente initiative intègre également les points de vue et les avis reçus au cours de la consultation publique réalisée à la fin de 2019 dans le cadre de l'évaluation de la directive API[19].

Les activités de consultation menées dans le cadre de la réalisation de l'analyse d'impact qui sous-tend la présente proposition ont permis de recueillir les avis des parties intéressées à l'aide de différentes méthodes. Ces activités comprenaient notamment une analyse d'impact initiale, une étude auxiliaire externe et une série d'ateliers techniques.

---

17 Commission européenne, document de travail des services de la Commission, «Evaluation of the Council Directive 2004/82/EC on the obligation of carriers to communicate passenger data (API Directive)», Bruxelles, 8.9.2020 [SWD(2020)174 final, p. 26 et 43].

18 SWD(2020)174 final, p. 57.

19 SWD(2020) 174 final.

Une analyse d'impact initiale a été publiée afin de recueillir des avis, entre le 5 juin 2020 et le 14 août 2020. Sept contributions ont été reçues, qui s'exprimaient sur l'extension du champ d'application de la future directive API, la qualité des données, les sanctions, la relation entre les données API et les données de dossiers passagers (PNR), et la protection des données à caractère personnel[20].

L'étude auxiliaire externe a été menée sur la base d'une recherche documentaire, d'entretiens et d'enquêtes auprès d'experts en la matière, qui ont examiné différentes mesures possibles pour le traitement des données API avec des règles claires qui facilitent les voyages légitimes et qui sont compatibles avec l'interopérabilité des systèmes d'information de l'Union, les exigences de l'Union en matière de protection des données à caractère personnel, et d'autres instruments de l'Union et normes internationales existants.

Les services de la Commission ont également organisé une série d'ateliers techniques avec des experts des États membres et des pays associés à l'espace Schengen. Ces ateliers avaient pour but de réunir des experts pour qu'ils échangent leurs points de vue sur les options possibles envisagées pour consolider le futur cadre API aux fins de la gestion des frontières, ainsi que de la lutte contre la criminalité et le terrorisme.

L'analyse d'impact qui accompagne la présente proposition contient une description plus détaillée de la consultation des parties intéressées (annexe 2).

- **Analyse d'impact**

Conformément aux lignes directrices pour une meilleure réglementation, la Commission a réalisé une analyse d'impact, présentée dans le document de travail des services de la Commission qui accompagne la présente proposition [référence]. Le comité d'examen de la réglementation a examiné le projet d'analyse d'impact lors de sa réunion du 28 septembre 2022 et a émis un avis favorable le 30 septembre 2022.

Compte tenu des problèmes décelés à l'égard de la collecte et du transfert des données API, l'analyse d'impact a évalué les options stratégiques concernant la portée de la collecte des données API aux fins de la gestion des frontières extérieures et à des fins répressives, ainsi que les options concernant les moyens d'améliorer la qualité des données API. En ce qui concerne la collecte des données API à des fins répressives, l'analyse d'impact a envisagé la collecte des données API sur tous les vols extra-UE d'une part, et la collecte des données API sur tous les vols extra-UE et sur certains vols intra-UE d'autre part. En outre, dans l'analyse d'impact, des options ont également été envisagées en vue d'améliorer la qualité des données API – recueillir les données API soit par des moyens automatisés et manuels, soit par des moyens automatisés uniquement.

Sur la base des conclusions du rapport d'analyse d'impact, l'option privilégiée concernant un instrument API à des fins répressives inclut la collecte des données API sur tous les vols en provenance et à destination de pays tiers, ainsi que sur certains vols intra-UE pour lesquels des données PNR sont transmises. Cette option permettra de renforcer considérablement la robustesse de l'analyse nécessaire des données pertinentes concernant les voyageurs aériens dans la lutte contre les formes graves de criminalité et le terrorisme, les unités d'informations passagers bénéficiant ainsi de la disponibilité de données API, vérifiées et donc de meilleure qualité, afin d'identifier les personnes mêlées à des formes graves de criminalité ou au terrorisme. La collecte et le transfert de données API à des fins répressives s'appuient sur les

[20] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12434-Frontieres-action-repressive-informations-prealables-sur-les-passagers-aeriens-donnees-API-revision-des-regles_fr.

capacités développées pour le transfert des données API, au moyen du routeur, aux fins de la gestion des frontières extérieures sans coûts supplémentaires pour l'eu-LISA. Les transporteurs aériens transmettent les données API uniquement au routeur, qui transmet ensuite ces données à l'unité d'informations passagers de chaque État membre concerné. L'analyse d'impact a conclu qu'il s'agissait d'une solution rentable pour les transporteurs aériens, qui réduit une partie des coûts de transmission supportés par les transporteurs aériens, tout en limitant les risques d'erreurs et d'utilisation abusive. Cependant, contrairement à la situation actuelle, au titre de la proposition de règlement, les transporteurs aériens devraient recueillir et transmettre des données API sur tous les vols couverts, qu'ils en aient besoin ou non dans le cours normal de leurs activités, y compris sur certains vols intra-UE. La proposition est compatible avec l'objectif de neutralité climatique défini dans la loi européenne sur le climat[21] et les objectifs de l'Union pour 2030 et 2040.

- **Droits fondamentaux**

La présente initiative prévoit le traitement des données à caractère personnel des voyageurs et limite donc l'exercice du droit fondamental à la protection de ces données tel qu'il est garanti par l'article 8 de la charte et par l'article 16 du TFUE. Ainsi que l'a souligné la Cour de justice de l'Union européenne(CJEU)[22], le droit à la protection des données à caractère personnel n'apparaît pas comme une prérogative absolue, mais toute limitation doit être prise en considération par rapport à sa fonction dans la société et satisfaire aux critères définis à l'article 52, paragraphe 1, de la charte[23]. La protection des données à caractère personnel est également étroitement liée au droit au respect de la vie privée, dans le cadre du droit au respect de la vie privée et familiale, protégé par l'article 7 de la charte.

Concernant la collecte et le transfert de données API sur certains vols intra-UE, la présente initiative affecte aussi l'exercice du droit fondamental à la liberté de circulation prévu à l'article 45 de la charte et à l'article 21 du TFUE. Selon la CJUE, un obstacle à la liberté de circulation des personnes ne peut être justifié que s'il est fondé sur des considérations objectives et s'il est proportionné à l'objectif légitime des dispositions nationales[24].

Conformément au présent règlement, la collecte et le transfert des données API peuvent uniquement avoir lieu aux fins de la prévention et de la détection des infractions terroristes et des formes graves de criminalité, ainsi que des enquêtes et des poursuites en la matière, tels que définis par la directive PNR. Les dispositions de la présente proposition prévoient des critères uniformes pour la collecte et le transfert des données API sur les vols extra-UE (entrants et sortants) d'une part, et sur certains vols intra-UE d'autre part, sur la base d'une évaluation effectuée par les États membres et sous réserve d'un réexamen régulier, conformément aux exigences définies par la Cour de justice dans l'affaire Ligue des droits humains. L'obligation pour les transporteurs aériens de recueillir et de transmettre des données API au routeur couvre tous les vols intra-UE. La transmission par le routeur à l'UIP est une solution technique en vue de limiter la transmission des données API aux unités

---

21 Article 2, paragraphe 1, du règlement (UE) 2021/1119 du 30 juin 2021 établissant le cadre requis pour parvenir à la neutralité climatique (loi européenne sur le climat).

22 Arrêt de la CJUE du 9 novembre 2010 dans les affaires jointes C-92/09 et C93/09, Volker und Markus Schecke et Eifert, Recueil 2010 I-0000.

23 Conformément à l'article 52, paragraphe 1, de la charte, des limitations peuvent être apportées à l'exercice du droit à la protection des données, dans la mesure où elles sont prévues par la loi, respectent le contenu essentiel du droit et des libertés en cause et, dans le respect du principe de proportionnalité, sont nécessaires et répondent effectivement à des objectifs d'intérêt général reconnus par l'Union européenne ou au besoin de protection des droits et libertés d'autrui.

24 CJUE, arrêt du 5 juin 2018 dans l'affaire C-673/16, Coman.

d'informations passagers sur certains vols uniquement, sans divulguer d'informations confidentielles concernant les vols intra-UE sélectionnés. Ces informations doivent être traitées de manière confidentielle, compte tenu du risque de contournement qui existerait si le grand public ou, plus précisément, les personnes participant à des formes graves de criminalité ou à des activités terroristes, en prenaient connaissance.

L'obligation pour les transporteurs aériens d'utiliser des moyens automatisés pour recueillir les données API des voyageurs peut entraîner des risques, notamment du point de vue de la protection des données à caractère personnel. Ces risques ont cependant été limités et atténués. Premièrement, l'obligation s'applique uniquement à certaines données API, pour lesquelles les moyens automatisés peuvent être utilisés de manière responsable, à savoir pour les données lisibles à la machine sur les documents des voyageurs. Deuxièmement, la proposition de règlement contient des exigences concernant les moyens automatisés à utiliser, qui doivent être précisées dans un acte délégué. Enfin, plusieurs garanties sont prévues, telles que la tenue de registres, des règles particulières concernant la protection des données à caractère personnel et une surveillance efficace.

Par ailleurs, s'il est vrai que – outre la disposition garantissant le respect du principe de limitation de la finalité – la proposition de règlement ne régirait pas l'usage fait par les autorités frontalières compétentes des données API qu'elles reçoivent au titre de celui-ci, étant donné que – comme expliqué ci-dessus – cet usage est déjà couvert par d'autres actes législatifs, dans un souci de clarté, il est néanmoins rappelé dans les considérants qu'un tel usage ne peut donner lieu à aucune des discriminations prévues à l'article 21 de la charte.

4. INCIDENCE BUDGÉTAIRE

La présente initiative législative concernant la collecte et le transfert des données API, respectivement, pour faciliter les contrôles aux frontières extérieures et pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que les enquêtes et les poursuites en la matière, aurait une incidence sur le budget et le personnel nécessaires à l'eu-LISA et aux autorités frontalières compétentes des États membres.

Pour l'eu-LISA, on estime qu'un budget supplémentaire d'environ 45 millions d'EUR [33 millions au titre de l'actuel cadre financier pluriannuel (CFP)] pour mettre le routeur en place et 9 millions d'EUR par an à partir de 2029 pour sa gestion technique, et environ 27 postes supplémentaires seraient nécessaires pour que l'eu-LISA dispose des ressources nécessaires pour exécuter les tâches qui lui sont confiées dans la présente proposition de règlement et dans la proposition de règlement sur la collecte et le transfert des données API pour faciliter les contrôles aux frontières extérieures.

Pour les États membres, il est estimé que 11 millions d'EUR (3 millions d'EUR au titre de l'actuel CFP), consacrés à la mise à niveau des systèmes et infrastructures nationaux nécessaires aux UIP, pourraient faire l'objet d'un remboursement par le Fonds pour la sécurité intérieure[25], et à partir de 2028, progressivement jusqu'à 2 millions d'EUR par an, selon les estimations. Ce droit à remboursement devra en définitive être déterminé conformément aux règles régissant ces fonds ainsi qu'aux règles relatives aux coûts figurant dans la proposition de règlement.

[25] Règlement (UE) 2021/1149 du Parlement européen et du Conseil du 7 juillet 2021 établissant le Fonds pour la sécurité intérieure

Compte tenu du lien étroit entre la présente proposition de règlement et la proposition de règlement sur la collecte et le transfert des données API pour faciliter les contrôles aux frontières extérieures, en particulier en ce qui concerne le transfert des données API au routeur, la fiche financière législative, en annexe de la présente proposition de règlement, est identique pour les deux propositions.

5. AUTRES ÉLÉMENTS

- **Plans de mise en œuvre et modalités de suivi, d'évaluation et d'information**

La Commission veillera à ce que les dispositions nécessaires soient en place pour contrôler le fonctionnement des mesures proposées et les évaluer au regard des principaux objectifs stratégiques. Quatre ans après le début des opérations prévues au titre du règlement API proposé, et tous les quatre ans par la suite, la Commission présentera un rapport au Parlement européen et au Conseil évaluant la mise en œuvre du règlement et sa valeur ajoutée. Le rapport rendra également compte de toute incidence directe ou indirecte sur les droits fondamentaux. Il s'agira d'examiner les résultats obtenus par rapport aux objectifs, de déterminer si les principes de base restent valables et d'en tirer toutes les conséquences pour les options futures.

Le caractère contraignant de l'obligation imposée aux transporteurs aériens de recueillir les données API sur les vols extra-UE et certains vols intra-UE et l'introduction du routeur API permettront d'obtenir une image plus claire du transfert des données API par les transporteurs aériens et de leur utilisation par les États membres conformément à la législation nationale et de l'Union applicable. Cela aidera la Commission dans ses tâches d'évaluation et d'application de la législation, en lui fournissant des statistiques fiables sur le volume de données transmises et sur les vols pour lesquels des données API seraient requises.

- **Explication détaillée de certaines dispositions de la proposition**

Le chapitre 1 énonce les dispositions générales du présent règlement, à commencer par les règles relatives à son objet et à son champ d'application. Il contient également une liste de définitions.

Le chapitre 2 énonce les dispositions relatives à la collecte, au transfert au routeur et à l'effacement des données API par les transporteurs aériens, et les règles relatives à la transmission des données API du routeur aux unités d'informations passagers.

Le chapitre 3 contient des dispositions particulières sur les registres, des précisions permettant de déterminer les responsables du traitement des données à caractère personnel en ce qui concerne le traitement des données API constituant des données à caractère personnel en vertu du présent règlement, et des dispositions sur la sécurité et sur l'autocontrôle par les transporteurs aériens et les UIP.

Le chapitre 4 énonce des règles concernant les connexions au routeur, et l'intégration à celui-ci, par les unités d'informations passagers et les transporteurs aériens, et concernant les coûts exposés par les États membres à cet effet. Il contient également des dispositions régissant le cas d'une impossibilité technique partielle ou totale d'utiliser le routeur et déterminant la responsabilité des dommages causés au routeur.

Le chapitre 5 contient des dispositions concernant le contrôle, les sanctions éventuelles applicables aux transporteurs aériens pour non-respect de leurs obligations définies dans le présent règlement, et l'élaboration d'un manuel pratique par la Commission.

Le chapitre 6 prévoit des modifications à apporter à d'autres instruments existants, à savoir le règlement (UE) 2019/818.

Le chapitre 7 contient les dispositions finales du présent règlement, qui concernent l'adoption d'actes délégués, le suivi et l'évaluation du règlement, et son entrée en vigueur et son application.

2022/0425 (COD)

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

LE PARLEMENT EUROPÉEN ET LE CONSEIL DE L'UNION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 82, paragraphe 1, point d), et son article 87, paragraphe 2, point a),

vu la proposition de la Commission européenne,

après transmission du projet d'acte législatif aux parlements nationaux,

vu l'avis du Comité économique et social européen[26],

statuant conformément à la procédure législative ordinaire,

considérant ce qui suit:

(1) La dimension transnationale de la grande criminalité organisée et la menace constante d'attentats terroristes sur le sol européen appellent une action au niveau de l'Union pour adopter des mesures appropriées, afin d'assurer la sécurité au sein d'un espace de liberté, de sécurité et de justice sans frontières intérieures. Les informations sur les voyageurs aériens, telles que les dossiers passagers (PNR) et en particulier les informations préalables sur les passagers (API), sont essentielles pour identifier les voyageurs à haut risque, notamment ceux qui ne sont pas autrement connus des services répressifs, pour établir des liens entre les membres de groupes criminels, et pour contrer les activités terroristes.

(2) Si la directive 2004/82/CE du Conseil[27] établit un cadre juridique pour la collecte et le transfert de données API par les transporteurs aériens, dans le but d'améliorer le contrôle aux frontières et de lutter contre l'immigration illégale, elle dispose également que les États membres peuvent utiliser les données API à des fins répressives. Toutefois, se borner à offrir une telle possibilité crée un certain nombre de divergences et de lacunes. En particulier, malgré leur utilité à des fins répressives, les données API ne sont pas systématiquement recueillies et transférées par les transporteurs aériens à ces fins. Par ailleurs, lorsque les États membres ont fait usage de cette possibilité, les transporteurs aériens sont confrontés à des exigences divergentes, imposées par le droit national, en ce qui concerne le moment et les modalités de la collecte et du transfert des données API à cette fin. Ces divergences entraînent non seulement des coûts et des complications inutiles pour les transporteurs

[26] JO C , , p. .

[27] Directive 2004/82/CE du 29 avril 2004 du Conseil concernant l'obligation pour les transporteurs de communiquer les données relatives aux passagers (JO L 261 du 6.8.2004, p. 24).

aériens, mais elles peuvent également nuire à la sécurité intérieure de l'Union et à l'efficacité de la coopération entre les services répressifs compétents des États membres. En outre, l'objectif de faciliter le contrôle aux frontières étant différent de celui de la facilitation de l'action répressive, il convient d'établir un cadre juridique distinct pour la collecte et le transfert de données API servant chacun de ces objectifs.

(3) La directive (UE) 2016/681 du Parlement européen et du Conseil[28] établit des règles concernant l'utilisation des données 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. En vertu de cette directive, les États membres doivent adopter les mesures nécessaires pour que les transporteurs aériens transfèrent les données PNR, y compris toute donnée API recueillie, à l'unité nationale d'informations passagers («UIP») créée en vertu de ladite directive, pour autant qu'ils aient déjà recueilli de telles données dans le cadre normal de leurs activités. Par conséquent, ladite directive ne garantit pas la collecte et le transfert de données API dans tous les cas, car la collecte d'un ensemble complet de ces données ne répond à aucune finalité commerciale pour les transporteurs aériens. Il importe de veiller à ce que les UIP reçoivent les données API en même temps que les données PNR, étant donné que le traitement conjoint de ces données est nécessaire pour que les services répressifs compétents des États membres soient en mesure de prévenir et de détecter efficacement les infractions terroristes et les formes graves de criminalité, ainsi que d'enquêter sur celles-ci et d'engager des poursuites. En particulier, ce traitement conjoint permet l'identification précise des passagers qui pourraient devoir faire l'objet d'un examen plus approfondi, conformément au droit applicable, par ces services. En outre, ladite directive ne précise pas quelles informations constituent des données API. Pour ces raisons, il convient d'établir des règles complémentaires imposant aux transporteurs aériens de recueillir et de transférer ensuite un ensemble spécifique de données API, règles qui devraient s'appliquer dans la mesure où les transporteurs aériens sont tenus, en vertu de ladite directive, de recueillir et de transférer des données PNR sur le même vol.

(4) Il est donc nécessaire d'établir, au niveau de l'Union, des règles claires, harmonisées et efficaces en matière de collecte et de transfert des données API aux fins de la prévention et de la détection des infractions terroristes et des formes graves de criminalité, ainsi que des enquêtes et des poursuites en la matière.

(5) Compte tenu de la relation étroite entre les deux actes, le présent règlement devrait être interprété comme complétant les règles prévues par la directive (UE) 2016/681. Par conséquent, les données API devront être recueillies et transférées conformément aux exigences spécifiques prévues dans le présent règlement, notamment pour les cas où cela doit avoir lieu et les modalités à appliquer. Toutefois, les règles de ladite directive s'appliquent à des questions que le présent règlement n'aborde pas, en particulier les règles concernant le traitement ultérieur des données API reçues par les UIP, l'échange d'informations entre les États membres, les conditions d'accès par l'Agence de l'Union européenne pour la coopération des services répressifs (Europol), les transferts vers des pays tiers, la conservation et la dépersonnalisation, et la protection des données à caractère personnel. Dans la mesure où ces règles s'appliquent, les règles de

[28] Directive (UE) 2016/681 du Parlement européen et du Conseil du 27 avril 2016 relative à l'utilisation des données des dossiers passagers (PNR) pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière (JO L 119 du 4.5.2016, p. 132).

ladite directive relatives aux sanctions et aux autorités de contrôle nationales s'appliquent également. Le présent règlement ne devrait pas affecter les règles en question.

(6) La collecte et le transfert des données API ont une incidence sur la vie privée des personnes et impliquent le traitement de données à caractère personnel. Afin de respecter pleinement les droits fondamentaux, en particulier le droit au respect de la vie privée et le droit à la protection des données à caractère personnel, conformément à la charte des droits fondamentaux de l'Union européenne (ci-après la «charte»), il convient de prévoir des limites et des garanties adéquates. En particulier, tout traitement de données API et, en particulier, de données API constituant des données à caractère personnel, devrait rester limité à ce qui est nécessaire et proportionné à la réalisation des objectifs poursuivis par le présent règlement. En outre, il convient de veiller à ce que les données API recueillies et transférées au titre du présent règlement n'entraînent aucune forme de discrimination interdite par la charte.

(7) Compte tenu du caractère complémentaire du présent règlement par rapport à la directive (UE) 2016/681, les obligations incombant aux transporteurs aériens en vertu du présent règlement devraient s'appliquer à tous les vols pour lesquels les États membres doivent exiger des transporteurs aériens qu'ils transmettent les données PNR au titre de la directive (UE) 2016/681, à savoir les vols, qu'ils soient réguliers ou non, entre États membres et pays tiers (vols extra-UE) et entre plusieurs États membres (vols intra-UE), dans la mesure où ces vols ont été sélectionnés conformément à la directive (UE) 2016/681, quel que soit le lieu d'établissement des transporteurs aériens effectuant ces vols.

(8) En conséquence, étant donné que la directive (UE) 2016/681 ne couvre pas les vols intérieurs, c'est-à-dire les vols qui partent et atterrissent sur le territoire du même État membre, sans escale sur le territoire d'un autre État membre ou d'un pays tiers, et compte tenu de la dimension transnationale des infractions terroristes et des formes graves de criminalité relevant du présent règlement, ces vols ne devraient pas non plus être couverts par le présent règlement. Le présent règlement ne devrait pas être interprété comme remettant en cause la possibilité pour les États membres de prévoir, en vertu de leur droit national et dans le respect du droit de l'Union, l'obligation pour les transporteurs aériens de recueillir et de transférer des données API sur ces vols intérieurs.

(9) Compte tenu de la relation étroite entre les actes du droit de l'Union concernés et dans un souci d'homogénéité et de cohérence, les définitions figurant dans le présent règlement devraient, dans la mesure du possible, être alignées sur les définitions figurant dans la directive (UE) 2016/681 et dans le règlement (UE) [API gestion des frontières], et être interprétées et appliquées à la lumière de ces définitions[29].

(10) En particulier, les éléments d'information qui constituent ensemble les données API à recueillir puis à transférer au titre du présent règlement devraient être ceux qui sont énumérés de manière claire et exhaustive dans le règlement (UE) API [gestion des frontières], c'est-à-dire qu'ils devraient couvrir à la fois les informations relatives à chaque passager et les informations relatives au vol pris par ce voyageur. En vertu du présent règlement, ces informations de vol ne devraient comprendre des informations relatives au point de passage frontalier d'entrée sur le territoire de l'État membre

[29] JO C du , p. .

concerné que lorsqu'il y a lieu, c'est-à-dire pas lorsque les données API se rapportent à des vols intra-UE.

(11) Afin de garantir, dans la mesure du possible, une approche cohérente de la collecte et du transfert des données API par les transporteurs aériens, les règles énoncées dans le présent règlement devraient, s'il y a lieu, être alignées sur celles énoncées dans le règlement (UE) [API gestion des frontières]. Cela concerne, notamment, les règles concernant la qualité des données, l'utilisation par les transporteurs aériens de moyens automatisés pour une telle collecte, la manière précise dont ils transfèrent les données API recueillies au routeur et l'effacement des données API.

(12) Afin de garantir le traitement conjoint des données API et des données PNR, pour lutter efficacement contre le terrorisme et les formes graves de criminalité dans l'Union tout en réduisant au minimum l'atteinte aux droits fondamentaux des passagers protégés par la charte, les UIP devraient être les autorités compétentes des États membres chargées de recevoir, puis de traiter et de protéger les données API recueillies et transférées en vertu du présent règlement. Par souci d'efficacité et afin de réduire au minimum les risques pour la sécurité, le routeur, tel qu'il a été conçu, développé, hébergé et techniquement entretenu par l'Agence de l'Union européenne pour la gestion opérationnelle des systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice (eu-LISA) conformément au règlement (UE) [API gestion des frontières], devrait transmettre aux UIP les données API, recueillies et transférées par les transporteurs aériens au titre du présent règlement. Compte tenu du niveau nécessaire de protection des données API constituant des données à caractère personnel, notamment pour garantir la confidentialité des informations concernées, les données API devraient être transmises par le routeur aux UIP concernées de manière automatisée.

(13) Pour les vols extra-UE, l'UIP de l'État membre sur le territoire duquel le vol atterrira ou du territoire duquel le vol décollera devrait recevoir les données API du routeur pour tous ces vols, étant donné que les données PNR sont recueillies pour tous ces vols conformément à la directive (UE) 2016/681. Le routeur devrait identifier le vol et les UIP correspondantes en utilisant les informations contenues dans le code repère du dossier passager, un élément de données commun aux ensembles de données API et PNR qui permet le traitement conjoint des données API et PNR par les UIP.

(14) En ce qui concerne les vols intra-UE, conformément à la jurisprudence de la Cour de justice de l'Union européenne (CJUE), afin d'éviter de porter atteinte aux droits fondamentaux concernés qui sont protégés par la charte et de garantir le respect des exigences du droit de l'Union en matière de libre circulation des personnes et de suppression du contrôle aux frontières intérieures, il convient de prévoir une approche sélective. Compte tenu de l'importance d'assurer que les données API puissent être traitées conjointement avec les données PNR, cette approche devrait être alignée sur celle de la directive (UE) 2016/681. Pour ces raisons, les données API relatives à ces vols ne devraient être transmises du routeur aux UIP concernées que lorsque les États membres ont sélectionné les vols concernés en application de l'article 2 de la directive (UE) 2016/681. Comme l'a rappelé la CJUE, la sélection implique que les États membres ciblent les obligations en question uniquement, entre autres, sur certaines liaisons, certains schémas de voyage ou certains aéroports, sous réserve du réexamen régulier de cette sélection.

(15) Afin de permettre l'application de cette approche sélective au titre du présent règlement aux vols intra-UE, les États membres devraient être tenus d'établir et de

soumettre à l'eu-LISA et à la Commission les listes des vols qu'ils ont sélectionnés, de sorte que l'eu-LISA puisse veiller à ce que seules les données API pour ces vols soient transmises du routeur aux UIP concernées et à ce que les données API relatives aux autres vols intra-UE soient immédiatement et définitivement effacées.

(16) Afin de ne pas compromettre l'efficacité du système qui repose sur la collecte et le transfert de données API, dans le cadre du présent règlement, et de données PNR, dans le cadre du système établi par la directive (UE) 2016/681 aux fins de la prévention et de la détection des infractions terroristes et des formes graves de criminalité, ainsi que des enquêtes et des poursuites en la matière, notamment en créant un risque de contournement, les informations sur les vols intra-UE sélectionnés devraient être traitées de manière confidentielle. Pour cette raison, ces informations ne devraient pas être partagées avec les transporteurs aériens, lesquels devraient donc être tenus de recueillir des données API sur tous les vols couverts par le présent règlement, y compris tous les vols intra-UE, puis de les transférer au routeur, dans les cas où la sélection nécessaire devrait être effectuée. En outre, la collecte de données API sur tous les vols intra-UE permet d'éviter que les passagers sachent quelles données API sélectionnées sur les vols intra-UE, et donc également quelles données PNR, sont transmises aux UIP conformément à l'évaluation des États membres. Cette approche garantit également que toute modification de cette sélection peut être appliquée rapidement et efficacement, sans imposer de charges économiques et opérationnelles indues aux transporteurs aériens.

(17) Afin de garantir le respect du droit fondamental à la protection des données à caractère personnel, et conformément au règlement (UE) [API gestion des frontières], le présent règlement devrait identifier les responsables du traitement. En vue d'assurer un contrôle efficace, de garantir une protection adéquate des données à caractère personnel et de réduire au minimum les risques pour la sécurité, il convient également de prévoir des règles relatives à l'enregistrement des données, à la sécurité du traitement et à l'autocontrôle. Lorsqu'elles concernent le traitement de données à caractère personnel, ces dispositions devraient être interprétées comme complétant les actes d'application générale du droit de l'Union relatif à la protection des données à caractère personnel, en particulier le règlement (UE) 2016/679 du Parlement européen et du Conseil[30], la directive (UE) 2016/680 du Parlement européen et du Conseil[31] et le règlement (UE) 2018/1725 du Parlement européen et du Conseil[32]. Ces actes, qui s'appliquent également au traitement des données à caractère personnel prévu par le présent règlement et effectué conformément à ses dispositions, ne devraient pas être affectés par le présent règlement.

---

30 Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), JO L 119 du 4.5.2016, p. 1.

31 Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil, JO L 119 du 4.5.2016, p. 89.

32 Règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) nº 45/2001 et la décision nº 1247/2002/CE, JO L 295 du 21.11.2018, p. 39.

(18) Le routeur qui doit être créé et exploité au titre du règlement (UE) [API gestion des frontières] devrait réduire et simplifier les connexions techniques nécessaires au transfert des données API, en les limitant à une connexion unique par transporteur aérien et par UIP. Par conséquent, le présent règlement prévoit l'obligation, pour les UIP et pour les transporteurs aériens, d'établir une telle connexion avec le routeur et de réaliser l'intégration requise à celui-ci, de manière à garantir le bon fonctionnement du système de transfert des données API établi par le présent règlement.

(19) Compte tenu des intérêts de l'Union en jeu, les coûts appropriés exposés par les États membres pour leurs connexions au routeur et leur intégration à celui-ci, conformément au présent règlement, devraient être pris en charge par le budget de l'Union, conformément à la législation applicable et sous réserve de certaines exceptions. Les coûts couverts par ces exceptions devraient être pris en charge par chaque État membre concerné lui-même.

(20) Conformément au règlement (UE) 2018/1726, les États membres peuvent confier à l'eu-LISA la tâche de faciliter la connectivité avec les transporteurs aériens afin d'aider les États membres à mettre en œuvre la directive (UE) 2016/681, notamment en recueillant et en transférant des données PNR par l'intermédiaire du routeur.

(21) Il ne peut être exclu que, en raison de circonstances exceptionnelles et malgré toutes les mesures raisonnables prises conformément au présent règlement et, pour ce qui est du routeur, conformément au règlement (UE) [API gestion des frontières], le routeur ou les systèmes ou l'infrastructure reliant les UIP et les transporteurs aériens au routeur ne fonctionnent pas correctement, entraînant l'impossibilité technique d'utiliser le routeur pour transmettre des données API. Compte tenu de l'indisponibilité du routeur et du fait qu'il ne sera, en général, pas raisonnablement possible aux transporteurs aériens de transférer les données API concernées par la défaillance de manière licite, sécurisée, efficace et rapide par d'autres moyens, l'obligation des transporteurs aériens de transférer ces données API au routeur devrait cesser de s'appliquer aussi longtemps que l'impossibilité technique persiste. Afin d'en réduire au minimum la durée et les conséquences négatives, les parties concernées devraient en pareil cas s'informer mutuellement sans tarder et prendre immédiatement toutes les mesures nécessaires pour remédier à l'impossibilité technique. Cette modalité devrait être sans préjudice des obligations qui incombent à toutes les parties concernées, au titre du présent règlement, de garantir le bon fonctionnement du routeur et de leurs systèmes et infrastructures respectifs, ainsi que du fait que les transporteurs aériens sont soumis à des sanctions lorsqu'ils ne respectent pas ces obligations, y compris lorsqu'ils cherchent à invoquer cette modalité lorsque cela ne se justifie pas. Afin de prévenir de tels abus et de faciliter la surveillance et, le cas échéant, l'imposition de sanctions, les transporteurs aériens qui se prévalent de cette modalité par suite de la défaillance de leur propre système et de leur propre infrastructure devraient en rendre compte à l'autorité de surveillance compétente.

(22) Afin de garantir l'application effective des règles du présent règlement par les transporteurs aériens, il convient de prévoir la désignation et l'habilitation des autorités nationales chargées de la surveillance de ces règles. Les dispositions du présent règlement relatives à cette surveillance, y compris en ce qui concerne l'imposition de sanctions si nécessaire, ne devraient pas porter atteinte aux missions et pouvoirs des autorités de contrôle instituées conformément au règlement (UE) 2016/679 et à la directive (UE) 2016/680, y compris en ce qui concerne le traitement des données à caractère personnel au titre du présent règlement.

(23) Il convient que les États membres prévoient des sanctions effectives, proportionnées et dissuasives, y compris des sanctions financières, à l'encontre des transporteurs aériens qui ne respectent pas leurs obligations en matière de collecte et de transfert de données API au titre du présent règlement.

(24) Afin d'adopter des mesures relatives aux exigences techniques et aux règles opérationnelles concernant les moyens automatisés de collecte de données API lisibles par machine, aux protocoles et formats communs à utiliser pour le transfert de données API par les transporteurs aériens, aux règles techniques et procédurales pour la transmission des données API du routeur aux UIP, et aux connexions des UIP et des transporteurs aériens au routeur ainsi qu'à leur intégration à celui-ci, il convient de déléguer à la Commission le pouvoir d'adopter des actes conformément à l'article 290 du traité sur le fonctionnement de l'Union européenne pour ce qui concerne les articles 4, 5, 10 et 11, respectivement. Il importe particulièrement que la Commission procède aux consultations appropriées durant son travail préparatoire, y compris au niveau des experts, et que ces consultations soient menées conformément aux principes définis dans l'accord interinstitutionnel du 13 avril 2016 «Mieux légiférer»[33]. En particulier, pour assurer leur égale participation à la préparation des actes délégués, le Parlement européen et le Conseil reçoivent tous les documents au même moment que les experts des États membres, et leurs experts ont systématiquement accès aux réunions des groupes d'experts de la Commission traitant de la préparation des actes délégués.

(25) Toutes les parties intéressées, et en particulier les transporteurs aériens et les UIP, devraient disposer de suffisamment de temps pour procéder aux préparatifs nécessaires afin d'être en mesure de satisfaire à leurs obligations respectives au titre du présent règlement, compte tenu du fait que certains de ces préparatifs, tels que ceux concernant les obligations de connexion au routeur et d'intégration à celui-ci, ne pourront être finalisés qu'une fois que les phases de conception et de développement du routeur auront été achevées et que le routeur commencera à fonctionner. Par conséquent, le présent règlement ne devrait s'appliquer qu'à partir d'une date appropriée postérieure à la date de début d'exploitation du routeur, telle que spécifiée par la Commission conformément au règlement (UE) [API gestion des frontières]. Il devrait toutefois être possible à la Commission d'adopter des actes délégués au titre du présent règlement avant cette date, de manière à ce que le système mis en place par le présent règlement soit opérationnel dans les meilleurs délais.

(26) Les objectifs du présent règlement, à savoir contribuer à la prévention et à la détection des infractions terroristes et des formes graves de criminalité, ainsi qu'aux enquêtes et aux poursuites en la matière, compte tenu de la dimension transnationale des infractions concernées et de la nécessité de coopérer sur une base transfrontière pour y faire face efficacement, ne peuvent pas être atteints de manière suffisante par les États membres individuellement, mais peuvent l'être mieux au niveau de l'Union. L'Union peut donc adopter des mesures conformément au principe de subsidiarité énoncé à l'article 5 du traité sur l'Union européenne. Conformément au principe de proportionnalité tel qu'énoncé audit article, le présent règlement n'excède pas ce qui est nécessaire pour atteindre cet objectif.

(27) Conformément aux articles 1er et 2 du protocole nº 22 sur la position du Danemark annexé au traité sur l'Union européenne et au traité sur le fonctionnement de l'Union

[33] JO L 123 du 12.5.2016, p. 1.

européenne, le Danemark ne participe pas à l'adoption du présent règlement et n'est pas lié par celui-ci ni soumis à son application.

(28) [Conformément à l'article 3 du protocole n° 21 sur la position du Royaume-Uni et de l'Irlande à l'égard de l'espace de liberté, de sécurité et de justice, annexé au traité sur l'Union européenne et au traité sur le fonctionnement de l'Union européenne, l'Irlande a notifié son souhait de participer à l'adoption et à l'application du présent règlement.] OU [Conformément aux articles 1er et 2 du protocole nº 21 sur la position du Royaume-Uni et de l'Irlande à l'égard de l'espace de liberté, de sécurité et de justice, annexé au traité sur l'Union européenne et au traité sur le fonctionnement de l'Union européenne, et sans préjudice de l'article 4 dudit protocole, l'Irlande ne participe pas à l'adoption du présent règlement et n'est pas liée par celui-ci ni soumise à son application.]

(29) Le Contrôleur européen de la protection des données a été consulté conformément à l'article 42, paragraphe 1, du règlement (UE) 2018/1725 et a rendu un avis le [XX][34],

ONT ADOPTÉ LE PRÉSENT RÈGLEMENT:

CHAPITRE 1

DISPOSITIONS GÉNÉRALES

Article premier

Objet

Aux fins de la prévention et de la détection des infractions terroristes et des formes graves de criminalité, ainsi que des enquêtes et des poursuites en la matière, le présent règlement établit les règles concernant:

a) la collecte par les transporteurs aériens d'informations préalables sur les passagers (ci-après les «données API») sur les vols extra-UE et certains vols intra-UE;

b) le transfert au routeur, par les transporteurs aériens, des données API;

c) la transmission par le routeur aux unités d'informations passagers (UIP) des données API sur les vols extra-UE et certains vols intra-UE.

Article 2

Champ d'application

Le présent règlement s'applique aux transporteurs aériens assurant des vols extra-UE ou intra-UE, réguliers ou non.

Article 3

Définitions

Aux fins du présent règlement, on entend par:

[34] [JO C …].

a) «transporteur aérien», une entreprise de transport aérien au sens de l'article 3, point 1), de la directive (UE) 2016/681;

b) «vol extra-UE», tout vol au sens de l'article 3, point 2), de la directive (UE) 2016/681;

c) «vol intra-UE», tout vol au sens de l'article 3, point 3), de la directive (UE) 2016/681;

d) «vol régulier», un vol au sens de l'article 3, point e), du règlement (UE) [API gestion des frontières];

e) «vol non régulier», un vol au sens de l'article 3, point f), du règlement (UE) [API gestion des frontières];

f) «passager», toute personne au sens de l'article 3, point 4), de la directive (UE) 2016/681;

g) «membre d'équipage», toute personne au sens de l'article 3, point h), du règlement (UE) [API gestion des frontières];

h) «voyageur», toute personne au sens de l'article 3, point i), du règlement (UE) [API gestion des frontières];

i) «informations préalables sur les passagers» ou «données API», les données au sens de l'article 3, point j), du règlement (UE) [API gestion des frontières];

j) «dossier(s) passager(s)» ou «PNR», un dossier relatif aux conditions de voyage de chaque passager au sens de l'article 3, point 5), de la directive (UE) 2016/681;

k) «unité d'informations passagers» ou «UIP», l'autorité compétente mise en place par un État membre, telle qu'elle figure dans les notifications et modifications publiées par la Commission conformément à l'article 4, paragraphes 1 et 5, respectivement, de la directive (UE) 2016/681;

l) «infractions terroristes», les infractions au sens des articles 3 à 12 de la directive (UE) 2017/541 du Parlement européen et du Conseil[35];

m) «formes graves de criminalité», les infractions au sens de l'article 3, point 9, de la directive (UE) 2016/681;

n) «routeur», le routeur au sens de l'article 3, point k), du règlement (UE) [API gestion des frontières];

o) «données à caractère personnel», toute information au sens de l'article 4, point 1), du règlement (UE) 2016/679.

CHAPITRE 2

TRAITEMENT DES DONNÉES API

[35] Directive (UE) 2017/541 du Parlement européen et du Conseil du 15 mars 2017 relative à la lutte contre le terrorisme et remplaçant la décision-cadre 2002/475/JAI du Conseil et modifiant la décision 2005/671/JAI du Conseil (JO L 88 du 31.3.2017, p. 6).

Article 4

Collecte, transfert et effacement des données API par les transporteurs aériens

1. Les transporteurs aériens recueillent les données API des voyageurs des vols visés à l'article 2, aux fins du transfert de ces données API au routeur conformément au paragraphe 6. Lorsqu'il s'agit d'un vol en partage de code entre un ou plusieurs transporteurs aériens, l'obligation de transférer les données API incombe au transporteur aérien qui assure le vol.

2. Les transporteurs aériens recueillent les données API de manière à ce que les données API qu'ils transfèrent conformément au paragraphe 6 soient exactes, complètes et à jour.

3. Les transporteurs aériens recueillent les données API visées à l'article 4, paragraphe 2, points a) à d), du règlement (UE) [API gestion des frontières] à l'aide de moyens automatisés permettant la collecte des données lisibles par machine du document de voyage du voyageur concerné. Ils recueillent ces données conformément aux exigences techniques et règles opérationnelles détaillées visées au paragraphe 5, lorsque de telles règles ont été adoptées et sont applicables.

   Toutefois, lorsqu'une telle utilisation de moyens automatisés n'est pas possible parce que le document de voyage ne contient pas de données lisibles par machine, les transporteurs aériens recueillent ces données manuellement, de manière à garantir le respect du paragraphe 2.

4. Tout moyen automatisé utilisé par les transporteurs aériens pour recueillir des données API au titre du présent règlement doit être fiable, sécurisé et à jour.

5. La Commission est habilitée à adopter des actes délégués conformément à l'article 19, afin de compléter le présent règlement en fixant des exigences techniques et règles opérationnelles détaillées pour la collecte des données API visées à l'article 4, paragraphe 2, points a) à d), du règlement (UE) [API gestion des frontières], à l'aide de moyens automatisés, conformément aux paragraphes 3 et 4 du présent article.

6. Les transporteurs aériens transfèrent par voie électronique au routeur les données API recueillies en application du paragraphe 1. Ils transfèrent ces données conformément aux règles détaillées visées au paragraphe 9, lorsque de telles règles ont été adoptées et sont applicables.

7. Les transporteurs aériens transfèrent les données API au moment de l'enregistrement et immédiatement après la clôture du vol, c'est-à-dire dès que les passagers ont embarqué à bord de l'aéronef prêt à partir et qu'il n'est plus possible à des passagers ni d'embarquer à bord de celui-ci ni d'en débarquer.

8. Sans préjudice de la possibilité pour les transporteurs aériens de conserver et d'utiliser les données lorsque cela est nécessaire au cours normal de leurs activités dans le respect du droit applicable, les transporteurs aériens soit rectifient, complètent ou mettent à jour immédiatement les données API concernées, soit les effacent de manière définitive, dans les deux situations suivantes:

   lorsqu'ils constatent que les données API recueillies sont inexactes ou incomplètes, ne sont plus à jour ou ont été traitées de manière illicite, ou que les données transférées ne constituent pas des données API;

   lorsque le transfert des données API conformément au paragraphe 3 a été effectué.

Lorsque les transporteurs aériens font la constatation visée au premier alinéa, point a), du présent paragraphe après avoir effectué le transfert des données conformément au paragraphe 6, ils en informent immédiatement l'Agence de l'Union européenne pour la gestion opérationnelle des systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice (eu-LISA). Dès réception de ces informations, l'eu-LISA informe immédiatement les UIP qui ont reçu les données API transmises par l'intermédiaire du routeur.

9. La Commission est habilitée à adopter des actes délégués conformément à l'article 19, afin de compléter le présent règlement en fixant les règles détaillées nécessaires concernant les protocoles communs et les formats de données reconnus à appliquer pour les transferts de données API au routeur visés au paragraphe 6.

Article 5

Transmission des données API du routeur aux UIP

1. Le routeur transmet immédiatement et de manière automatisée les données API, transférées par les transporteurs aériens conformément à l'article 4, aux UIP de l'État membre sur le territoire duquel le vol atterrira ou du territoire duquel il décollera, ou des deux États membres dans le cas de vols intra-UE. Lorsqu'un vol comporte une ou plusieurs escales sur le territoire d'autres États membres que celui de départ, le routeur transmet les données API aux UIP de tous les États membres concernés.

   Aux fins de cette transmission, l'eu-LISA établit et tient à jour un tableau de correspondance entre les différents aéroports d'origine et de destination et les pays auxquels ils appartiennent.

   Toutefois, pour les vols intra-UE, le routeur ne transmet les données API à l'UIP que pour les vols figurant sur la liste visée au paragraphe 2.

   Le routeur transfère les données API conformément aux règles détaillées visées au paragraphe 3, lorsque de telles règles ont été adoptées et sont applicables.

2. Les États membres qui décident d'appliquer la directive (UE) 2016/681 aux vols intra-UE, ainsi que le prévoit son article 2, établissent chacun une liste des vols intra-UE concernés et la communiquent à l'eu-LISA, au plus tard à la date d'application du présent règlement visée à l'article 21, deuxième alinéa. En application de l'article 2 de ladite directive, ces États membres réexaminent régulièrement ces listes et, si nécessaire, les actualisent, et ils communiquent immédiatement à l'eu-LISA toute liste actualisée. Les informations figurant sur ces listes sont traitées de manière confidentielle.

3. La Commission est habilitée à adopter des actes délégués conformément à l'article 19, afin de compléter le présent règlement en fixant les règles techniques et procédurales détaillées nécessaires à appliquer pour les transmissions de données API au routeur visées au paragraphe 1.

CHAPITRE 3

JOURNALISATION, PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL ET SÉCURITÉ

Article 6

Tenue de registres

1. Les transporteurs aériens établissent des registres de toutes les opérations de traitement effectuées au titre du présent règlement, en utilisant les moyens automatisés visés à l'article 4, paragraphe 3. Ces registres indiquent la date, l'heure et le lieu de transfert des données API.

2. Les registres visés au paragraphe 1 ne peuvent servir qu'à garantir la sécurité et l'intégrité des données API et la licéité du traitement, en particulier en ce qui concerne le respect des exigences énoncées dans le présent règlement, y compris les modalités de sanction en cas de violation de ces exigences, prévues aux articles 15 et 16.

3. Les transporteurs aériens prennent des mesures appropriées pour protéger les registres créés conformément au paragraphe 1 contre un accès non autorisé et d'autres risques pour la sécurité.

4. Les transporteurs aériens conservent les registres créés conformément au paragraphe 1 pendant un délai d'un an à compter de la date de leur création. Ils effacent lesdits registres immédiatement et de manière définitive à l'expiration de ce délai.

   Toutefois, si lesdits registres sont nécessaires aux procédures destinées à contrôler ou à garantir la sécurité et l'intégrité des données API ou la licéité des opérations de traitement, ainsi qu'il est mentionné au paragraphe 2, et si ces procédures ont déjà démarré à la date d'expiration du délai visé au premier alinéa, les transporteurs aériens peuvent conserver ces registres aussi longtemps que nécessaire aux fins de ces procédures. Dans ce cas, ils effacent lesdits registres dès qu'ils ne sont plus nécessaires aux fins de ces procédures.

Article 7

Responsables du traitement des données à caractère personnel

Les UIP sont des responsables du traitement, au sens de l'article 3, point 8), de la directive (UE) 2016/680, en ce qui concerne le traitement des données API constituant des données à caractère personnel en vertu du présent règlement par l'intermédiaire du routeur, y compris la transmission et le stockage de ces données sur le routeur pour des raisons techniques.

Les transporteurs aériens sont des responsables du traitement, au sens de l'article 4, point 7), du règlement (UE) 2016/679, pour le traitement des données API constituant des données à caractère personnel effectué lorsqu'ils recueillent ces données et les transfèrent au routeur en vertu du présent règlement.

Article 8

Sécurité

Les UIP et les transporteurs aériens veillent à la sécurité des données API qu'ils traitent en application du présent règlement, en particulier celles constituant des données à caractère personnel.

Les UIP et les transporteurs aériens coopèrent entre eux et avec l'eu-LISA, en fonction de leurs responsabilités respectives et dans le respect du droit de l'Union, afin d'assurer cette sécurité.

Article 9

Autocontrôle

Les transporteurs aériens et les UIP contrôlent le respect de leurs obligations respectives au titre du présent règlement, en particulier pour le traitement des données API constituant des données à caractère personnel, notamment par une vérification régulière des registres conformément à l'article 7.

CHAPITRE 4

DISPOSITIONS RELATIVES AU ROUTEUR

Article 10

Connexion des UIP au routeur

1. Les États membres veillent à ce que leurs UIP soient connectées au routeur. Ils veillent à ce que leurs systèmes et infrastructures nationaux pour la réception et le traitement ultérieur des données API transférées en vertu du présent règlement soient intégrés au routeur.

   Les États membres veillent à ce que la connexion à ce routeur et l'intégration à celui-ci permettent à leurs UIP de recevoir et de traiter ultérieurement les données API, ainsi que d'échanger toute communication y afférente, de manière licite, sécurisée, efficace et rapide.

2. La Commission est habilitée à adopter des actes délégués conformément à l'article 19, afin de compléter le présent règlement en fixant les règles détaillées nécessaires à appliquer pour les connexions au routeur et l'intégration à celui-ci visées au paragraphe 1.

Article 11

Connexion des transporteurs aériens au routeur

1. Les transporteurs aériens veillent à être connectés au routeur. Ils veillent à ce que leurs systèmes et infrastructures pour la transmission des données API au routeur prévue par le présent règlement soient intégrés au routeur.

   Les transporteurs aériens veillent à ce que la connexion au routeur et l'intégration à celui-ci leur permettent de transférer les données API, ainsi que d'échanger toute communication y afférente, de manière licite, sécurisée, efficace et rapide.

2. La Commission est habilitée à adopter des actes délégués conformément à l'article 19, afin de compléter le présent règlement en fixant les règles détaillées nécessaires à appliquer pour les connexions au routeur et l'intégration à celui-ci visées au paragraphe 1.

Article 12

Coûts exposés par les États membres

1. Les coûts exposés par les États membres pour leurs connexions au routeur et l'intégration à celui-ci, conformément à l'article 10, sont à la charge du budget général de l'Union.

   Toutefois, les coûts suivants sont exclus et sont à la charge des États membres:

   a) les coûts de gestion du projet, dont les coûts des réunions, des missions et des bureaux;

   b) les coûts afférents à l'hébergement des systèmes d'information nationaux, dont ceux liés à l'espace, à la mise en œuvre, à l'électricité et au refroidissement;

   c) les coûts afférents au fonctionnement des systèmes d'information nationaux, dont ceux liés aux contrats conclus avec les opérateurs et aux contrats d'appui;

   d) les coûts afférents à la conception, au développement, à la mise en œuvre, au fonctionnement et à la maintenance des réseaux de communication nationaux.

2. Les États membres prennent également en charge les coûts afférents à la gestion, à l'utilisation et à la maintenance de leurs connexions au routeur et de l'intégration à celui-ci.

Article 13

Mesures à prendre en cas d'impossibilité technique d'utiliser le routeur

1. Lorsqu'il est techniquement impossible d'utiliser le routeur pour transmettre des données API, en raison d'une défaillance de celui-ci, l'eu-LISA informe, immédiatement et de manière automatisée, les transporteurs aériens et les UIP de cette impossibilité technique. Dans ce cas, l'eu-LISA prend immédiatement des mesures pour remédier à l'impossibilité technique d'utiliser le routeur et informe immédiatement ces parties lorsqu'il y a été remédié.

   Durant la période comprise entre ces notifications, l'article 4, paragraphe 6, ne s'applique pas, dans la mesure où l'impossibilité technique empêche le transfert de données API au routeur. Le cas échéant, l'article 4, paragraphe 1, ne s'applique pas non plus aux données API en question pendant cette période.

2. Lorsqu'il est techniquement impossible d'utiliser le routeur pour transmettre des données API, en raison d'une défaillance des systèmes ou de l'infrastructure d'un État membre, visés à l'article 10, l'UIP dudit État membre informe, immédiatement et de manière automatisée, les transporteurs aériens, les autres UIP, l'eu-LISA et la Commission de cette impossibilité technique. Dans ce cas, ledit État membre prend immédiatement des mesures pour remédier à l'impossibilité technique d'utiliser le routeur et informe immédiatement ces parties lorsqu'il y a été remédié.

   Durant la période comprise entre ces notifications, l'article 4, paragraphe 6, ne s'applique pas, dans la mesure où l'impossibilité technique empêche le transfert de données API au routeur. Le cas échéant, l'article 4, paragraphe 1, ne s'applique pas non plus aux données API en question pendant cette période.

3. Lorsqu'il est techniquement impossible d'utiliser le routeur pour transmettre des données API, en raison d'une défaillance des systèmes ou de l'infrastructure d'un transporteur aérien, visés à l'article 11, ledit transporteur aérien informe, immédiatement et de manière automatisée, les UIP, l'eu-LISA et la Commission de cette impossibilité technique. Dans ce cas, ledit transporteur aérien prend

immédiatement des mesures pour remédier à l'impossibilité technique d'utiliser le routeur et informe immédiatement ces parties lorsqu'il y a été remédié.

Durant la période comprise entre ces notifications, l'article 4, paragraphe 6, ne s'applique pas, dans la mesure où l'impossibilité technique empêche le transfert de données API au routeur. Le cas échéant, l'article 4, paragraphe 1, ne s'applique pas non plus aux données API en question pendant cette période.

Lorsqu'il a été remédié à l'impossibilité technique, le transporteur aérien concerné soumet, sans tarder, à l'autorité de contrôle nationale compétente visée à l'article 15 *bis* un rapport contenant toutes les précisions nécessaires sur l'impossibilité technique, notamment ses raisons, son ampleur et ses conséquences, ainsi que les mesures prises pour y remédier.

Article 14

Responsabilité concernant le routeur

Si le non-respect, par un État membre ou un transporteur aérien, des obligations qui lui incombent au titre du présent règlement cause un dommage au routeur, cet État membre ou ce transporteur en est tenu pour responsable, sauf si, et dans la mesure où, l'eu-LISA, n'a pas pris de mesures raisonnables pour prévenir le dommage ou en atténuer les effets.

CHAPITRE 5

CONTRÔLE, SANCTIONS ET MANUEL

Article 15

Autorité de contrôle nationale

1. Les États membres désignent une ou plusieurs autorités de contrôle nationales chargées de contrôler l'application, sur leur territoire, des dispositions du présent règlement par les transporteurs aériens et de veiller au respect de ces dispositions.

2. Les États membres veillent à ce que les autorités de contrôle nationales disposent de tous les moyens nécessaires et de tous les pouvoirs d'enquête et d'exécution requis pour s'acquitter de leurs missions prévues par le présent règlement, y compris en imposant les sanctions visées à l'article 16, s'il y a lieu. Ils fixent les modalités d'exécution de ces missions et d'exercice de ces pouvoirs, en veillant à ce que l'exécution et l'exercice soient effectifs, proportionnés et dissuasifs, et soient encadrés dans le respect des droits fondamentaux garantis par le droit de l'Union.

3. Les États membres communiquent à la Commission, au plus tard à la date d'application du présent règlement visée à l'article 21, deuxième alinéa, le nom et les coordonnées des autorités qu'ils ont désignées en vertu du paragraphe 1, ainsi que les modalités qu'ils ont arrêtées en application du paragraphe 2. Ils l'informent sans tarder de tout changement ou de toute modification ultérieurs à cet égard.

4. Le présent article est sans préjudice des pouvoirs des autorités de contrôle visées à l'article 51 du règlement (UE) 2016/679 et à l'article 41 de la directive (UE) 2016/680.

Article 16

Sanctions

Les États membres déterminent le régime des sanctions applicables en cas de violation du présent règlement et prennent toutes les mesures nécessaires pour assurer l'application de ces sanctions. Les sanctions prévues sont effectives, proportionnées et dissuasives.

Les États membres informent la Commission, au plus tard à la date d'application du présent règlement, mentionnée à l'article 21, deuxième alinéa, du régime et des mesures ainsi déterminés et l'informent sans tarder de toute modification ultérieure.

Article 17

Manuel pratique

La Commission, en étroite coopération avec les UIP, les autres autorités concernées des États membres, les transporteurs aériens et les agences compétentes de l'Union, élabore et met à la disposition du public un manuel pratique contenant des lignes directrices, des recommandations et des bonnes pratiques pour la mise en œuvre du présent règlement.

Le manuel pratique tient également compte des manuels pertinents existants.

La Commission adopte le manuel pratique sous la forme d'une recommandation.

CHAPITRE 6

LIEN AVEC D'AUTRES INSTRUMENTS EXISTANTS

Article 18

Modifications apportées au règlement (UE) 2019/818

___

À l'article 39, les paragraphes 1 et 2 sont remplacés par le texte suivant:

«1. Un répertoire central des rapports et statistiques (CRRS) est créé pour soutenir les objectifs du SIS, d'Eurodac et de l'ECRIS-TCN, conformément aux différents instruments juridiques régissant ces systèmes, et pour fournir des statistiques intersystèmes et des rapports analytiques à des fins stratégiques, opérationnelles et de qualité des données. Le CRRS soutient également les objectifs du règlement (UE).../... du Parlement européen et du Conseil* [*le présent règlement*].»

* Règlement (UE) [numéro] du Parlement européen et du Conseil du xy relatif à/au [titre officiellement adopté] (JO L...)».

«2. L'eu-LISA établit, met en œuvre et héberge sur ses sites techniques le CRRS contenant les données et les statistiques visées à l'article 74 du règlement (UE) 2018/1862 et à l'article 32 du règlement (UE) 2019/816, séparées logiquement par système d'information de l'UE. L'eu-LISA recueille également les données et les statistiques provenant du routeur visé à l'article 13, paragraphe 1, du règlement (UE) .../... * [*le présent règlement*]. L'accès au CRRS est accordé, moyennant un accès contrôlé et sécurisé et des profils d'utilisateur spécifiques, aux seules fins de

l'élaboration de rapports et de statistiques, aux autorités visées à l'article 74 du règlement (UE) 2018/1862, à l'article 32 du règlement (UE) 2019/816 et à l'article 13, paragraphe 1, du règlement (UE) .../... * [*le présent règlement*].

CHAPITRE 7

DISPOSITIONS FINALES

Article 19

Exercice de la délégation

1. Le pouvoir d'adopter des actes délégués conféré à la Commission est soumis aux conditions fixées au présent article.

2. Le pouvoir d'adopter des actes délégués visé à l'article 4, paragraphes 5 et 9, à l'article 5, paragraphe 3, à l'article 10, paragraphe 2, et à l'article 11, paragraphe 2, est conféré à la Commission pour une période de cinq ans à compter [*date d'adoption du règlement*]. La Commission élabore un rapport relatif à la délégation de pouvoir au plus tard neuf mois avant la fin de la période de cinq ans. La délégation de pouvoir est tacitement prorogée pour des périodes d'une durée identique, sauf si le Parlement européen ou le Conseil s'oppose à cette prorogation au plus tard trois mois avant la fin de chaque période.

3. La délégation de pouvoir visée à l'article 4, paragraphes 5 et 9, à l'article 5, paragraphe 3, à l'article 10, paragraphe 2, et à l'article 11, paragraphe 2, peut être révoquée à tout moment par le Parlement européen ou le Conseil. La décision de révocation met fin à la délégation de pouvoir qui y est précisée. La révocation prend effet le jour suivant celui de la publication de ladite décision au Journal officiel de l'Union européenne ou à une date ultérieure qui est précisée dans ladite décision. Elle ne porte pas atteinte à la validité des actes délégués déjà en vigueur.

4. Avant l'adoption d'un acte délégué, la Commission consulte les experts désignés par chaque État membre, conformément aux principes définis dans l'accord interinstitutionnel du 13 avril 2016 «Mieux légiférer».

5. Dès qu'elle adopte un acte délégué, la Commission le notifie au Parlement européen et au Conseil simultanément.

Article 20

Suivi et évaluation

1. Au plus tard [*quatre ans après l'entrée en vigueur du présent règlement*], et ensuite tous les quatre ans, la Commission établit un rapport présentant une évaluation globale du présent règlement, dont une évaluation de:

   a) l'application du présent règlement;

   b) la mesure dans laquelle le présent règlement a atteint ses objectifs;

   c) l'incidence du présent règlement sur les droits fondamentaux protégés par le droit de l'Union;

   d) La Commission présente le rapport d'évaluation au Parlement européen, au Conseil, au Contrôleur européen de la protection des données et à l'Agence des

droits fondamentaux de l'Union européenne. S'il y a lieu, au vu de l'évaluation effectuée, la Commission soumet une proposition législative au Parlement européen et au Conseil en vue de modifier le présent règlement.

2. Les États membres et les transporteurs aériens communiquent à la Commission, à sa demande, les informations nécessaires à l'établissement des rapports visés au paragraphe 1. Toutefois, les États membres peuvent s'abstenir de communiquer ces informations si, et dans la mesure où, c'est nécessaire pour ne pas divulguer des méthodes de travail confidentielles ou ne pas compromettre des enquêtes en cours de leurs UIP ou d'autres autorités répressives. La Commission veille à ce que toute information confidentielle communiquée soit correctement protégée.

Article 21

Entrée en vigueur et application

Le présent règlement entre en vigueur le vingtième jour suivant celui de sa publication au *Journal officiel de l'Union européenne*.

Il s'applique deux ans après la date de mise en service du routeur, telle que spécifiée par la Commission conformément à l'article 27 du règlement (UE) [API gestion des frontières].

Toutefois, l'article 4, paragraphes 5 et 9, l'article 5, paragraphe 3, l'article 10, paragraphe 2, l'article 11, paragraphe 2, et l'article 19 sont applicables à partir de [*date d'entrée en vigueur du présent règlement*].

Le présent règlement est obligatoire dans tous ses éléments et directement applicable dans les États membres conformément aux traités.

Fait à Strasbourg, le

Par le Parlement européen	*Par le Conseil*
La présidente	*Le président*

FICHE FINANCIÈRE LÉGISLATIVE

Les incidences financières de la présente proposition sont incluses dans la fiche financière législative commune annexée à la proposition de règlement (UE) [API gestion des frontières].